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

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

Факультет соціології і права
Навчально-науковий центр інформаційного права
та правових питань інформаційних технологій

ПРАВА, СВОБОДИ І БЕЗПЕКА ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

10 травня 2018 року

Київ
КПІ ім. Ігоря Сікорського
2018

УДК 34 : 004] (063)
П-68

Права, свободи і безпека людини в інформаційній сфері: матеріали наук.-практ. конф. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв // Нац. техн. ун-т України «КПІ ім. Ігоря Сікорського». – 10 трав. 2018 р. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. – 174 с.

Матеріали конференції присвячені розгляду теоретико-правових та практичних питань забезпечення прав, свободи і безпеки людини в інформаційній сфері в сучасних умовах, а також шляхів їх вирішення.

Для спеціалістів у сферах правотворення, правозастосування та правоохоронної діяльності, 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, передусім, з позицій осмислення трансформаційних суспільних процесів, що відбуваються 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 .участь провідні експерти і вчені наукових установ і навчальних закладів, представники зацікавлених державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право», «Правова інформатика» та Вісник «КПІ» «Політологія. Соціологія. Право»

ISBN 978-966-622-898-0

Матеріали подано у авторській редакції.
Упорядники: Фурашев В. М., Петряєв С. Ю.
Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП КПІ ім. Ігоря Сікорського
designlab.kpi.ua@gmail.com \
Балашов Д. В. (balashov.dim@gmail.com)

Рекомендовано до друку:

Вченою радою Науково-дослідного інституту інформатики і права
Національної академії правових наук України *(Протокол № 5 від 06.06.2018 р.).*

Вченою радою факультету соціології і права
Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» *(Протокол № 10 від .01.06.2018 р.).*

УДК

ISBN 978-966-622-898-0

ЗМІСТ

***Мельниченко А.А.**, к.ф.н., доцент,*
декан факультету соціології і права
КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ГАРАНТУВАННЯ ПРАВ ЛЮДИНИ І ГРОМАДЯНИНА В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Нові виклики, характерні сучасному соціуму, все більше актуалізують проблему захисту та гарантування прав людини і громадянина не тільки в Україні, а й у світі.

Сучасне суспільство, яке узвичаєно називати інформаційним, вже стикнулося з цілою низкою викликів, що несуть в собі, здавалося б, ординарні атрибути розвитку інформаційних технологій. Відомий інноватор-підприємець, фундатор SpaceX та Tesla - Ілон Маск цього року вже висловив побоювання, що штучний інтелект може створити «безсмертного диктатора», від якого нікуди не втечеш [Wagstaff K. Elon Musk warns that AI could become an 'immortal dictator' Режим доступу https://mashable.com/2018/04/06/elon-musk-artificial-intelligence-chris-paine-do-you-trust-this-computer/#JjBITvsc_mql]. З одного боку, такі коментарі мають характер замаскованого PR-ходу, проте з іншого – окремі тези про недалеке майбутнє мають сенс і обґрунтованість. Навіть найобережніша людина в питанні захисту своїх персональних даних, швидше за все має в різних мережевих базах даних «інформаційний слід». Так формування в Україні всіляких різноманітних реєстрів (освітні, медичні, банківські тощо) створюють можливість для тотального стеження за людиною (освітні, медичні, банківські), а відтак – надають додаткові інструменти вищевказаному «безсмертному диктатору».

Відтак, є необхідність вести мову про створення таких правових механізмів, які зможуть «випереджальним чином» передбачити захист конституційних прав і свобод людини вже в умовах поширення різноманітних феноменів інформаційного суспільства на кшталт Інтернету речей. Йдеться не тільки про ймовірність повсюдного порушення права на свободу вираження поглядів, права на повагу до приватного життя, права на доступ до публічної інформації тощо, а про загрози порушення таких прав як право на свободу й особисту недоторканність, право на життя, свободу пересування etc. По суті, сучасна людина в інформаційному суспільстві повинна не тільки бути обізнаною щодо своїх прав, але й мати принаймні базові знання в сфері ІТ, щоб ефективніше захищати їх.

Ще одним фактором, що сприяє збільшенню випадків порушення прав і свобод людини в інформаційній сфері, є бойові дії на території нашої держави. Під час проведення Антитерористичної операції або ж Операції об’єднаних сил, навіть без оголошення військового стану діяльність силових відомств суттєво

актуалізується і активізується. Часто це при зводить до того, що право на свободу вираження поглядів і відповідні практики щодо його реалізації «кваліфікуються» як загроза національній безпеці з відповідними наслідками для людини та громадянина. Звичайно, статтею 10 Конвенції про захист прав людини і основоположних свобод передбачено, що здійснення права на свободу вираження поглядів «може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду». Проте, визначення того, у якому випадку є загроза інтересам національної безпеки, а у яких її немає, має достатньо суб'єктивний характер, що може мати наслідком необґрунтоване обмеження прав і свобод людини. Показовою у цьому сенсі є справа «Букур і Тома проти Румунії» Європейського суду з прав людини. Рішення, яке було ухвалене у 2013 році цим судом за вказаною справою передбачало, що «кримінальне засудження державного службовця за розголошення інформації у ході резонансної прес-конференції, порушення в рамках розвідувальної програми прослуховування телефонних розмов призвели до порушення права на свободу вираження поглядів за статтею 10 Конвенції про захист прав людини і основоположних прав» [Рішення Європейського суду з прав людини щодо доступу до інформації / За заг. редакцією Шевченко Т.С., Розкладай І.Є. – К.: Москаленко О.М., 2014. – 200 с.]. Йдеться про те, Константін Букур, співробітник румунської розвідки (SRI), який відповідав за моніторинг і запис телефонних розмов осіб зі спеціального реєстру, помітив відсутність обґрунтувань необхідності прослуховувати окремих журналістів, політиків і бізнесменів, оприлюднивши низку записів на прес-конференції. Це стало причиною того, що військовий суд засудив Букура до двох років позбавлення волі за крадіжку та незаконне розкриття таємної інформації або інформації, яка стосується приватного життя, честі і репутації. В Україні є висока ймовірність виникнення таких прецедентів, адже діяльність держави щодо збереження балансу між гарантуванням демократичних прав і свобод з одного боку, і захистом національної безпеки з іншого, у період протидії гібридної агресії може отримати непередбачуваний розвиток подій.

----------***----------

Баранов О. А., *д. ю. н., с. н. с.*
НДІІП НАПрНУ

ПРАВО НА ЦИФРОВУ РІВНІСТЬ – ФУНДАМЕНТАЛЬНЕ ПРАВО СУЧАСНОСТІ.

Проблема цифрової нерівності, цифрової прірви (digital divide) дістала великого резонансу з минулого сторіччя, коли була оприлюднена у Декларації тисячоліття Організації Об'єднаних Націй (2000 р.) [1], в декларації, яка охопила практично всі відомі на той час глобальні загальнолюдські проблеми і визначила вектори розвитку землян. Спочатку ця проблема була зустрінута громадськістю неоднозначно. Висловлювалися полярні точки зору: від визнання цієї проблеми як однієї з глобальних погроз для держав і суспільств в інформаційну епоху до позначення її як надуманої, сприяючої подальшому збагаченню комп'ютерних і телекомунікаційних корпорацій і фірм. З часом дискусії перейшли в площину розробки практичних рекомендацій по подоланню цифрової нерівності, як в міжнародному масштабі, так і масштабах окремих держав.

Перш ніж досліджувати проблему цифрової нерівності слід відмітити, що нерівність як така є атрибутивною властивістю людського суспільства. Нерівність з'явилася і має місце у всіх сферах соціального життя суспільства з моменту його виникнення. Це нерівність в доступі до життєво важливих ресурсів (продовольчим, сировинним, енергетичним тощо), до робочих місць, освіти, медичних послуг, культурного спадку тощо. У основі нерівності лежать відмінності людей в соціальному статусі, кількості наявних грошових коштів, освіті, віці, місці мешкання, расі тощо. Наслідки нерівності негативно позначалися не тільки на відносинах між людьми, але і на відносинах між державами.

Різниця в соціальному і економічному статусі і можливостях громадян, напевно, є найочевиднішою, з погляду задоволення потреб людини. Безперечно те, що соціальний статус і наявність грошей багато в чому визначають доступ до соціальних благ, тому це і призводить до основного розшарування суспільства. Нерівність через віковий чинник не завжди однозначна. Наприклад, при прийомі на роботу можуть бути обмеження, як по максимальному, так і мінімальному віку.

Нерівність по місцю мешкання. Перший вододіл нерівності: місто – село. Нерівність, що викликається мешканням в сільській місцевості характерна для всіх країн. Крім того, позначається і географічна нерівність: для держав – як міжконтинентальна, так і всередині континенту; нерівність усередині країн: центр – провінція. Рівень освіти відіграє визначальну роль не тільки при

отриманні хорошої роботи, але і в реалізації високої якості соціального життя людини.

Нерівність є причиною конфліктів і соціальних катаклізмів різних масштабів і глибини в соціальних групах і в державах. Тому світова спільнота, в першу чергу розвинені країни, докладають зусилля для нейтралізації погроз глобальної і локальної стабільності, що викликаються різного роду нерівністю. Впродовж століть всі прогресивні вчення і рухи в якості основної мети декларували досягнення рівності. Практично у всіх конституціях держав одне з основних положень – це проголошення рівності громадян.

Проте, слід зазначити те, що реальної, фактичної політичної, соціальної і економічної рівності громадян і держав поки що ніхто не досяг, та і навряд чи це відбудеться в досяжному майбутньому людства.

Нерівність – це погано або добре? Питання не риторичне. З одного боку, безумовно, соціальна нерівність окремо взятих людей або держав явище негативне. Але з іншого боку, **усвідомлена нерівність є могутнім стимулом для прогресивних соціальних перетворень, для розвитку окремих людей, соціальних груп і в цілому держав.**

У разі забезпечення потенційного рівного доступу до соціальних, економічних, культурних, освітніх, технологічних можливостей для всіх людей, всіх держав їм надається реальна потенційна можливість досягти рівного соціального положення. І вже від їх волі, від їх зусиль залежить, чи продовжуватиметься фактична нерівність або вона буде усунена. Тому акцентування вирішення проблеми усунення нерівності повинно лежати не в площині забезпечення фактичної рівності, а в площині забезпечення потенційної рівності в доступі до можливостей реалізації своїх потреб, рівень і якість яких визначається суб'єктом цих потреб.

Сьогодні найбільш поширено наступне визначення: цифрова нерівність – розділення суспільства, країн на основі нерівного доступу до сучасних інформаційних технологій. Це достатньо вузьке, технократичне визначення, що не дає можливості врахувати соціальну значущість використання інформаційних технологій.

Прослідкуємо діалектику взаємовідношення цифрової нерівності і інших історично ранніх нерівностей. Цифрова нерівність є слідством ряду інших нерівностей. Дійсно, люди, що мають невисокий дохід, низький освітній рівень, вік вище за середнє, що проживають в сільській місцевості, в країнах з неефективною економікою мають значно менше шансів дістати доступ до сучасних інформаційних комп'ютерних технологій, чим молоді випускники університетів, що працюють в центральних офісах багатих транснаціональних компаній. Але з іншого боку, з урахуванням сучасних реалій, цифрова нерівність може бути причиною поглиблення традиційних нерівностей. Таким

чином, ми маємо як би замкнутий круг – цифрова нерівність є слідством інших нерівностей і, в теж час, воно заглиблює інші, історично ранішні, нерівності.

Таким чином, приходимо до ширшого визначення: **цифрова нерівність – нерівність в доступі до соціальних, економічних, освітніх, культурних і інших можливостей, що заглиблюється унаслідок нерівного доступу до інформаційних комп'ютерних технологій.** Такий підхід до визначення дозволяє системно і обґрунтовано підійти до розгляду проблеми цифрової нерівності з урахуванням всіх соціальних і економічних аспектів використання інформаційних комп'ютерних технологій.

В кінці минулого сторіччя вперше в історії людства окрім гасел політичної, соціальної і економічної рівності держав і громадян, було проголошене гасло технологічної рівності – цифрової рівності, рівності того, що несе в собі величезний соціально-економічний і етичний потенціал. Необхідно усвідомлювати те, що це зовсім не альтруїстичний порив. Багаті країни піклуються про збереження світової стабільності, про ринки збуту свій продукції, і далеко не тільки комп'ютерів, про ринки робочої сили, яку можна привертати в свою економіку. Але, не дивлячись на це, вирішення проблеми цифрової нерівності, перш за все, переслідує власні інтереси національних держав.

При обговоренні проблеми цифрової нерівності часто говорять про те, що для всіх слаборозвинених країн і для низки країн з перехідною економікою вона не є актуальною. Для них важливіше вирішити насущні проблеми: будівництво житла, доріг, виробничої інфраструктури, реформування економіки і соціальних відносин, а проблеми інформаційних технологій – це від лукавого, що відводять від рішення першочергових задач. Але вже наявний світовий досвід самих різних країн говорить про те, що таке зіставлення не вірно. **Широке використання інформаційних комп'ютерних технологій дозволяє ефективніше і швидше вирішити питання забезпечення населення доступом до багатьох соціальних можливостей і благ.**

Цифрова нерівність є слідством раніше відомих соціальних нерівностей. Практично на можливість доступу до інформаційних комп'ютерних технологій впливають і економічний стан, і освітній рівень, і вік, і місце мешкання громадян. Ці чинники носять загальний характер і лежать в основі багатьох видів нерівностей. Проте існує особлива група чинників, яка впливає на зменшення саме цифрової нерівності. Це наявність в державі розвиненої сучасної телекомунікаційної мережі, відповідної повно функціональної інфраструктури інформаційних технологій, системи освіти, орієнтованої на комп'ютерні технології, наявність відповідної атмосфери, сприяючої затребуваності інформаційних технологій в суспільстві тощо. Саме ці чинники реально впливають на зниження ступені цифрової нерівності в суспільстві.

Список використаних джерел:

1. Декларация тысячелетия Организации Объединенных Наций. Резолюция, принятая Генеральной Ассамблеей 55/2. Генеральная ассамблея ООН. 18 сентября 2000 г. URL: http://www.un.org/ru/documents/ods.asp?m =A/RES/55/2

----------***----------

Черненко Т. В., *к.ф.н., завідувач відділу гуманітарної безпеки НІСД.*

СВОБОДА СЛОВА У «ЦИФРОВУ ДОБУ» : ЗАНЕПАД ЧИ НОВИЙ РОЗКВІТ?

Успішне сприйняття та засвоєння людством новітніх цифрових технологій, які стрімко витісняють аналогові, що лише деякий час тому були актуальними, викликало до життя термін «цифрове суспільство». Як зазначав свого часу Д. Белл «Мірою того, як ми наближаємось до кінця двадцятого століття, стає дедалі очевиднішим, що ми вступаємо до інформаційної ери… базованих на «інтелектуальних технологіях», що дозволяє нам говорити про новий **принцип** суспільної організації і соціальних змін. Це також ставить в центр уваги теоретичне знання як джерело оновлення і зміни природи технічного прогресу. Так само це робить значущою й ідею глобалізації…» [2].

Необхідно констатувати, що успішна інтеграція України до актуальних світових процесів можлива лише за умови надшвидкого, випереджального розвитку та модернізації усіх без винятку галузей суспільного життя (від системи отримання нових знань до «оцифровування» економіки, соціальної сфери, культурних практик) шляхом оперативного розширення інтерактивних обмінів, взаємодій та якісної трансформації суспільства, здатного сприйняти мобільну та гнучку віртуальну єдність світу.

Ознаками сьогодення та показниками фундаментальних зрушень у пізнанні та творчості окремого індивіда є переважно інформаційна-віртуальна форма його соціалізації у суспільстві. Слушною з цього приводу є думка І. Валлерстайна стосовно того, що «…сьогоднішній вибір в одному відрізняється від попередніх. Це перший вибір, до якого залучений увесь світ, оскільки історична система, в якій ми живемо, вперше охоплює всю планету»[3]. **І це явище вимагає об'єктивного всебічного дослідження фахівців різних галузей, бо фактично у свідомості людей відбувається процес формування «гіперреальності», яка маргіналізує фізичну, подекуди дезорієнтуючи індивіда, створюючи ілюзію реального життя у соціальних**

мережах, моральної підтримки однодумців та дописувачів. Зокрема, Ян ван Дейк у роботі «Мережеве суспільство» (De Netwerkmaatschappij) підкреслює значення стрімкого росту системи соціальних комунікацій для постіндустріального суспільства, бо розглядає це суспільство як комбінаторне поєднання соціальних мереж і медіа, що, у свою чергу, формує основні засади організації та функціонування найважливіших структур цього суспільства. На нашу думку, такий підхід дещо завузький та застарілий, бо трансформації людства, пов'язані з його входженням у «цифрову добу» багато в чому непередбачувані, хоч і несуть у собі значні якісні зміни, як економічні, так і соціальні.

Так, наприклад, **суспільство XXI сторіччя** за Д. Тапскоттом має дванадцять вузлових ознак [4], серед яких найбільш визначальними є орієнтація на знання, цифрова форма представлення об'єктів, віртуалізація виробництва, інноваційна природа розвитку, інтеграція, конвергенція, динамізм, глобалізація тощо. Однак, на нашу думку, слід зважати, що будь-яка ідеалізація можливостей сучасних технологій видається сумнівною без урахування етичної складової.

Не можна не погодитись із думкою, що «рівень розвитку цифрової культури українського суспільства є недостатнім, зокрема це стосується регіонального виміру проблеми. Якщо подивитися на соціальну стратифікацію України та на рівень «комп'ютеризації», «інформатизації» регіональних шкіл, закладів культури та освіти, стає очевидним, що в нашій країні у соціальному та інтелектуальному плані співіснують як «модерні», так і «постмодерні» сегменти, поняття й цінності індустріальної і постіндустріальної (постінформаційної) доби»[1]. У той час, коли у світі вже давно зрозуміли, що зволікання із впровадженням новітніх цифрових розробок відчутно скорочує можливості розвитку економіки. Так, наприклад відповідно до дослідження «Цикл зрілості IT-трансформації», проведеного компанією Enterprise Strategy Group (ESG) на замовлення DELL (EMC) у 2017 році 96% компаній більш ніж у двічі збільшили прибуток у порівнянні з компаніями, що знаходяться на більш ранніх етапах IT-трансформації; Переважна більшість респондентів опитування (71%) підтримали думку, що IT-трансформація необхідна для подальшого ведення бізнесу та утримання ним конкурентоспроможності. Серед опитаних представників компаній, що успішно трансформувались, 85 % вважають, що їх організація «дуже потужна» або просто «потужна» і найближчими роками матимуть змогу успішно конкурувати на ринку та здобувати бізнесові перемоги на своїх напрямах роботи, лишаючи позаду ті 43% компаній, які знаходяться на більш ранніх стадіях цифрової трансформації. Представники вже трансформованих організацій зауважили, що вже активно прогресують як на шляху втілення інновацій, так і у напрямку виведення продуктів на ринок,

автоматизації «ручних» процесів та завдань,управлінні IT як центром нарощування прибутку, а не витрат на бізнес [5].

Отже, не можна не погодитись із думкою , що «**цифрова культура… за своєю гнучкістю, операційністю та мобільністю виявляється значно ефективнішою за моделі системного бачення та відповідної організації економічних процесів»[1] і сучасне українське суспільство потребує її, втім існує і ряд ризиків, як для суспільства, так і для окремої людини, на які неможливо не звертати уваги.**

Список використаних джерел:

1. Астаф'єв А.О. Питання розвитку цифрової культури українського соціуму. Аналітична записка // Національний інститут стратегічних досліджень при Президентові України. – Режим доступу:http://www.niss.gov.ua/articles/1631/.

2. Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / пер. с англ. – М.: Academia, 1999.

3. Валлерстайн И. Конец знакомого мира: Социология XXI века / пер. с англ. – М.: Логос, 2003. – С. 183.

4. Див.: Тапскотт Д. Электронно-цифровое общество: Плюсы и минусы эпохи сетевого интеллекта / пер. с англ.– К.: INT Пресс; М.: Рефл-бук, 1999. – 432 с.

5. 95% крупных компаний не отвечают требованиям нового цифрового бизнеса, – исследование ESG по заказу Dell EMC. Режим доступу: http://www.dell.com/learn/ua/ru/uacorp1/press-releases/2017-04-25-esg-study-it-transformation-maturity-curve/

----------***----------

Петряев С. Ю., *к. ю. н., доцент, заведующий кафедрой информационного права и права интеллектуальной собственности ФСП КПИ им. Игоря Сикорского.*

КЛИПОВЫЕ ЭЛЕМЕНТЫ СОВРЕМЕННОГО ОБРАЗОВАНИЯ

Термин «клиповая культура» или «клиповое сознание» ворвался в наш обиход и наше сознание совсем недавно, каких-то пятнадцать лет назад, и стал привычным для слуха миллиарда людей информационно развитых стран мира. Элвин Тоффлер, предложивший в 2003 году термин «клиповая культура», рассматривал это явление *как принципиально новое социальное явление в общей информационной культуре будущего, основанное на бесконечном мелькании информационных отрезков, и комфортное для людей соответствующего склада ума*[1]. С этим феноменом XXI века сегодня смирились практически все

пользователи информационных социальных сетей, а многие, культивируя его, успешно на нем зарабатывают. Пожалуй, единственных, кого тревожит данное явление – это учёных, которые беспрестанно бьют тревогу за будущее сознание нового поколения. Хотя, и среди них мы видим скептиков и оптимистов.

Для скептиков, а их большинство, клиповое сознание отупляет людей, делает их примитивными, податливыми для манипуляции и влияния; вокруг происходящее они рассматривают как яркую картинку в ряду множества; у них обеднена устная и письменная речь, минимизирована умственная активность и атрофирована память; они не интересуются сущностью событий и не переживают за последствия. Они просто живут, как живет зверь, жуя траву и созерцая происходящее вокруг себя. Оптимисты же, в клиповости видят адаптацию человеческого мозга к новым условиям социальной среды, сформированной на основе быстро развивающихся информационных технологий. Другими словами – чему быть, тому не миновать.

На предмет сущности клипового сознания в последнее врем проведено достаточно много исследований, которые свидетельствуют о высокой скорости «поиска» и «фиксации» необходимой информации и, в то же врем, неспособности ее осмысления. Исследования подтверждают, что у людей с клиповым сознанием мозг эффективнее обрабатывает картинки, чем текст, причем делает это с высокой скоростью [2]. Иначе говоря, *глубокомыслие само по себе отпадает, доминирует образа над знанием* [3]. В чём сходятся взгляды скептиков и оптимистов, это в том, что люди, обладающие клиповым сознанием, утрачивают способность к когнитивному мышлению.

Поступление в вузы сегодня связано со сдачей внешнего независимого оценивания (укр. зовнішнє незалежне оцінювання – ЗНО), который осуществляется Украинским центром оценивания качества образования (УЦОКО). Цель внешнего независимого оценивания: обеспечение реализации конституционных прав граждан на равный доступ к качественному образованию, осуществления контроля за соблюдением Государственного стандарта базового и полного среднего образования, и анализа состояния системы образования, прогнозирование её развития. Оценка знаний осуществляется на основе выбора правильных ответов на поставленные вопросы выбранных дисциплин.

К данной процедуре отбора претендентов из выпускников школ на получение высшего образования отношение двойственное. С одной стороны, данная форма отбора как бы исключает субъективность оценки знаний претендентов и сводит на нет коррупцию в системе образования. С другой стороны, тестирование сводится к ответам на вопросы, вырванные из системы знаний дисциплины и не отражает реальное знания предмета в целом.

Практика последних лет показывает, что студенты первых курсов ни только не владеют достаточными знаниями включая предметы, по которым прошли независимое тестирование, но и не способные к когнитивному мышлению. Основываясь на наблюдениях автора, сегодня приблизительно 70-75 процентов студентов первых курсов обладают клиповым сознанием. Возникает вопрос, каким образом молодые люди умудряются сдавать внешнее независимое тестирование? Ответ – либо низкий уровень тестовых вопросовс одной стороны, либо – бессознательное заучивание ответов на тестовые вопросы, с другой стороны. Коррупцию мы исключили.

Можно по-разному относиться к данной процедуре оценки знаний учеников общеобразовательных учебных заведений, но вывод по данному вопросы напрашивается один, у детей работает клиповое сознание, которое внешним независимым тестированием только углубляется.

Если еще 7-10 лет назад концентрация внимания студентов на занятиях длилась 40 минут, а порой и все полтора часа, то сегодня, она снизилась до 10-15 минут. Затем наступает рассеянность внимания, появляется блуждающий взгляд, который переключает внимание слушателя на более мягкие раздражители. Из-за клипового сознания традиционные формы проведения занятий для современных студентов становятся неэффективными, скучными, трудноперенosимыми. Неспособность мозга к накоплению информации (запоминанию) и развивающийся у молодых людей гедонизм, привели к необходимости увеличить и расширить интерактивные формы проведения занятий. Начался активней процесс замены традиционной формы проведения лекций на яркие картинки –слайд шоу, т. е.клиповая форма восприятия лекционного материала, своего рода «Мурзилка» (*популярный детский литературно-художественный журнал, адресованный* ***детям от 6 до 12 лет***), где внимание слушателя направлено не на преподавателя, а на красочный информационно ограниченный слайд. Тем самым теряется контакт с лектором, а содержание контента, растворяется в яркой картинке слайда.

Невольно возникает ситуация, когда студент начинает «требовать» зрелищ уже не только на улице, но и в стенах альма-матер, ибо его мозг уже ничем не отличается от уровня «уличных народных масс». Таким образом, историю альма-матер сегодня можно представить, как тысячелетнее движение от духовного воспитания к формированию клиповых знаний.

Список використаних джерел:

1. Элвин Тоффлер. ШОК БУДУЩЕГО. URL: http://yanko.lib.ru/ books/cultur/toffler-future_shock-ru-l.pdf (дата доступа: 28.05.18).

2. Они менее образованные, но умнее вас. URL:https://s-t-o-l.com /obrazovanie/oni-menee-obrazovanny-no-umnee-vas/ (дата доступа: 28.05. 18).

3. Петряев С.Ю. «Киберцивилизация»: А ≠ А, а в общем напоминают прежних… - Інформація і право. Науковий журнал НДІІП НАПрН України. – №3(12). -2014. – С.25-30.

----------***----------

Довгань О. Д., *д.ю.н., с.н.с., перший заступник директора з наукової роботи НДІІП НАПрН України.*

ПРАВА І БЕЗПЕКА ЛЮДИНИ: ПРАВОВІ НОРМИ

Як відомо в демократичному суспільстві загальновизнані права людини і громадянина в сфері інформації виступають основним критерієм, що характеризує стан інформаційної безпеки конкретної особи і суспільства в цілому. Одним з основних пріоритетів інформаційної політики будь-якої країни є дотримання 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.

Конституція України виступає гарантом зазначених положень.

Так, стаття 3 Конституції України *(норми прямої дії)* проголошують: «Людина, її життя і здоров'я, честь і гідність, недоторканість 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].

Нам відомо, що проблему людини вивчають практично всі науки, але кожна з них під своїм кутом зору, ті аспекти, які обумовлені її потребами, і зосереджують увагу лише на певних якостях людини.

Що стосується права, для нього важливі насамперед ті риси *(властивості, ознаки)* людини, які ним охороняються. Насамперед, це найвищі соціальні

[1] Конституція України від 28 червня 1996 року // Відом. Верховної Ради України. − 1996. – № 30. – Ст. 141.

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.

Право людини, – писав творець німецької класичної філософії І. Кант, – повинно забезпечувати їй безпеку, воно надійніше за всі стіни[2].

З історії ми пам'ятаємо, що права людини були гаслом буржуазних революцій, що зруйнували феодалізм, і відіграли подібну роль у падінні тоталітарних режимів, розвалі комуністичної системи, розпаді СРСР та створенні на його теренах цілої низки суверенних, незалежних, соціальних, правових, демократичних держав[3]. Права людини були ідеологічної основою Конституції Пилипа Орлика.

Ідея невід'ємних прав людини стала основою перших у світі конституцій. В Декларації незалежності Сполучених Штатів *(підписана 1776 року в Америці)*[4] визначено, що всі люди створені рівними і всі вони наділені Творцем невід'ємними правами, до яких належать права на життя, на свободу і на прагнення до щастя. Цікавим моментом було те, що у разі порушення владою (урядом) прав, народ має право ліквідувати і встановити нову, засновану на таких принципах, які повинні якнайкраще забезпечити безпеку і благополуччя народу.

Подібні права людини були проголошені і у Декларації прав людини і громадянина Франції (*прийнята постановою Французьких Національних зборів 26 серпня 1789)*. Зокрема, зазначалося «Люди народжуються і залишаються вільними і рівними в правах. Суспільні відмінності можуть ґрунтуватися лише на загальній користі. Мета всякого політичного союзу – забезпечення природних і невід'ємних прав людини. Такі – свобода, власність, безпека і опір пригнобленню»[5]. Таким чином, ми бачимо, означене підтверджує не тільки життєздатність ідеї невід'ємних прав людини, а й їх універсальність. Основні права і свободи людини становлять підвалини справедливості, миру та безпеки для всього світового співтовариства, про що свідчать міжнародні акти та інші документи з прав людини і громадянина.

В основу Основного Закону України (*Конституції України)* також були покладені права і свободи людини *(ст.ст. 3, 21, 22, 24, 26 та ін..)*.

На підвищення стандартів законотворчості та забезпечення прав і свобод людини, акцентував увагу Голова Конституційного Суду України Станіслав Шевчук під час проведення робочих зустрічей з керівниками парламентських

---

[2] Кант.И Из лекций по этике /И.Кант// Этическая мысль: науч.- публицист.чтения. – М., 1988. – С.299-333.

[3] Тихий В.П. Безпека людини: поняття, правове забезпечення, значення, види / В. П. Тихий // Вісник Національної академії правових наук України. - 2016. - № 2. - С. 31-46. - Режим доступу: http://nbuv.gov.ua/UJRN/vapny_2016_2_5

[4] https://uk.wikipedia.org/wiki/ Декларація незалежності

[5] https://uk.wikisource.org/wiki/ Декларація_прав_людини_і_громадянина

фракцій та груп. При цьому, ним було піднято питання щодо зміцнення авторитету Основного Закону держави і зазначено, що «Українська Конституція має бути сакральним документом, спрямованим на служіння людині».

Що стосується безпеки людини, то сама ідея була висунута в теорії суспільного договору, яка по суті є безпековою (захисною) теорією. Оскільки, згідно з нею людини свідомо будували суспільство *(поступалися свободою на користь держави для забезпечення особистих прав)*, укладали союз для охорони власних інтересів.

І 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 людина – 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***.

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 безпеці, 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.

Список використаних джерел:

1. Конституція України від 28 червня 1996 року // Відом. Верховної Ради України. − 1996. – № 30. – Ст. 141.

2. . Довгань О.Д. Дотримання інформаційних прав і свобод громадян: правові норми /О.Д. Довгань/ Проблеми захисту прав людини в інформаційному суспільстві: Матеріали науково-практичної конференції, 1 квітня 2016. – К.: НДІІП НАПрН України, Національний інститут стратегічних досліджень, Секретаріат уповноваженого Верховної Ради України з прав людини, НТУУ «КПІ», 2016. – С.21-23.

3. Кант. И. Из лекций по этике /И.Кант// Этическая мысль: науч.-публицист.чтения. – М., 1988. – С.299-333.

4. Тихий В.П. Безпека людини: поняття, правове забезпечення, значення, види / В. П. Тихий // Вісник Національної академії правових наук України. – 2016. – № 2. – С. 31-46. – Режим доступу: http://nbuv.gov.ua/UJRN/ vapny_2016_2_5

5. https://uk.wikipedia.org/wiki/Декларація незалежності

6.https://uk.wikisource.org/wiki/Декларація_ прав_людини_і_громадянина

7.https://www.ccu.gov.ua/ Голова КСУ Станіслав Шевчук закликав керівників парламентських фракцій та груп до діалогу на користь захисту прав людини.

----------***----------

Мисливий В. А., *д. ю. н., професор, професор кафедри публічного права ФСП КПІ ім. Ігоря Сікорського*

КРИМІНАЛЬНО–ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ГАРАНТІЯ КОНСТИТУЦІЙНИХ ПРАВ І СВОБОД ЛЮДИНИ

Конституція України (ст. 17) проголошує захист інформаційної безпеки України найважливішою функцією держави, гарантією якої є кримінально-правова охорона суспільних відносин в інформаційній сфері.

Проте, звернення до витоків вітчизняного кримінального законодавства, перших кримінальних кодексів 1922 і 1927 років, показує, що в них термін «інформація» взагалі не використовувався. Наступний Кримінальний кодекс УРСР 1960 року (далі – КК) також не містив його понад 30 років. Уперше він з'явився у нормах, пов'язаних з паростками ринкових відносин, у таких складах злочинів, як «Шахрайство з фінансовими ресурсами» (ст. 145^5 КК) у контексті надання суб'єктом злочину завідомо неправдивої *інформації* державним органам, банкам або іншим кредиторам з метою одержання субсидій, субвенцій, дотацій, кредитів чи пільг щодо податків та «Порушення порядку випуску (емісії) та обігу цінних паперів» (ч. 2 ст. 148^8 КК) як внесення особою в документи, які подаються для реєстрації емісії цінних паперів, завідомо

недостовірної *інформації*, а так само затвердження таких документів. Нарешті, серйозним кроком у кримінальному законі, спрямованим на охорону інформаційних відносин, була ст. 198[1] КК «Порушення роботи автоматизованих систем» про відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації. На той час кодекс вживав термін «інформація» лише у 6 випадках.

Наступним етапом стало прийняття Кримінального кодексу України 2001 року, який, нарешті, передбачив елементи системної охорони відносин у сфері безпеки інформації в окремому Розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», який містив 3 норми: «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» (ст. 361 КК); «Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем» (ст. 362 КК); «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем» (ст. 363 КК). Безпека комп'ютерної інформації була визнана родовим об'єктом цих злочинів, а поняття інформації – усталеним в кримінальному законі.

Аналіз чинного кримінального законодавства показує, що суспільні відносини у цій сфері охороняються значним числом норм. Зокрема, серед злочинів проти основ національної безпеки України – це ст. 109 «Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади», яка забороняє публічні заклики щодо вчинення таких дій, розповсюдження матеріалів із закликами до їх вчинення, або з використанням ЗМІ. Інформаційна безпека є об'єктом державної зради у формі шпигунства (ст. 111 КК).

У Розділі V Особливої частини КК охорону виборчих прав громадян від умисного подання до органу ведення Державного реєстру виборців неправдивих відомостей та інші несанкціоновані дії з інформацією, що міститься у вказаному реєстрі, передбачає ст. 158 КК. Злочином вважається порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, а також ці дії з використанням засобів, призначених для негласного зняття інформації (ст. 163 КК). Посилення охорони прав і свобод людини набула недоторканність приватного життя з огляду на відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації (ст. 182 КК). Законом карається

перешкоджання законній професійній діяльності журналістів у сфері інформації (ст. 171 КК), а також посягання на законні інтереси громадян у сфері інтелектуальної власності, передбачені ст. 176 КК, яка переслідує порушення авторського права і суміжних прав щодо творчого інформаційного продукту.

У сфері господарської діяльності, пов'язаній з незаконним поводженням з інформацією, визнано незаконними: дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима та обладнанням для їх виготовлення (ст. 200 КК), контрабанду спеціальних технічних засобів негласного отримання інформації (ст. 201 КК), фінансування тероризму через неподання (несвоєчасне подання) або подання недостовірної інформації про фінансові операції, якщо це заподіяло істотну шкоду правам, свободам або інтересам громадян (ст. 209^1 КК).

Потреби захисту законних прав і інтересів громадян-вкладників банків обумовили криміналізацію таких діянь, як порушення порядку ведення бази даних про вкладників або порядку формування звітності, у тому числі внесення до бази даних або до Фонду гарантування вкладів фізичних осіб завідомо неправдивих відомостей у звітність про вкладників, а також дії, що унеможливлюють ідентифікацію вкладника (ст. 220^1 КК), злочинними є дії, пов'язані з фальсифікацією фінансових документів і звітності фінансової організації, приховування неплатоспроможності фінустанови (ст. 220^2 КК).

Інтереси громадян охороняє ст. 222 «Шахрайство з фінансовими ресурсами», тобто надання завідомо неправдивої інформації органам влади, банкам або іншим кредиторам з метою одержання субсидій, субвенцій тощо, а також норми, пов'язані із незаконним використанням та приховуванням інсайдерської інформації на ринку цінних паперів (ст. 232^1, 232^2 КК).

Деякі норми, пов'язані з інформацією, охороняють права і свободи людини у сфері довкілля, зокрема приховування або перекручення відомостей про екологічний стан або захворюваність населення, що пов'язано із забрудненням довкілля, харчових продуктів та є небезпечним для життя і здоров'я людини (ст. 238 КК), а також забруднення моря, якщо це створює небезпеку для життя та здоров'я людей (ст. 243 КК).

Серед злочинів проти громадської безпеки можна відзначити заздалегідь не обіцяне сприяння учасникам злочинних організацій та укриття їх злочинної діяльності шляхом надання інформації (ст. 256 КК), а також ст. 258^2 «Публічні заклики до вчинення терористичного акту» та деякі інші діяння.

У Розділі XIV «Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації» склади злочинів у сфері інформації сформульовані у ст. 329 «Втрата документів, що містять державну таємницю», яка передбачає втрату документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, та у

ст. 330 КК, яка карає за передачу чи збирання з метою передачі іноземним суб'єктам відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

Норми, спрямовані на охорону життя, здоров'я і власності журналістів у зв'язку з їх професійною діяльністю, пов'язані зі створенням чи використанням інформації через друковані ЗМІ, телерадіоорганізації, інформаційні агентства, мережу Інтернет (ст. 345^1 КК), передбачено у Розділі XV «Злочини проти авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян та злочини проти журналістів», що також містять відповідальність за надання народному депутату України, депутату місцевої ради, комітетам чи тимчасовим слідчим комісіям Верховної Ради України недостовірної інформації (ст. 351 КК) або Рахунковій палаті чи її членам (ст. 351^1 КК).

Важливою особливістю ст. 358 КК в інформаційному аспекті є визначення офіційного документа як такого, що містить зафіксовану на будь-яких матеріальних носіях інформацію, яка підтверджує чи посвідчує певні події, явища або факти, які спричинили чи здатні спричинити наслідки правового характеру.

Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» відчув суттєвих трансформацій, пов'язаних з імплементацією положень Конвенції про кіберзлочинність (2001 р.), і обіймає на сьогодні 6 норм, зокрема: **«**Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» (ст. 361 КК), що передбачає виток, втрату, підробку, блокування інформації, спотворення процесу її обробки або порушення порядку її маршрутизації; «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» (ст. 361^2 КК); «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», в якій йдеться про несанкціоновану зміну, знищення, блокування, перехоплення або копіювання інформації, якщо це призвело до її витоку, вчинені такою особою (ст. 362 КК) та деякі інші.

Особливого значення інформація набуває у протидії корупції, що у Розділі XVII «Злочини у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг» відображає ст. 366^1 «Декларування

недостовірної інформації», яка передбачає відповідальність за подання суб'єктом декларування завідомо недостовірних відомостей у декларації або умисне неподання суб'єктом декларування зазначеної декларації. Захисту прав і свобод людини в системі правосуддя слугує протидія незаконному втручанню в роботу автоматизованої системи документообігу суду, що передбачено ст. 376^1 КК.

Обсяг тез не дозволяє здійснити розгляд усіх складів злочинів, що забезпечують охорону прав і свобод громадян в інформаційній сфері, проте викладене дає підстави для таких висновків: суспільні відносини у цій сфері вимагають її кримінально-правової охорони, зокрема щодо забезпечення прав і свобод людини; більшість розділів Особливої частини КК містить норми, які охороняють права і свободи громадян у різних сегментах інформаційної сфери; окремі норми регулюють указані відносини в межах різних родових об'єктів злочинів; наявна правова матерія, яку становлять наведені й інші норми КК, пов'язані з інформаційною сферою, є достатньою для переходу кількості в якість – передбачення в КК України окремого розділу Особливої частини «Злочини у сфері інформаційної безпеки».

Зазначене виокремлення норм щодо інформаційної безпеки сприятиме теоретико-прикладному дослідженню і підвищенню ефективності кримінально-правової охорони прав і свобод громадян в інформаційній сфері.

----------***----------

Ожеван М. А., *д.ф.н., професор,*
головний науковий співробітник
Національного інституту стратегічних
досліджень при Президентові України.

PER ASPERA – AD ASTRA: БЕЗПЕКОВІ ВИКЛИКИ СТАНОВЛЕННЯ УКРАЇНСЬКОЇ СИСТЕМИ eHEALTH

Закон України *«Про державні фінансові гарантії медичного обслуговування населення»* (набув чинності 30 січня 2018 р.; підписаний Президентом 19 жовтня 2017 року) вперше в історії незалежної України формулює на юридичному рівні поняття «електронної системи охорони здоров'я». Ст. 11 цього закону проголошує принципові положення «електронної системи» у частині реєстрації даних про пацієнтів.

З посиланням на Закон України *«Про захист персональних даних»* прописуються умови надання доступу до Е-бази даних про пацієнта. Вказується на необхідність отримання згоди такого пацієнта (його законного представника) у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. Без згоди доступ до інформації про пацієнта можливий лише у трьох у

випадках: (а) наявності ознак прямої загрози життю пацієнта; (б) неможливості отримання згоди такого пацієнта чи його законних представників (до часу, коли отримання згоди стане можливим); (в) за рішенням суду [1].

«Електронна система охорони здоров'я» в її українській версії явно підпорядкована меті централізації фінансів в особі новостворюваної агенції Національної служби здоров'я України (НСЗУ). Водночас центральна влада в особі МОЗ явно має намір перекласти на органи місцевого самоврядування утримання інфраструктури медичних установ включно з придбанням комп'ютерів та підтримкою комп'ютерних мереж (з розрахунку на одну поліклініку знадобиться сума біля 3 млн. грн.).

Реформа системи охорони здоров'я, безперечно, належить до найскладніших серед тих, яких потребує Україна й супроводжується інформаційною війною, учасники якої не дуже доброчесно добирають аргументи. Йдеться передусім про подолання інерційності мислення, у вимірах якого «лікує лікарняне ліжко», а не «смартфон» й важливим є контакт з лікарем у «фізичному тілі», а не віртуальним лікарем з Інтернету.

Криза медичної допомоги не є суто українським феноменом. Водночас важко очікувати позитивів, орієнтуючись виключно на впровадження у медицину новітніх інформаційних технологій. У США зокрема такі технології впроваджуються в медицину вже більше 60-ти років. Інтернетизація системи охорони здоров'я (як і будь-якої іншої системи) має виражену антикорупційну складову, бо дозволяє за рахунок збільшення «прозорості» більш ефективно контролювати фінансові та інші потоки. Не дивно що подібні тренди просуваються переважно державними чиновниками «від медицини». Але за відгуками американських фахівців вони охопили тільки третину лікарняних закладів, що зазвичай пояснюють приватним характером американської системи охорони здоров'я [2]. Таке гальмування має просте пояснення: для благополучних американців та європейців набагато вагомішими від питань фінансових є питання таємниці персональних даних. За компанії Trend Micro Incorporated лише 2015 р. було викрадено 113,2 млн. медичних записів вартість яких на чорному ринку може становити близько $500 тис., бо саме стільки коштує база електронних медичних карток. Лише в США кібератаки на медичні установи щорічно обходяться системі охорони здоров'я у $6 млрд., а фінансові втрати від витоків даних у середньому становлять $2,1 млн. Зловмисники використовують викрадені дані для нелегального придбання ліків, податкових махінацій та інших протиправних дій [3].

Разом з тим, важко заперечувати, що Інтернет – потужне джерело знань для багатьох людей про здоров'я й хвороби, медичну допомогу та її доступність чи недоступність, способи лікування чи самолікування тощо. У розвинених країнах типу США чи країн ЄС біля половини нас ведення користується

подібною онлайновою інформацією. Проте, окрім доступу до самого Інтернету, існує щонайменше два обмежувальні чинники ефективного застосування Інтернету в подібних цілях: електронно-онлайнова та медична грамотність [4].

eHealth – це використання електронних ресурсів для збереження та передачі даних, які стосується здоров'я пацієнтів, а також діагностичних, лікувальних та інших ресурсів охорони здоров'я (лікарень та інших лікарняних закладів, лікарів, медсестер, відповідного обладнання, ліків тощо). eHealth тлумачать також як використання Інтернету та різноманітних «додатків» (аплікацій) до нього з метою більш оптимального використання ресурсів системи охорони здоров'я й зокрема її: (а) якості; (б) ефективності; (в) доступності). Розробники української версії eHealth розуміють її суто технологічно як «інформаційно-телекомунікаційну систему, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією в електронному вигляді, до складу якої входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін даними через відкритий програмний інтерфейс (Application Programming Interface, – API) [5].

Спільними зусиллями МОЗ та учасників «публічної ініціативи» було підготовлено «принципи взаємодії» та опис Мінімального життєздатного продукту (MVP). eHealth впроваджувалася в чотири етапи в 2017-2018 рр. 25.11.2016. було підписано меморандум про співпрацю між МОЗ й учасниками «публічної ініціативи». 06.04.2017 відбулась офіційна презентація демонстраційної версії перших складових eHealth у рамках MVP, щоби лікарі та пацієнти зрозуміли логіку перших електронних сервісів для реформування первинної ланки на засадах (а) реєстрації закладів та лікарів; (б) укладання декларацій між пацієнтами та лікарями. На початку 2018 року MVP було передано МОЗ й розпочалося його впровадження. 01.04.2018 стартував процес укладання декларацій, хоча його темпи значно повільніші від очікуваних. Підтримку та консультації Проектному офісу надавало Державне агентство з питань електронного урядування. Представники громадських організацій, які утворили проектний офіс – це передусім Дмитро Шерембей, який представляв Всеукраїнську мережу ЛЖВ («Люди які живуть з ВІЛ/СНІД»; «People Living with HIV/AIDS»), та Ярослав Юрчишин з Transparency International Україна, що відповідав за розробку та тестування елементів системи, її юридичний супровід, комунікацію, технічну підтримку. Мережа «ЛЖВ» має великий досвід залучення та розподілу ресурсів, співпраці з донорами, ведення фінансової та публічної звітності, пацієнтського контролю за роботою офісу, організації аудиту міжнародними компаніями «великої четвірки» (не менше двох разів на рік).

Проте офіс розробників лише адмініструватиме систему, але володіти нею і відповідати за її цілісність та безпеку буде МОЗ, аби система eHealth «відповідала найвищим стандартам безпеки та потребам усіх її користувачів: закладів, лікарів, пацієнтів та держави». МОЗ, у свою чергу, часто посилається на відповідальність органів місцевого самоврядування. Усе це неважко розцінювати як бажання зняти з себе відповідальність заради «вищого блага» не може не насторожувати. оскільки йдеться про персональні дані пацієнтів, якими не тільки можуть зловживати аморальні люди, але які може використовувати різноманітний криміналітет.

Особливо такі побоювання в Україні посилилися після ухвалення 17.05.2018 Верховною Радою України закону *«Про застосування трансплантації анатомічних матеріалів людині»,* який остаточно легалізував пересадку трупних органів. Законом визначено, що кожна повнолітня дієздатна особа має право надати письмову згоду або незгоду на вилучення анатомічних матеріалів з її тіла для трансплантації та/або виготовлення біоімплантатів після визначення її стану як незворотна смерть (смерть мозку або біологічна смерть). Кожна повнолітня дієздатна особа має право у будь-який час подати письмову заяву про відкликання своєї письмової згоди або незгоди на посмертне донорство, надати нову письмову згоду або незгоду на посмертне донорство. Ця згода чи незгода заносяться до Єдиної державної інформаційної системи трансплантації [6].

За даними проведеного у 2013 р. дослідження у світі тільки у вказаному році було здійснено 118 127 пересадок органів, що склало лише 10% від потреби. «Waiting lists» в країнах ЄС передбачають не менше 3-5 років очікування на орган, придатний для даного реципієнта за своїми антигенними характеристиками. Біля третини очікуючих вмирають так і не дочекавшись «свого органу». Водночас 5-10% пересаджуваних нирок походять від жертв нелегального трафику органів [7]. Неважко здогадатися, якими кримінальними наслідками може обернутися існування в зубожілій Україні легальної чи нелегальної електронної бази антигенних імунних характеристик пацієнтів, яку неважко буде пристосувати до потреб кримінальної чи напівкримінальної медицини.

У тій частині, яка стосується ролі eHealth у поліпшенні ефективності охорони здоров’я інноваційну медичну дилему часто формулюють як *«смартфони проти лікарняних ліжкомісць»*, маючи вочевидь на увазі, що, чим більше в даній країні буде розвинений широкосмуговий Інтернет з підключеними до нього мобільними пристроями (смарфонами), тим менше у цій країні знадобиться ліжкомісць. Традиційно число ліжко-місць із розрахунку на тисячу населення вважалося показником екстенсивного розвитку медицини. Зокрема в Україні таких ліжок було 9-ть (станом на 2012 рік), тоді як в інших

країнах воно помітно не відрізнялося: РФ – 9,7; в Білорусі – 11, в Японії – 13,7 й т.п. Парадоксальним є той факт, що, хоча у багатьох слаборозвинених країнах цей показник є набагато нижчим, але і в багатьох високорозвинених країнах він також є порівняно низьким (США – 2,9; Сінгапур – 2 й т.п.) [8]. У цілому на 7,4 млрд. світової популяції (дані на серпень 2016 р.) припадало близько 200 млн. лікарняних ліжок, які мали би «виліковувати» людей. 436,4 тис. ліжок перебуває в Україні у 2537 медичних закладах, підпорядкованих МОЗ [9]. Щоправда,серйозні нарікання викликає інфраструктура первинної медицини. Планується, що впродовж 2018-2019 рр. буде створено низку сучасних амбулаторій, у яких передбачено мережу телемедицини, яку Україна отримає від канадських партнерів.

Іноземну допомогу слід звичайно вітати. Але вона не вирішить усіх проблем. Адже насичення населення України комп'ютерами й зокрема – смартфонами є надто низьким, щоб ставити всерйоз питання про «перехід кількості в якість».

Станом на серпень 2016 р., у світі існував 1 млрд. мобільних пристроїв типу смартфон або айфон, і кожен другий з цих пристроїв (близько 500 млн.) був цілковито придатними для розміщення в них мобільних медичних ресурсів (Mobile applications – Apps). Очікується, що в 2018 р. таких смартфонів і «таблетів» у масштабах планети налічуватиметься вже 3,4 млрд. і всі вони будуть придатними для завантаження медичних аплікацій для потреб як професіоналів у сфері медицини, так і споживачів медичних продуктів та пацієнтів [10].

Україна явно вибивається із загальносвітового графіка за обома показниками: (а) бродбенду; (б) пенетрації смартфонів. За показником передплатників фіксованого Інтернету широкої смуги – Україна на 25-тій позиції в світі (РФ – 7), а мобільного версії цього Інтернету – 59 (РФ – 6) [11]. В Україні показник пенетрації смартфонів склав в 2017 р. лише 27% (для порівняння: Півд. Корея – 88%; США – 72%; РФ – 45%) [12].

Розробники української системи eHealth наголошують на поліпшенні доступності медичної допомоги, зручності контактування пацієнта з лікарем тощо (на прийом до лікаря можна записатися, не виходячи з дому тощо), але явно відволікаються від моментів, пов'язаних з якістю й безпекою медичної допомоги.

Водночас центральна проблема eHealth пов'язана з електронними правами, обов'язками та безпекою пацієнтів та лікарів, їхньою взаємною відповідальністю за результати власної діяльності або бездіяльності. Ці питання в Україні могла би вирішити тільки багаторівнева страхова медицина, яка поки що із різних причин не запроваджується.

Успадкована від радянських часів бюджетна медицина навряд чи може бути реформованою за посередництвом ще однієї бюджетної установи, – НСЗУ, яка поєднала в собі рольові функції розпорядника коштів, контролера якості і «чистильника» мережі медичних установ у процесі реалізації красивого мему – «гроші ходять за пацієнтом».

Список використаних джерел:

1. Закон України. Про державні фінансові гарантії медичного обслуговування населення (Відомості Верховної Ради (ВВР), 2018, № 5, ст.31).
2. SWOT Analysis on ICT Theme e-Health. [Електронний ресурс]. – Режим доступу: http://www.eseeinitiative.org/file/2017/08/eSEE_Agenda_ Plus _signed.pdf
3. Колісник Тетяна. Чи врятує вітчизняну медицину e-Health? /Тетяна Колісник / Ваше здоров'я. 30.06.2017. [Електронний ресурс]. – Режим доступу: http://www.vz.kiev.ua/chy-vryatuye-vitchyznyanu-medytsynu-e-health/
4. EHealth // Вікіпедія. [Електронний ресурс]. – Режим доступу: https:// uk. wikipedia.org/wiki/EHealth
5. Robinson, Christie. Graham, Joy. Perceived Internet health literacy of HIV–positive people through the provision of a computer and Internet health education intervention / Christie Robinson & Joy Graham // Health Information and Libraries Journal. 2010. Vol. 27, pp.295–303.
6. Проект Закону про внесення змін до деяких законодавчих актів України щодо охорони здоров'я та трансплантації органів та інших анатомічних матеріалів людині. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/ zweb2/webproc4_1?pf3511=56231
7. ORGANized Crime: Trafficking for Organ Removal. [Електронний ресурс]. – Режим доступу: http://iomx.org/organized-crime-trafficking-for-organ-removal/
8. Hospital bed density 2018 Country Ranks, by Rank // Countries of the world. [Електронний ресурс]. Режим доступу: https://photius.com/rankings/ 2018/ population/hospital_bed_density_2018_0.html
9. Охорона здоров'я в Україні // Вікіпедія. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki
10. Mobile Medical Applications. [Електронний ресурс]. – Режим доступу : https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedical Applications/ucm255978.htm
11. List of countries by number of broadband Internet subscriptionshttps… using data compiled by the International Telecommunication Union // Wikipedia. [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/List_of_ countries _by _smartphone_penetration. en.wikipedia.org/wiki/List_of_countries _by_number_of_ broadband_Internet_subscriptions.
12. List of countries by smartphone penetration // Wikipedia [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/List_of_ countries_by _smartphone_ penetration

----------***----------

***Фурашев В.М.**, к.т.н., с.н.с, директор Центру інформаційного права та правових питань інформаційних технологій КПІ ім. Ігоря Сікорського.*

ІНФОРМАЦІЙНЕ ПРАВО – ОДИН З ГОЛОВНИХ ЧИННИКІВ ЗАБЕЗПЕЧЕННЯ ПРАВ, СВОБОДИ І БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Є два основних показника рівня демократичності держави – рівень участі громадянина в управлінні державою та рівня гарантованих державою прав, свободи і безпеки людини.

З урахуванням особливостей сучасного етапу розвитку світового суспільства, рівень демократичності в держави, у багатьому, визначається рівнем гарантованих державою прав, свободи і безпеки людини саме в інформаційній сфері.

Державна гарантованість забезпечення прав, свободи і безпеки людини в інформаційної сфері забезпечується Конституцією України та системою правовідносин, які встановлюються у розвиток та конкретизацію її положень, та забезпечення їх неухільного дотримання.

Але необхідно постійно мати на увазі, що безпеки без визначеного рівня обмеження прав і свободи людини не буває і тому ми дуже добре сприймаємо будь-які положення, які касаються зміцнення і розширення наших прав і досить негативно - положення, що обмежують, на наш погляд, ці права. Особливо, болісно сприймаються положення, які стосуються правопорушень в інформаційній сфері.

Як було вже зазнчено автором[6]:

Інформаційне право – система соціальних загальнообов`язкових норм поводження з інформацією на всіх стадіях її життєвого циклу, дотримання і виконання яких забезпечується державою, предметом якого є повна сукупність інформаційних та інформаційно-інфраструктурних суспільних відносин, які виникають під час забезпечення обороту інформації.

Функція інформаційного права – правове регулювання суспільних відносин, пов`язаних з оборотом інформації, незалежно від її виду та типу, забезпеченням цього обороту незалежно від виду, технологій та засобів, які при цьому використовуються.

[6] Інформаційне право та право інтелектуальної власності – взаємозв`язок / Фурашев В.М. // Створення, охорона та захист об`єктів інновацій : матеріали наук. – практ. Семінару, м. Київ, 26 квіт. 2018 р. / Упорядн. : В.М. Фурашев, С.Ю. Петряєв. – Київ : КПІ ім Ігоря Сікорсвького, Вид-во «Політехника, 2018. – 84 с. С. 19 – 21.

Основні цілі інформаційного права – забезпечення і захист конституційних прав і свобод людини в інформаційній сфері; забезпечення інформаційної безпеки особистості, суспільства і держави; формування правових основ для сприяння максимальному розвитку інформаційного суспільства та інформаційної сфери та, цілком природно, гармонізація з міжнародним правом в інформаційній сфері.

Таким чином питання:

– встановлення видів інформації та інформаційної діяльності *(створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації)*;

– встановлення режиму доступу до інформації;

– формування базового термінологічного апарату в інформаційної сфері та сферах охорони і захисту інформації, інформаційної безпеки людини, суспільства, держави;

– встановлення соціальних загальнообов`язкових норм поводження з інформацією на всіх стадіях її життєвого циклу, дотримання і виконання яких забезпечується державою;

– інші питання пов`язані з оборотом інформації та інформаційною сферою взагалі є функціональним обов`язком інформаційного права.

Коли говоримо про інформаційне право як одного з головних чинників забезпечення прав, свободи і безпеки людини в інформаційної сфері, необхідно мати на увазі наступне:

– інформаційна безпека, з одного боку, одночасно є невід'ємною складовою національної безпеки та інформаційного права, а з іншого – самостійним напрямом в науці та техніці, а відповідно і в системі права;

– кібербезпека, з одного боку, є невід'ємною складовою інформаційного права, а з іншого – самостійним напрямом в науці та техніці, а відповідно і в системі права;

– саме питання забезпечення інформаційної безпеки людини, суспільства та держави визначають характер та спрямованість правовідносин в інформаційнійсфері, а також юридичної відповідальності за їх порушення.

На основі викладеного можна зробити наступні ***висновки:***

1. З урахуванням досягнень у науково-технічній сфері, а також тенденцій подальшого її розвитку, важко заперчувати одну з провідних ролей та місце інформаційного права в системі забезпечення прав, свободи і безпеки людини в інформаційної сфері.

2. Ефективність системі забезпечення прав, свободи і безпеки людини в інформаційної сфері, у багатьому, залежить від структурірованості (упорядкованості), чіткості (однозначності розуміння), актуальності та

правозастосування положень інформаційного права, тобто – від ефективності інформаційного права.

3. Не можна стверджувати, що сучасний стан національного законодавства в інформаційній сфері незадовільний, але можна стверджувати, що він відстає від темпів та спрямованості науково-технічного прогресу, якій має дуже суттєвий вплив на формування нових суспільних відносин.

4. З метою підвищення ефективності загальної системі забезпечення прав, свободи і безпеки людини в інформаційної сфері необхідно дуже суттєво переглянути погляди на її правову складову:

а) інформаційне право повінно стати «випереджаючим», а не «констатуючим». Мова іде про те, що вже на етапах дослідної та дослідно-випробувальної роботи по створенню нових зразків «продукції» науково-технічного прогресу розглядати ступень їх впливу на існуючі суспільні відносини. У разі виявлення необхідності їх суттєвої трансформації або формування нових, одразу необхідно починати формування та встановлювання відповідних правовідносини, без вичікування широкомасштабного впровадження цієї «продукції». Це, з одного боку, дозволить заздалегідь підготувати суспільство до впровадження нової «продукції», а, по-друге, значно прискорити науково-технічний прогрес за рахунок скорочення циклу впровадження досягнутих результатів, підвищить конкурентоспроможність вітчизняної науки і техніки. Правова наука повинна працювати в одному ритмі з іншими галузями науки, а законотворець – в одному ритмі з правовою наукою;

б) здійснити первинне упорядкування діючого законодавства в інформаційної сфері. В першу чергу це стосується питань актуальності, повноти та однозначного тлумачення положень тих чі інших законів України, які встановлюють правовідносини в інформаційній сфері. Особливу увагу неохідно зосередити на наведенні ладу у понятіно-категоріальному апарат;

в) розробити, свого роду, «конституцію» базових термінів та їх визначень, основних положень правовідносин в інформаційної сфері, поклав в основу, наприклад, закони України «Про інформацію» *(інформаційні суспільні відносини)* та «Про телекомунікацію» *(інформаційно-інфраструктурні суспільні відносини)* як початковий етап цілеспрямованої роботи по систематизації інформаційного права.

5. Суттєвою проблемою становлення та розвитку інформаційного права як окремої галузі права, на погляд автора, є недостатнє усвідомлення на всіх рівнях законотворчого процесу та системи державного управління, його ролі та місця в системі права в умовах все зростаючого значення інформації у забезпеченні життєдіяльності сучасного суспільства та його розвитку.

Скоріше за всього, саме цим можна пояснити багаторічні «блокування» виконання чисельних рішень Президента України, Ради національної безпеки і

оборони України, Кабінету Міністрів України щодо упорядкування, систематизації системи законодавства в інформаційної сфері.

Законодавча база в інформаційній сфері стрімко розширюються, але цей процес відбувається фрагментарно, хаотично, фактично без урахування тих трансформаційних процесів, які відбуваються у середовищі інформаційних та інформаційно-інфраструктурних суспільних відносин.

Крім того ситуація, яка склалася у сфері інформаційного права, є основою появи чисельних питань майбутніх правознавців, щодо практичного правозастосування положень інформаційного права, працевлаштування та спектру практичних сфер застосування цих знань.

----------***----------

Архипова Є. О., *к.ф.н., доцент кафедри теорії та практики управління КПІ ім. Ігоря Сікорського.*

ЛЮДИНА (НЕ)ІНФОРМАЦІЙНА ЯК ПРОДУКТ СУЧАСНОГО СУСПІЛЬСТВА

Успіх сучасної людини багато в чому залежить від того, наскільки добре вона здатна взаємодіяти з інформацією, координувати інформаційні потоки, отримувати необхідну інформацію та дані, трансформувати їх в знання, а потім використовувати для свого подальшого розвитку. Розвиток інформаційного суспільства та суспільства знань, як зазначає велика кількість дослідників новітніх соціальних трансформацій, починаючи з Д. Бела, Й. Масуди, Е. Тофлера, В. Іноземцева та інших, має призвести до формування людини нового типу, основними об’єктами і результатами діяльності якої є інформація та знання, а провідні цінності пов’язані із інтелектуальною діяльністю. Провідні характеристики такої людини ми можемо об’єднати під терміном «людина інформаційна». Вважатимемо, що людині інформаційній притаманна постійна включеність в інформаційні процеси та системи різних рівнів; активне використання сучасних ІКТ для забезпечення професійних та особистих, в тому числі побутових, комунікативних, розважальних, пізнавальних потреб; споживання та/або створення чисельних інформаційних продуктів та послуг.

Сучасні ІКТ, в першу чергу інтернет, відкривають нові можливості для комунікації, організації бізнесу, проведення дозвілля, виконання робочих і побутових завдань, самореалізації, освіти і багато чого іншого. Наше суспільство неможливо уявити без інтернету, який став його своєрідною візитівкою. «Запитати у Гугла», «знайти в інтернеті», «інтернет знає все» – цими фразами сьогодні нікого не здивуєш. Інтернет став нашим незамінним

помічником, нашим другом, з яким ми «спілкуємося» часом набагато частіше, ніж з реальними друзями. Інтернет є практично безмежним сховищем інформації, інструментом, який істотно спрощує доступ до світових інформаційних ресурсів. Здавалося б: повна свобода вибору, адже в інтернеті інформація представлена на будь-який смак і для будь-яких цілей.

Однак слід зазначити, що свобода, яка нібито надається користувачам інтернету в питанні вибору інформації, яка ними споживається, та й взагалі способу використання інтернету, має певні обмеження. У даній роботі ми навмисно опускаємо такі негативні прояви інтернету, як вірусні атаки, виникнення залежності у інтернет-користувачів, інтернет-шахрайство, здійснювані через мережу кібернетичні атаки, сайти, що поширюють протизаконну продукцію і послуги тощо. Зупинимося лише на можливості адекватного сприйняття інформації, розміщеної в інтернет-просторі.

В інтернеті ми можемо знайти інформацію різних видів, форм, походження і призначення: ту, яка дозволяє нам якісніше виконати свою роботу і ту, що дає можливість відпочити від роботи; ту, що можна подивитися, послухати або почитати; яка змушує думати або яка дає можливість розслабитися; яка дається нам в готовому вигляді, яку можна видозмінювати або яку ми створюємо самостійно; що надходить із офіційних джерел або неофіційних; відображає факти, містить обґрунтовані гіпотези або голі припущення і домисли ... Активне використання ІКТ практично у всіх сферах діяльності людини призводить до накопичення надмірної кількості інформації, а надлишок інформації, за влучним виразом С. Даниленка [3, 39], вбиває інформацію, так само як і надмірна кількість комунікації вбиває комунікацію. В цьому ж контексті можна навести цікаву метафору професора Університету Кіото Terufumi Ohno, який причинами інтелектуального застою людей в сучасному суспільстві називає «болото гіпертрофованої інформації» та надмірну спеціалізацію дослідницьких дисциплін [1, 33].

Велику роль у посиленні інтелектуального застою людей інформаційної епохи слід відвести багатогранному феномену інформаційної нерівності, зокрема нерівності різних суспільних верств у можливості створювати і масово транслювати інформацію. Той, хто контролює інформаційні потоки, здатний закладати в свідомості користувачів певні інформаційні вподобання і смаки, задавати рамки інформаційного сприйняття, формувати світогляд і таким чином направляти поведінку людей в бажане русло [2].

Ця закономірність успішно працює як в традиційних ЗМІ, так і в сучасних інформаційно-комунікативних каналах. Відзначимо, що соціальні мережі є більш дієвим інструментом впливу на свідомість молодих людей, ніж традиційні засоби масової інформації. Просунуті інтернет-користувачі вже давно засвоїли, що олігархи через підвладні ЗМІ транслюють вигідну їм

інформацію. Повідомлення, що надходять від «друзів», мають більший кредит довіри ніж інформація «з телевізора», оскільки нею діляться звичайні користувачі інтернету, у яких теоретично відсутня особиста зацікавленість. Чим більше число користувачів репостять, «лайкають» повідомлення, тим менше бажання її перевіряти і критично переосмислювати, тим сильніше підсвідома впевненість в об'єктивності поширюваної інформації – загалом, досить сумнівна впевненість, враховуючи кількість фейковий акаунтів, проплачених інтернет-агітаторів і сумну звичку деяких користувачів «роздавати лайки» не особливо вчитуючись в повідомлення. Ось чому інтернет називають не тільки джерелом корисної інформації, але і, наприклад, гігантським інформаційним звалищем, що містить велику кількість недостовірної і неактуальної інформації.

Велика кількість інформації, з одного боку, надає широкі можливості вибору, але, з іншого боку, в рази ускладнює процедуру відбору та верифікації інформації. Клонована або злегка модифікована інформація, наприклад повідомлення-близнюки на новинних сайтах, витісняє альтернативні версії подій, пригод, тлумачень. Причому витіснення відбувається на декількох рівнях: спочатку з перших сторінок результатів пошукової системи, а в кінцевому підсумку, і зі свідомості окремих користувачів інтернету – звичайно, не всіх поголовно, але досить великої їх частини. Таке витіснення має цілком об'єктивні і закономірні причини: принципи роботи людського мозку (кількість інформації, яка може бути критично сприйнята, обмежена її загальною різноманітністю, тривалістю впливу та складністю) у поєднанні з інформаційною перевантаженістю, силою звички, впливом авторитетів і банальною лінню.

В інтернеті серйозні матеріали, що вимагають розумової напруги, перемежовуються такими, які «розм'якшують мізки» і перетворюють людину на ледачого споживача простенької інформації; чисті факти розбавляються фейками; новинні повідомлення з дотриманням всіх канонів журналістської етики конкурують з репортажами із завуальованим просуванням або відвертим нав'язуванням якоїсь ідеї чи товару. Як правило, виграють у цій конкурентній боротьбі не правдиві повідомлення, а такі, які є зрозумілішими та простішими, зовні несуперечливими, які звертаються до базових емоцій, потреб і бажань, а також такі, що не потребують побудови складних умовиводів.

Побудова умовиводів (особливо, із залученням додаткової інформації, яка безпосередньо не міститься в інформаційному повідомленні, що читається або переглядається), є складним розумовим процесом. Дуже мала кількість людей здатне тримати себе в постійній напрузі, піддаючи сумніву і перевіряючи десятки повідомлень щодня – це вимагає не тільки великого бажання, а й розвинених аналітичних здібностей, доброї пам'яті, наявності певних умінь і

навичок (від елементарної комп'ютерної грамотності до роботи з сучасними базами даних) і, що не менш важливо, – часу.

В умовах величезного розмаїття інформації та знань людина фізично не здатна розібратися у всьому. Навіть маючи бажання, вона може бути фахівцем (експертом) лише в деяких областях, в інших сферах їй доведеться покладатися на визнані авторитети, усталені думки, мигцем прочитану новину, на інтуїцію – на що завгодно, крім раціонального аналізу і самостійного критичного осмислення інформації. Така ситуація сприяє збільшенню використання сучасних ІКТ з метою маніпулювання, а принаймні деякі представники людей інформаційних вироджуються в людей неінформаційних: постійна включеність в інформаційні процеси та системи різних рівнів віднімає масу часу, але не несе жодної користі, використання сучасних ІКТ слугує не інтелектуальному розвитку людини, а зменшенню кількості розумових зусиль, необхідних для виконання певного завдання; споживання інформаційних продуктів значно переважає над їх створенням. Якість пропонованих інформаційних продуктів (в перерахунку на одиницю) знижується у відповідь на зниження вимог до інформації через неспроможність споживачів визначити її реальну цінність, натомість збільшується її загальна кількість, що додатково ускладнює пошук якісної, актуальної та потрібної споживачеві інформації.

Список використаних джерел:

1. Terufumi Ohno. Role of university museums from the view point of congnitive evolution of Homo sapiens. In: Program of Taiwan Association for Educational Communications and technology 2015 International Conference“Educational and Communication Technology Transforms the Future”, 2015, p.33.
2. Архипова Є.О. Цифрова нерівність як соціальна проблема інформаційного суспільства / Є.О. Архипова // Інформаційні технології та комп’ютерна інженерія: Міжнародний науково-технічний журнал. – 2008. – №2(12). – С. 34-37.
3. Даниленко С. Тенденції розвитку електронних ЗМІ / С. Даниленко // Нові медіа. – 2009. – С. 38–41.

----------***----------

Гордієнко С. Г., *д. ю. н, доцент, доцент кафедри інформаційного права та права інтелектуальної власності, ФСП КПІ ім. Ігоря Сікорського.*

ІНФОРМАЦІЯ – ІННОВАЦІЇ – ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ: ПРОБЛЕМИ ПРАКТИКИ В УКРАЇНІ

Як показує практика, останнім десятиліттям, зазначеній тематиці приділяється все більше і більше уваги, як науковцями, так і державним апаратом, однак результативність таких дій є негативною, про що свідчать парламентські слухання та наша попередня публікація.

Популяризація і розробка науковцями даної проблематики останнім десятиліттям натикається на стіну явного нерозуміння реальною державницькою практикою важливості внесення об'єктів інтелектуальної власності до нематеріальних активів[7].

В той час, коли наука розглядає питання інноваційної діяльності та інтелектуальної власності різносторонньо і достатньо активно, то практика вкрай специфічно – лише під певним політичним та соціальним кутом.

Цьому є просте пояснення – надто політично популярними є заклики до розвитку інноваційної діяльності в Україні, частиною якої є інтелектуальна власність, тобто якісно нове знання, яке належить Українській державі і виступає потужним, і майже невичерпним нематеріальним активом на відміну від застарілого виробництва епохи індустріалізації. З таким політичним гаслом є можливості досягти популярності серед електорату, однак це не працює на державу.

Тобто практика і наука йдуть своїми шляхами замість того, щоб єдиним виявом політичної волі поєднати зусилля.

Продемонструємо виказане вище.

Автором у 2007 році було зроблено висновок, що «вчасно та у повному обсязі заходи з інвентаризації інтелектуальної власності та постановки її на бухгалтерський облік в якості нематеріальних активів не виконано у жодному із міністерств і відомств. І фактично, інвентаризацію об'єктів інтелектуальної власності, створених за рахунок коштів державного бюджету, в масштабах держави можна вважати зірваною».

Наразі, від вказаного часу вже пройшло десять років, а що ж змінилося?

---

[7] *Гордієнко С.Г.* Чиновництво України та її інтелектуальна власність // Матеріали науково-практичної конференції / 17 травня 2016 р., м. Київ / Упорядн. Дорогих С.О.: – К. : НДІІП НАПрН України, Науково-дослідний інститут інтелектуальної власності Національної академії правових наук України, Навчально-науковий центр інформаційного права та правових питань інформаційних технологій ФСП НТУУ «КПІ», 2016. – 227 с., – С. 57 – 71.

Учасники неодноразових парламентських слухань звертають увагу на у цілому незадовільний стан розвитку інформаційної та інноваційної сфери держави, а також сфери інтелектуальної власності. За результатами знову лише надають рекомендації всім органам влади та управління[8].

Ряд Указів Президента України[9] та Розпоряджень Кабінету Міністрів України[10] також передбачають ряд завдань з реформування державної політики в зазначених сферах.

Однак, при цьому розвиток державної системи розвитку інноваційної діяльності і правової охорони інтелектуальної власності в Україні виливається на практиці у хаос.

Адже відсутність прийнятих на довгостроковий період стратегій соціально-економічного, науково-технологічного, інноваційного розвитку країни; незавершеність процесів перерозподілу власності; сформованість світового ринку високотехнологічних товарів і послуг та тяжіння в управлінні інноваційною сферою до галузевих засад є чинниками, які стримують інноваційний розвиток України.

На даний час існує потреба в перегляді й актуалізації змісту державної наукової політики, визначеності її доктринальних завдань та стратегічних напрямів, а також у створенні простих, зрозумілих науковцям, владі та суспільству механізмів забезпечення зростання ролі науки та її інноваційного потенціалу в соціально-економічному розвитку країни.

Реальною загрозою інноватиці є те, що в Україні в даний час **зупинено** реалізацію законів України «Про Загальнодержавну комплексну програму розвитку високих наукоємних технологій», «Про пріоритетні напрями інноваційної діяльності в Україні», «Про спеціальний режим інноваційної діяльності технологічних парків», **стримується реалізація** законів України «Про наукові парки» та «Про державне регулювання діяльності у сфері трансферу технологій» та Державної цільової економічної програми «Створення

---

[8] Постанова Верховної Ради України «Про Рекомендації парламентських слухань на тему: «Національна інноваційна система України: проблеми формування та реалізації» // Відомості Верховної Ради України (ВВР), 2007, № 46, ст. 525; Постанова Верховної Ради України «Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» від 3 липня 2014 року № 1565-VII; Постанова Верховної Ради України Про Рекомендації парламентських слухань на тему: «Про стан та законодавче забезпечення розвитку науки та науково-технічної сфери держави» від 11 лютого 2015 року № 182-VIII; Проект Рекомендацій комітетських слухань на тему: «Інтелектуальна власність в Україні. Стан та концептуальні засади розвитку» http://kno.rada.gov.ua/komosviti/control/uk/publish/article?art_id=61850&cat_id=44731 тощо.

[9] Указ Президента України № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»; Указ Президента України № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

[10] Розпорядження Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України»; Розпорядження Кабінету Міністрів України від 4 червня 2015 р. № 575-р «Про затвердження плану заходів з реалізації Концепції реформування державної політики в інноваційній сфері на 2015–2019 роки»

в Україні інноваційної інфраструктури на 2009-2013 роки». **Відсутній план заходів** із запровадження Концепції розвитку національної інноваційної системи. **Не виконуються положення Закону України** «Про наукову і науково-технічну діяльність» щодо бюджетного фінансування науки на рівні 1,7% ВВП, принципи базового і конкурсного забезпечення науки та заходи із створення сприятливих економічних умов діяльності наукових установ.

Як відзначалося нами раніше, парламентарі (за врахування, що Україна – це парламентсько-президентська республіка) **лише рекомендують, пропонують та доручають всій вертикалі влади** державних органів виконати якесь поінформування когось, а за рідкими випадками виконати конкретні заходи без їх наступного контролю.

Беззаперечним фактом являється те, що реалізація зазначених заходів практично не береться під контроль, лише за певними виключеннями!!!

Тобто зазначена сфера державної діяльності вимагає негайного реформування шляхом систематизації норм права з чіткого визначення компетенції державних органів та організацій з питань інноваційної та науково-технічної діяльностей і трансферу технологій.

Абсолютно все виказане вище неможливо реалізувати на практиці без політичної волі керівництва України, яке має забезпечити відповідне завданню фінансування та матеріальне забезпечення.

----------*----------**

Щириця Т. В., *доцент кафедри філософії КПІ ім. Ігоря Сікорського.*

ЦІННІСНІ ЗАСАДИ ПРАВ ЛЮДИНИ ЗА УМОВ ДЕЛІБЕРАТИВНОЇ ДЕМОКРАТІЇ

Актуальним правничо-політичним дослідженням в світі загалом і в Україні, зокрема, є одна з провідних категорій громадянського суспільства, а також сфери публічного дискурсу, а саме категорія деліберативної демократії. У своєму виступі я прагнутиму висвітлити насамперед деякі методологічні аспекти цієї проблеми, спираючись на дослідження філософів і соціологів, оскільки в сфері публічності як раз і формуються форми і змісти деліберативної демократії.

Залучається термін деліберативної демократії в останній третині 20-го століття. При цьому висвітлюються його древні корені, давньогрецькі, коли в містах-полісах на агорі відбувались дії, які сьогодні ми можемо назвати прообразами сучасних демократій. Прообрази саме через те, що участь в таких практиках брали, як відомо, тільки вільні громадяни міст-полісів. В цей же час

формуються нові вербальні практика, а саме діалоги і як літературний жанр (діалоги Платона) і як методологія отримання знання (діалогічний пошук істини Сократа).

Латинське дієслово delibero перекладається як зважувати, обговорювати, обмірковувати. Його семантика розширюється якщо використовувати такі словосполучення, як deliberandi spatium - час на роздуми, міркування, deliberare de summa rerum – міркувани про інтереси держави. Іншим значенням є запитувати, зокрема коли запитує оракул, а також приймати рішення, зокрема deliberatum mihi est – мною вирішено.

Отже, деліберативна демократія – демократія, яка залучає всі можливі форми обговорення актуальних проблем людського буття, від локальних до глобальних. Акцент робиться саме на постійних трансляціях різних механізмів обговорення й прийняття рішень. У такому сенсі така форма демократії постає як реакція на кризу представницької демократії, причому в обох її варіантах, а саме ліберальної і консервативної.

Критика представницької демократії з боку протаганістів деліберативної загострюється в просторово-часовому вимірі її змісту. Йдеться про такий складник демократичних процедур, як вибори. В залежності від політичної культури цей період триває чотири, п’ять, шість років. Ці терміни по-різному аргументуються, проте важливим є не так їхня періодичність, як смисл, який полягає у тому, що прийняття рішення фокусується в момент виборів і все подальше суспільне життя точиться навколо такого рішення (правильного чи помилкового, прогресивного чи консервативного, оптимістичного чи алярмісько-апокаліптичного). При цьому важливим аргументом на користь деліберативної демократії постає теза про пришвидшення розвитку всіх сфер людського буття. Наочно збільшення швидкостей ми вбачаємо в технологічних сферах. Згадаймо як змінюються наші гаджети. Причому не тільки функціонально, а й ззовні, оскільки з’являються нові матеріали, які використовуються у виробництві багатьох товарів.

Вирішивши необмежені можливості різних форм обговорення для розв’язання актуальних проблем людського існування – від господарсько-економічних до персонально-індивідуалістичних слушно запитати: у який спосіб таке обговорення стає дієвим і нагальним? Відповідь є простою, а саме люди хочуть бути почутими, отже беруть участь у дискусіях, публічних обговореннях, інтерактивних практиках, зокрема через мас-медіа. Але чи маємо ми як мовці достатньо навичок брати участь в таких відповідальних практиках, адже саме тут формується рішення, які згодом втілюються в життя? Відповідь не така вже проста і знайти її можна в теорії дискурсу як актуального міждисциплінарного інструментарію дослідження соціокультурної сфери сучасного інформаційного суспільства.

Така теорія дискурсу постала в галузі лінгвістики, проте є евристичною на теренах гуманітаристики в межах лінгвістичного повороту в філософії 20 століття (з 50-х років). Вона надає критерії розрізнення дискурсу й абсурду, раціонально-аргументативного й ірраціонально-хибного, спрямованого на порозуміння чи на насильство тощо. Йдеться про форми, процедури, приховані локутиви, які спотворюють дискурсивні практики, з одного боку, проте, з іншого, виявляють емансипаційний потенціал дискурсів. Я маю можливість знайомити студентів-бакалаврів і аспірантів з такою теорією в межах двох навчальних дисциплін, які запропоновані кафедрою філософії нашого університету (навчальні дисципліни відповідно: соціальна етика і комунікативна етика). Мій досвід викладання свідчить про зацікавленість студентів теоретичними знаннями про дискурси й практичними навичками участі в них.

Насамкінець поясню, чому доречно говорити про ціннісні засади прав людини в сучасному українському суспільстві. Сьогодні на пленарному засіданні згадували Конституцію Пилипа Орлика. Текстологи і правники дослідили цей документ і дійшли висновку, що він був найкращим для початку 18-го століття. Попри це соціальні умови його реалізації в Україні й досі не створені. Звичайно, процес модернізації, демократизації, розвитку громадянського суспільства, персональних ініціатив вимагає часу з огляду на контроверсійні умова становлення української незалежності. Проте в політиці євроінтеграції часто-густо спостерігається крен в бік інструменталізації цього процесу, тобто переважають прагматичні мотивації над ціннісними. Ми залюбки купуємо німецькі і французькі авто, італійський одяг і взуття, мандруємо європейськими столицями з відвідуванням їхніх музеїв, відпочиваємо в Іспанії тощо. І маємо суперечності з Венеційською комісією щодо прав і свобод людини, з Угорщиною щодо цінностей освіти, з Польщею щодо історичної пам'яті. Добре, що такі теми потрапляють до публічної сфери, але вони вимагають компетентного обговорення. А такі компетентності набуваються індивідами в процесе навчання і опанування різним досвідом, зокрема й дискурсивними. Ми маємо говорити про дискурсивне право і забезпечувати його реалізацію. Я вдячна організаторам конференцію за надання мені можливості обговорити актуальну проблему деліберативної демократії.

----------***----------

Головатий А. А., *студент ФСП КПІ ім. Ігоря Сікорського*
Науковий керівник: ***Фурашев В. М.,***
к.т.н, с.н.с.

ФІЛОСОФІЯ СУСПІЛЬНИХ ВІДНОСИН МАЙБУТНЬОГО[11]

Що чекає нас завтра, за черговим поворотом історії? Це питання зараз доречне як ніколи раніше. Всеохоплюючий розвиток технологій набрав небувалих темпів. Віртуальна реальність, відновлення органів та кінцівок - це тільки те, що з'явиться зі дня на день. А скільки всього ще лишається безіменним, не створеним ще навіть багатою людською фантазією? Так чи інакше, все що з'явиться в найближчі десятиріччя приведе до змін, які торкнуться всіх аспектів життя як суспільства в цілому, так і окремих індивідів.

Одним із найперших видів соціальних відносин, який підпаде під колосальні зміни, швидше за все, буде система освіти. Завдяки розвитку і поширенню інтернету класичні методи навчання вже сьогодні здаються морально застарілими. Вже в близькому майбутньому як учень, так і викладач будуть змушені бути надзвичайно креативними. Пояснюється це тим, що тоді залишиться набагато менше спеціальностей, доступних людині, адже велика частина механічної роботи (якщо не вся цілком) буде перекладена на роботів. Основна проблема навчання вже зараз полягає в тому, що будь-яка інформація стала настільки доступною, що виділити щось дійсно корисне, не вміючи відсівати непотрібні дані, стало дуже важко.

В умовах роботизації багато професій зовсім зникнуть, тож очевидно, що дуже серйозно постане питання про безробіття. Як виживатиме суспільство, яке майже цілком складається з безробітних людей? Якщо керуватися здоровим глуздом, то великі компанії, в яких велику частину роботи виконуватимуть роботи, повинні будуть виплачувати податки (відповідно до степені роботизації) державі, яка, в свою чергу, займатиметься соціальними виплатами. З огляду на той факт, що поширення роботів-робітників буде абсолютним, можна справедливо вважати, що вищевказана система зможе стабілізувати матеріальний стан суспільства. Однак, хоч це і вирішить матеріальне питання, залишається інше, значно складніше - зайнятість. Більшій частині населення буде просто нічим зайнятися. Пафосні промови про всезагальний саморозвиток всього суспільства варто відкласти вбік, адже болісний досвід минулого підказує, що реалії цього часу будуть зовсім іншими – значно страшнішими,

[11] Внаслідок органаційно-технічного збою дана робота не була опубліквана у збірнику «Теоретико-правові основи формування та розвитку інформаційного суспільства : Матеріали науково-практичної конференції. 29 листопада 2017 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : КПІ ім. Ігоря Сікорського» Вид-во «Політехніка». 2017».

ніж ми можемо собі уявити. Алкоголь і наркотики знайдуть друге дихання і, у всякому випадку спочатку, заберуть забагато життів.

З попереднього пункту випливає одне цікаве питання - які ж будуть функції і обов'язки держави у відношенні до індивідів у майбутньому? Перш за все, відповідь на це питання залежить від двох таких явищ як масове переселення в мегаполіси і глобалізація. І якщо в першому сумніватися не доводиться, то друге поки-що виглядає доволі сумнівно. Як би там не було, держава або ж держави повинні будуть гарантувати населенню гідне життєзабезпечення - контролювати різноманітні соціальні виплати, поставку продукції, підтримання правопорядку й багато іншого.

Також не можна забувати про таку неймовірно важливу форму соціальних відносин як сім'я і, власне, шлюб. У цієї традиції неймовірно довге коріння, кінці якого губляться далеко в історії людства. Ще з найдавніших часів, у тому чи іншому форматі, завжди існував шлюб із усіма подальшими правовідносинами. І перше, що зникне вже зовсім скоро – стереотип необхідності шлюбу. Ні, назовсім ця традиція не зникне, напевне, ніколи, але поява роботів «спеціалізованого призначення» однозначно позначиться на ставленні людей до шлюбу як до такого. У далекому майбутньому це призведе до стирання кордонів у відносинах між людьми і роботами, незалежно від статі. У контексті всього вищесказаного можуть виникнути деякі побоювання щодо культурного (в нашому розумінні) розвитку підростаючих поколінь, однак бояться цього не варто - не дивлячись на всю відкритість нового суспільства завжди будуть витримуватися певні рамки етики, ймовірно, відмінні від наших, але точно не менш ефективні.

Наостанок варто відзначити, що зміни, зумовлені науково-технічним прогресом, призведуть до повного переосмислення всіх аспектів соціальних відносин, що призведе до безповоротного оновлення суспільства.

----------***----------

Шмоткін О. В., *к. ю. н., професор, професор кафедри теорії та історії держави і права Національної академії Служби безпеки України.*

ПРАВА ОСОБИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У сучасному цивілізованому світі забезпечення прав людини є метою і сенсом існування держави і права. Це знайшло своє юридичне відображення у Конституції України, ст.3 якої встановлює: «Утвердження і забезпечення прав і свобод людини є головним обов’язком держави». Відповідно до Закону України

«Про основи національної безпеки України» конституційні права і свободи людини і громадянина є об'єктом національної безпеки України.

З нашої точки зору, під правами людини слід розуміти можливості людини щодо задоволення її матеріальних, фізичних та духовних потреб, які зумовлені природою людини, а також політичним, соціальним, економічним і культурним рівнем розвитку суспільства.

Треба відмітити, що реалізація права людини неможлива без здійснення відповідного обов'язку. Це зумовлено тим, що результатом реалізації права є наявність у людини певного матеріального або нематеріального блага. Це благо може виникнути лише внаслідок відповідної необхідної, обов'язкової суспільної діяльності індивідів. Залежно від результатів цієї обов'язкової діяльності виникає і певний рівень реалізації прав людини. Зміст прав людини є еквівалентом здійснення нею відповідних соціальних обов'язків. Якщо людина не виконує їх, вона не має певних благ, як результат здійснення її прав або має їх за рахунок виконання соціального обов'язку іншими індивідами. Але ці блага, які отримуються внаслідок експлуатації інших, не можна вважати правами людини. Таким чином права людини не можуть існувати без її обов'язків.

На наш погляд, обов'язок людини – це міра необхідної поведінки, якої людина повинна дотримуватись для забезпечення реалізації прав. Розглядаючи проблему прав людини в аспекті забезпечення національної безпеки, насамперед слід зазначити, що у ст. 3 Закону України «Про основи національної безпеки» об'єктами національної безпеки визначені:

– людина і громадянин – їхні конституційні права і свободи;

– суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне та навколишнє природне середовище і природні ресурси;

– держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Отже, перше місце серед об'єктів національної безпеки було надано саме правам і свободам людини і громадянина, які сьогодні є однією з основоположних цінностей світової цивілізації.

Стосовно цього об'єкта, головним є повна, своєчасна, точна реалізація прав і свобод людини і громадянина.

Повна реалізація передбачає, що на практиці повинні реалізовуватись усі можливості людини, які закріплені нормами про її права.

Своєчасна реалізація вимагає, щоб між виникненням потреб у людини в реалізації певного права та його практичним здійсненням було мінімум часу.

Точна реалізація означає, що здійснення права повинно відбуватись відповідно до букви й духу норми права, що закріплює певне право людини.

Відповідно до загроз реалізації прав людини як об'єкта національної безпеки є неповна, несвоєчасна, неточна реалізація прав людини, а також їх порушення.

Треба відмітити, що об'єкти національної безпеки є системою, вони нерозривно взаємопов'язані. Права і свободи людини є, з одного боку, першоелементом цієї системи, з другого, – головним елементом. Це зумовлено тим, що людина є самоцінністю цивілізації, для забезпечення потреб та інтересів якої виникають усі соціальні інститути, зокрема суспільство і держава, тобто права і свободи людини є метою, а суспільство, держава та інші соціальні інститути – засобами реалізації цієї мети. Отже, якщо не забезпечуються належним чином реалізація прав і свобод людини, не можна говорити про належний рівень забезпечення національної безпеки загалом.

Викладене вище дає змогу вважати права людини головним об'єктом національної безпеки України, оскільки лише на основі безпеки особи, закріплюючи, реалізуючи, охороняючи і захищаючи насамперед її права і свободи, а також обов'язки, які є не менш важливим аспектом, можна планувати і здійснювати заходи щодо забезпечення безпеки більш складних соціальних систем, наприклад, таких, як суспільство і держава, та створювати умови для забезпечення національної безпеки загалом.

Проголошення людини, її прав і свобод, безпеки вищою цінністю України на законодавчому рівні є значним кроком на шляху до демократії, створення громадянського суспільства та правової держави. Проте сьогодні доводиться констатувати, що в Україні людина залишається вищою цінністю переважно в теорії, а держава виконує свій обов'язок щодо неї вкрай незадовільно.

На нашу думку, важливим кроком щодо поліпшення ситуації, в якій опинилася людина в Україні, могло б стати прийняття закону, який би врегулював суспільні відносини у сфері забезпечення безпеки особистості (назва може бути, наприклад, «Про безпеку людини в Україні» чи «Про організаційно-правові заходи забезпечення безпеки людини в Україні»). Закон України «Про основи національної безпеки України» закріпив, як вже згадувалося, основні засади державної політики у сфері забезпечення національної безпеки, зокрема засади такої політики у сфері безпеки людини, створивши таким чином фундамент для подальшого формування законодавчої бази із зазначених питань. Тому нормативно-правовий акт, що пропонується, стане логічним продовженням як зазначеного Закону, так і Конституції України та засобом розвитку її певних положень.

Необхідно відмітити, що забезпечення прав людини повинно бути спрямовано, по-перше, на збереження біологічних та духовних основ особи, по-друге, на неприпустимість руйнування цих основ, по-третє, удосконалення біологічної та духовної природи людини. Без здійснення цих трьох

взаємопов'язаних цілей сенс існування прав людини втрачається. Головним при цьому є забезпечення високого рівня духовності особи, без якого навіть за максимального задоволення матеріальних потреб вона перетворюється з людини у бездуховну біологічну істоту.

Права особи за своєю сутністю, сенсом, призначенням існують для того, щоб людина звільнилася від негативних тваринно-біологічних рис, а не навпаки.

Треба відмітити, що без здійснення обов'язків людиною щодо себе, щодо свого оточення, щодо суспільства загалом вирішити цю проблему неможливо.

При удосконаленні механізму забезпечення прав особи слід враховувати ті зміни, які відбулися у соціальній практиці в останні роки у сфері прав людини.

На нашу думку, крім трьох відомих прав поколінь людини: громадянських та політичних (XVIII-XIX сторіччя), соціально-економічних (початок XX сторіччя), солідаристських (середина XX сторіччя) слід виокремити четверте покоління прав особи – прав на самозбереження.

Ця група прав спрямована на захист особи від деструктивного фізичного або ідеологічного впливу. До неї можна, зокрема, віднести такі права: право на мирне існування, на захист від життєвонебезпечних хвороб, захист від клонування, захист від генетично модифікованих продуктів, захист від негативного інформаційно-психологічного впливу та деякі інші права.

Незважаючи на життєву актуальність цих прав, бо вони стосуються існування людини як біологічної і духовної істоти, це четверте покоління прав людини, на жаль, не виокремлюється фахівцями у сфері прав особи. Однак, ігнорування цією групою прав неприпустимо, тому що це загрожує існуванню людської цивілізації.

Насамперед, це стосується інформаційних прав особи. Без перебільшення можна стверджувати, що на теперішній час інформація стала основною рухомою силою суспільства. Якщо інформація об'єктивна, повна, своєчасна суспільство прямує в прогресивному напрямку і навпаки. При цьому повинна існувати еквівалентна кореляція між інформаційними правами і обов'язками суб'єктів права. Якщо вони не виконують інформаційних обов'язків щодо об'єктивності, повноти, своєчасності інформації, що стосується, насамперед, офіційних розповсюджувачів інформації, це наносить не меншу шкоду ніж відсутність інформаційних прав, або їх різноманітні девіації.

Крім цього, при формуванні механізму забезпечення прав особи, в тому числі і інформаційних, слід зважати на те, що в конкретному суспільстві вони, в першу чергу, зумовлюються тими економічними, соціальними, культурними умовами, що існують в цьому суспільстві. Ці суспільні умови, що породжують права особи є об'єктивними для даного конкретного суспільства. Цими національними закономірностями неможливо нехтувати для дотримання

міжнародних норм. Право на національну безпеку у загальносвітовому масштабі аналогічно праву особи у масштабі держави. Тому неможливо вимагати пріоритету прав особи перед державою, не вимагаючи пріоритету права нації перед міжнародною спільнотою. Таким чином, при вирішенні проблем прав особи слід зважати на реалії свого національного суспільства, орієнтуючись на загальносвітові стандарти, тобто внутрішньодержавні закономірності у цьому процесі повинні бути імперативними, а загальносвітові – диспозитивні.

Як вважається, викладені пропозиції будуть сприяти удосконаленню забезпеченню прав особи як об'єкта національної безпеки України.

----------***----------

Ткачук Т. Ю., *к.ю. н., доцент, заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки НА СБ України.*

ВЗАЄМОЗВ'ЯЗОК НАЦІОНАЛЬНИХ ЦІННОСТЕЙ, ІНТЕРЕСІВ ТА ЦІЛЕЙ У КОНЦЕПЦІЇ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Об'єктами правового забезпечення інформаційної безпеки України є: людина і громадянин – їхні конституційні права і свободи, фізичне та психологічне здоров'я, захищеність від негативного впливу інформаційних технологій та інформації; суспільство і держава – захищеність їх законних інтересів в інформаційній сфері; інформаційні ресурси та інформаційна інфраструктура – їх цілісність, доступність та захищеність.

Зважаючи на той факт, що об'єктами інформаційної безпеки можуть бути свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення, пропонуємо об'єктом правового забезпечення інформаційної безпеки держави розглядати:

- національні цінності в інформаційній сфері;
- національні інтереси в інформаційній сфері;
- національні цілі в інформаційній сфері

Американські військові дослідники Ярґер Річард та Джордж Барбер, розглядаючи дану тріаду в системі забезпечення національної безпеки держави, національні цінності визначають як найменш рухомий і найстабільніший елемент системи. Цінності формуються під час історичного процесу, розвитку матеріальної та духовної культури суспільства, відповідають геополітичному спрямуванню країни. Національні інтереси – елемент порівняно динамічний, що

формується на основі національних цінностей під впливом довгострокових тенденцій суспільного розвитку. Національні цілі – найрухоміший елемент [1].

Доктрина інформаційної безпеки України визначає та змістовно наповнює тільки національні інтереси в інформаційній сфері.

Реалізація визначених в Доктрині інформаційної безпеки України національних інтересів в інформаційній сфері буде ефективною і дієвою за умови законодавчого визначення національних цінностей, які зумовлюють потребу у розробці національних (державних) інтересів. Таким чином першочергового законодавчого визначення потребують саме національні цінності в інформаційній сфері. Дана тріада повинна бути чіткими орієнтирами формування та розвитку державної політики.

Національні цінності в інформаційній сфері – це сукупність духовних та матеріальних цінностей людини, суспільства і держави, яким властиві чітко окреслені світоглядні, соціокультурні, соціально-економічні, географічні та демографічні ознаки. Вони формують правову, філософську та етичну основу для забезпечення подальшого існування суспільства і держави, дають змогу усвідомити національну мету держави в інформаційній сфері. Національні цінності в інформаційній сфері, виходячи із сутнісного їх тлумачення, являють собою найбільш особливий сегмент, той який потребує особливого захисту. До *національних цінностей в інформаційній сфері,* з огляду на сучасний стан державотворення в Україні, слід віднести:

1. **Матеріальний добробут** населення, у тому числі й на основі розвитку ІКТ.

2. **Інформаційна захищеність** людини, суспільства, держави.

3. **Духовність**. Доступність віросповідання, відсутність загроз, попередження релігійного фанатизму та екстремізму, недопустимість використання релігії як психологічного чиннику у тероризмі, розвиток традиційних українських релігійних напрямів.

4. **Мова**, як основний ідентифікатор нації, як спосіб передачі інформації та знань, як пам’ять поколінь.

5. **Культура** інформаційних відносин.

6. **Свобода інформації.** Захищеність інформаційних прав людини, доступ до інформації, нейтралізація негативних інформаційних впливів.

Первинним у структурі національних цінностей в інформаційній сфері має стати соціально-економічна складова інформаційної безпеки. Таким чином, на наше глибоке переконання, добробут населення, як базова категорія економічної політики держави, має стати базовим компонентом й інформаційної безпеки держави, а особливо, національної безпеки нашої держави.

На думку Г. Ситника об’єктивне існування і вплив на безпеку особи, суспільства, держави та людської цивілізації природних і суспільних явищ

зумовлює можливість розподілу цінностей на природні й соціальні [2, с. 123], що загалом й відображено у запропонованому вище переліку національних цінностей в інформаційній сфері.

Відомий вчений у галузі філософії та національної безпеки Б. Парахонський ще на початку 90-их років минулого століття зазначав, що у сучасному світі захист національних інтересів уже не може спиратися лише на стратегію силового протистояння. Ефективнішою стає реалізація власних національних інтересів за допомогою економічної, духовно-інтелектуальної експансії [3, с. 3]. Дане твердження підтверджене вітчизняною історію останнього десятиріччя зі своєю кульмінацією у 2014 році.

До **національних цілей в інформаційній сфері** відносимо:

1. *Покінчити* з порушенням та спотворенням поглядів людей на навколишній світ і самих себе, що здійснюється шляхом культивування уявних цінностей, насадження деструктивних пріоритетів, завдань і цілей перед суспільством і окремою особистістю (духовна безпека);
2. *Забезпечити* впровадження інформаційних технологій у військову сферу та забезпечити їх захист (військова безпека);
3. *Прискорити* розробку та впровадження новітніх конкурентоспроможних ІКТ в суспільно-економічну сферу (економічна безпека);
4. *Досягти* належного рівня культури інформаційних відносин (соціальна безпека);
5. *Створити* загальнодержавні інформаційні системи для постійного екологічного моніторингу стану навколишнього середовища (економічна безпека);
6. *Сприяти* інтеграції національної інформаційної інфраструктури із світовою інфраструктурою.
7. *Зміцнити* захист інформаційних прав людини;
8. *Вжити термінові заходи* для створення позитивного іміджу держави в умовах інформаційної глобалізації.

Варто підтримати позицію відомого українського дослідника державного правління національною безпекою Г.Ситника, який дійшов висновку, що національні цінності визначають сутність (зміст), цілісність і стійкість, національні інтереси – структуру і характер, а національні цілі – конфігурацію та спрямованість формування та функціонування даної системи [4, с. 46]. Це стосується в цілому й інформаційної безпеки держави.

Список використаних джерел:

1. Yarger Richard H, George Barber The U.S. Army War College Mehtodology for Determining Interests and Levels of Intensity. Carlisle Barracs, U.S. Army War College, 1997 http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm

2. Ситник Г. П. Державне управління національної безпеки (теорія і практика) / Г. П. Ситник. – Київ : Вид-во НАДУ, 2004. – 408 с.
3. Парахонський Б.О. Національні інтереси України (духовно-інтелектуальний аспект): монографія. — К.: НІСД, 1993. — 43 с.
4. Ситник Г. П. Державне управління національної безпеки (теорія і практика) / Г. П. Ситник. – Київ : Вид-во НАДУ, 2004. – 408 с.

----------***----------

Доронін І. М., *к. ю. н., доцент, зав. наукової лабораторії НДІІП НАПрН України.*

ТРАНСФОРМАЦІЯ ПРАВА ВІЙНИ В ІНФОРМАЦІЙНУ ЕПОХУ

Дослідження прав і свобод людини, а саме їх природи, напрямів реалізації, підстав та можливостей до їх обмежень завжди були у полі зору правових наукових досліджень. Незважаючи на значний масив наукових праць у цій сфері, саме розуміння прав і свобод останнім часом піддається трансформації з огляду на виклики і загрози, характерні для інформаційної епохи. Окрім цього феномен прав людини вийшов зі сфери правових наук і активно розглядається філософами, соціологами, політологами. Вплив інформаційної епохи змінив і саму суть прав людини. Як зазначено в літературі права людини «потрібно винаходити і відновлювати в нових історичних контекстах і за інших силових співвідношень» [1, с. 13].

Так звані нові «силові співвідношення» поряд із глобальними загрозами останнього часу (тероризм, міграція, транснаціональна організована злочинність», означають і нові аспекти соціальних явищ, що постійно виникають та трансформуються. До цих аспектів можливо віднести так звані «нетрадиційні» війни в їх соціальному та правовому розумінні. Насамперед мова йде про «гібридну війну» та «кібервійну».

«Гібридна війна» перебуває в поле зору широкого кола науковців різних спеціальностей з початком агресії проти України в 2014 році. Саме цей фактор зумовив вихід дослідження «гібридної війни» зі сфери військових наук та політології до широкого кола дослідників, що зосереджуються як на загальному розумінні цього феномену так і на окремих його проявах. Зазвичай «гібридну війну» розуміють як такий спосіб ведення війни, що включає в себе постійне поєднання власне бойових дій (як державними військовими формуваннями так і недержавними учасниками) з небойовими діями в інших сферах (пропаганда, саботаж, диверсії, втручання у внутрішню політику, економічна війна (торгівельні та фінансові обмеження). При цьому ведення бойових дій здійснюється одночасно з вказаними допоміжними факторами з можливим частковим припиненням окремих з них на певний час. Якщо проаналізувати

війни та збройні конфлікти XX-XXI сторіччя в історичній ретроспективі, можливо прийти до висновку, що практично всі вони велись зазначеними вище методами. Це характерно як для війн, що розпочинались у формі внутрішньодержавного конфлікту із подальшим залученням підтримки інших держав, так і для агресій, що маскувались внутрішньодержавними конфліктами. Холодна війна другої половини XX сторіччя також цілком може вважатись тривалою світовою «гібридною війною» стратегічного характеру.

Аналізуючи загальну термінологію у цій сфері слід, на нашу думку, слід чітко виокремити суто військове розуміння «гібридної війни» (як напрям або вид військової стратегії, вид військових операцій або характеристику бойових дій). Як правило, у військовій науці увага дослідників зосереджена на певному аспекті зазначеного виду військових дій. Наприклад, Ф.Хоффман зосереджує увагу на участі в «гібридній війні» недержавних учасників, або учасників, чітко не пов'язаних із конкретною державою [2]. Зазначена точка зору, висловлена у 2007 році в основному ґрунтувалась на емпіричному матеріалі, що надала глобальна терористична активність ісламістських екстремістських організацій на зразок «Аль-Каїди», хоча з точки зору зовнішніх проявів можливі історичні паралелі із діяльністю лівоекстремістських угруповань, що тривалий час здійснювали партизанську війну в окремих регіонах (Латинська Америка, Філіппіни, Південно-Східна Азія), націоналістичних організацій (починаючи з арабських та африканських політичних груп, утворених всередині XX сторіччя).

Ототожнення проявів «гібридної війни» безпосередньо з діями Росії увійшло до наукового дискурсу після анексії Криму 2014 року, хоча фіксувались і інші прояви (придністровська війна, вторгнення до Грузії, інформаційні акції проти країн Балтії). Але розуміння суті такого виду війни ґрунтувалось на зміні підходів до пізнання явищ та трансформації його проявів. Так, академік В.П. Горбулін у 2014 році, досліджуючи суть «гібридної війни» через призму геостратегії, визначав наступні стратегічні елементи, характерні для такої війни у цілому – політична складова (використання зовнішньополітичного фактору та конкретної ситуації в країні-об'єкті агресії, широке залучення політичних суб'єктів, парамілітарних угруповань, недержавних суб'єктів та навіть відверто кримінальних структур), – економічна (у випадку агресії проти України це енергетична) складова, – інформаційна складова (сучасні форми пропаганди та розповсюдження ідей у першу чергу непрямими методами серед населення у зоні конфлікту, в країні – об'єкті агресії, у власній країні та у міжнародному співтоваристві) [3, с. 7-9].

Як правило, численні публікації українських вчених останніх двох років визначаючи відсутність терміну «гібридна війна» в міжнародному праві, пропонують врегулювати це питання на міжнародному рівні або дати визначення шляхом правової регламентації в Україні. Зазначена точка зору, на

нашу думку, не зовсім ґрунтується на правовому аналізі становища, що склалась, та видається передчасною.

Іншою «нетрадиційною війною» в літературі вважається «кібервійна». Зазначений термін у військовій науці зарубіжних країн розроблено більш детально аніж «гібридна війна». Ключовим є розуміння застосування сили у іншому (поряд із сушею, морем та повітрям) вимірі. Кіберпростір розуміється як театр військових дій. За такого розуміння різниця між традиційними театрами військових дій та кіберпростором полягає лише у застосуванні інших видів зброї та інших тактичних дій. Зрозуміло, що в американській військовій науці на сьогодні домінує точка зору розуміння «розширеного» театру військових дій, коли комплексно під загальним керівництвом застосовуються усі сили та засоби. Відмінність «кібервійни» полягає у тому, що їх сили та засоби можливо застосовувати окремо від інших, приховано і водночас ефективно. Але оскільки мова у такому разі йде про бойові дії, неодмінно виникає питання розгляду «кібервійни» як війни у розумінні міжнародного права, на що вже звернуто увагу юристів [4, 5, 6]. Сукупність проблем, що виникають у цьому контексті, зумовлює дослідження, які спрямовані на вирішення питань визначення моменту початку війни, допустимості застосування до таких ситуацій норм міжнародного гуманітарного права, правового статусу зброї у конфлікті, що відбувається у кіберпросторі тощо.

Актуалізацію зазначеної проблематики спричинили «кібератаки», які здійснювались та підтримувались державами, і мали за своєю суттю характер агресії. Насамперед мова йде про кібератаки 09 травня 2007 року, що у подальшому стали відомі як «естонські кіберінциденти». Під «естонськими кіберінцидентами» слід розуміти масштабні дії, спланованні та скоординовані з Росії, стосовно державних органів та об’єктів інфраструктури Естонії, які відбувались у кіберпросторі, та полягали у нанесенні шкоди зазначеним об’єктам. Загальний характер проведених операцій та аналіз заподіяних збитків є предметом низки наукових досліджень, спрямованих, в першу чергу, на пошук шляхів реалізації державної політики у сфері кібербезпеки [7, p. 21].

Відразу після «естонських кіберінцидентів» виникло питання чи можливо розуміти такі акти агресії «актами війни» у світлі права війни, а якщо так – які саме межі та умови застосування сили держави проти таких актів, чи викликають кібератаки стан війни за нормами права?

Правова відповідь на зазначені питання відбувалась у контексті реагування на зазначені інциденти з боку НАТО. Розробка проблем застосування норм права війни до кіберпростору проводилась на базі спільного Центру НАТО зі співробітництва у кібербезпеці (м. Таллінн, Естонія) з 2009 року із залученням фахівців у галузі міжнародного права, правових проблем військової сфери та інформаційного права передусім з США, Канади, Великої

Британії та Естонії. Консультативну допомогу надавали науковці з університетів та науково-дослідних установ Нідерландів, Данії, Швейцарії, Швеції та Бельгії. Наслідком їх роботи став узагальнюючий документ під назвою «Талліннський статут» (Tallinn Manual, у деяких перекладних джерелах документ також згадується як «Талліннський документ»), перший варіант якого було опубліковано у 2013 році [8]. У лютому 2017 року вийшла доповнена версія документа під найменуванням «Талліннський статут 2.0», яка уточнила певні правові позиції, не змінюючи загальні підходи. Зазначений статут не є нормативно-правовим актом і не має методичного характеру для державних органів або військових структур. Він є інформаційно-аналітичним документом, що відображає точку зору наукових кіл, а його вплив на формування державної політики у державах-учасницях НАТО є значним.

Щодо застосування положень права війни у кіберпросторі визначені наступні позиції:

– загальні положення права війни мають повною мірою застосовуватись щодо відносин у кіберпросторі, а застосування загальних правових принципів не вимагають створення особливого виду права щодо війни у кіберпросторі;

– щодо об’єктів кіберінфраструктури застосовується принцип суверенітету держави за ознакою територіального знаходження об’єкту, а також загальні міжнародні принципи прапору або місця реєстрації (за аналогією з повітряними та морськими судами);

– будь-який напад на об’єкт, що вчинений будь-яким шляхом порушує державний суверенітет з усіма відомими міжнародному праву наслідками;

– при проведенні операцій із застосування сили у кіберпросторі повинні виконуватись положення міжнародного гуманітарного права, які застосовуються до збройних конфліктів;

– вчинення злочинів проти людства, а також порушень права та звичаїв війни підлягає розгляду міжнародними судовими інстанціями. При цьому відповідальність держави розповсюджується не тільки на дії комбатантів (військовослужбовці, державні органи, спецслужби, парамілітарні групи), а і на окремих осіб, у т.ч. негромадян, які діють з території держави, і держава не здійснює заходи протидії щодо них.

Отже сучасна ситуація ведення «гібридної війни» та кібервійни проти України зумовлює необхідність пошуку нових шляхів та методів забезпечення національної безпеки. Певні явища трансформації суті і характеру сучасних війни здійснюють вплив на стан правового регулювання суспільних відносин. Водночас існуюча концепція міжнародного права (у т.ч. права війни) цілком може бути застосована до ситуацій із трансформацією війн в інформаційну епоху, враховуючи її ведення у кіберпросторі як театрі військових дій. Певна модифікація характеру правового регулювання можлива, ґрунтуючись на

загальних стабільних принципах права. Детального правового регулювання потребуватимуть питання удосконалення стратегічного планування у сфері забезпечення кібербезпеки та проведення ефективного реформування діяльності державних органів сектору безпеки і оборони в інформаційній сфері у першу чергу стосовно визначення їх правового статусу та надання відповідного обсягу повноважень.

Список використаних джерел:

1. Рєпа А. Права людини: філософія долання перешкод/А. Рєпа// Філософія прав людини. За ред. Ш. Госепата та Г.Ломана. – К.: Ніка-центр, 2016. – С. 7-14.
2. Hoffman Frank. Conflict in the 21st Century: the Rise of Hybrid War/ Frank G.Hoffman. – Arlington, Potomac Institute for Policy Studies, 2007. – 72 p.
3. Горбулін В.П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу/В.П.Горбулін//Стратегічна панорама. – 2014. – № 4 (33). – С. 5-12.
4. Graham David. Cyber Threats and the Law of War/ David E. Graham// Journal of National Security and Law Policy. – 2010. – Vol. 4:87. – P. 87-102.
5. Dunlap Charles. Perspectives for Cyber Strategists on Law for Cyberwar/ Charles Dunlap Jr.// Strategic Studies Quarterly. – 2011. – Spring Vol. – P. 81-99.
6. Putnik N. Kiber ratovanje – novi oblik savremenih društvenih konflikata/Nenad Putnik// Belgrade: University of Belgrade, 2012, – 476 p.
7. Kovacs Laszlo. Cyber Security Policy and Strategy in the European Union and NATO /Laszlo Kovacs// Revista Academiei Fortelor Terestre. – 2018. – № 1(89). – P. 16-24.
8. Tallinn Manual on the International Law Applicable to the Cyber Warfare/ Michael Schmitt (ed.). New York, Cambridge University Press, 2013 – 302 p.

----------***----------

Косогов О. М., *к.військ.н., с.н.с.,*
провідний науковий співробітник в/ч А1906;
Гордієнко Л. О., *м.н.с., в/ч А1906*

МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ЗАХОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ У ВОЄННІЙ СФЕРІ

На сьогодні світовий геополітичний простір та внутрішньодержавні відносини формуються в умовах інформаційного протиборства. Для нашої держави ця проблема особливо актуальна. Зважаючи на певну невизначеність геополітичного статусу, політичну нестабільність, нестійкість вітчизняного інформаційного простору, Україна перебуває під систематичним інформаційним тиском.

В умовах збройної агресії Росії проти України, а саме анексії Криму, підбурювання, організації та всебічного забезпечення збройного протистояння

на сході нашої держави, проявляється нова тенденція ведення Росією воєнних дій.

Відомий американський військовий теоретик Френк Хоффман одним з перших зазначив: "…війни сучасної епохи характеризує процес гібридизації, у рамках якого змішуються традиційні форми війни, кібервійни, організованої злочинності, іррегулярних конфліктів, тероризму тощо".

Водночас всі ці заходи супроводжуються цілеспрямованою потужною інформаційною кампанією. В часи інтенсивного розвитку інформаційних технологій, наявності глобальних інформаційних мереж і не менш глобалізованих засобів масової інформації, складова "інформаційного супроводу" у гібридних війнах має надзвичайно важливе, якщо не вирішальне, значення. У цих умовах гостро постає проблема захисту національного інформаційного простору.

Враховуючи викладене, пошук шляхів надійного виявлення інформаційних загроз та протидії їм є актуальним науковим та практичним завданням.

Процес забезпечення безпеки інформації повинен носити комплексний характер і має ґрунтуватися на глибокому аналізі можливих негативних наслідків (логіко-евристичний аналіз). Такий аналіз припускає обов’язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їхньому прояву (уразливостей) і, як наслідок, визначення актуальних загроз інформаційній безпеці.

У ході аналізу необхідно переконатися, що всі можливі загрози та їх джерела ідентифіковані, всі можливі уразливості ідентифіковані та зіставлені з ідентифікованими джерелами загроз, всім ідентифікованим джерелам загроз і уразливостям (факторам) зіставлені методи реалізації.

При цьому важливо мати можливість, у разі потреби, не змінюючи самого методичного інструментарію, вводити нові види джерел загроз, методів їх реалізації, уразливостей, які стануть відомі в результаті подальшого отримання знань у цій сфері.

Виходячи з такого принципу, моделювання й класифікацію джерел загроз, загроз та їх проявів, а також розробку ефективних заходів протидії доцільно проводити на основі аналізу взаємодії логічного ланцюжка: Джерела загроз $\rightarrow$ Загрози $\rightarrow$ Реалізація загроз (атаки) $\rightarrow$ Уразливості $\rightarrow$ $\rightarrow$Об’єкти $\rightarrow$ Наслідки (збиток) $\rightarrow$ Заходи протидії.

Виявлення та аналіз загроз інформаційній безпеці є першим етапом у розробці стратегії протидії інформаційних загроз (політики безпеки). При цьому процес виявлення та аналізу загроз слід розглядати в органічному зв’язку з процесом протидії загрозам.

Процес аналізу починається з визначення основних загроз та їх джерел.

На основі ідентифікованих загроз та їх джерел аналогічним чином складаються таблиці методів реалізації загроз (атак), можливих у даній сфері, уразливостей об'єктів, якими ці атаки можуть скористатися, переліку об'єктів забезпечення інформаційної безпеки та заходів забезпечення інформаційної безпеки.

Таким чином, на першому етапі аналізу загроз ідентифікуються всі елементи множин загроз, джерел, об'єктів і заходів забезпечення інформаційної безпеки.

На другому етапі необхідно експертним методом встановити відносини між такими видами елементів.

"Джерела загроз – Загрози", тобто встановити, яке джерело породжує які загрози.

"Загрози – Атаки", – встановити, яка загроза через яку атаку реалізується.

"Атаки – Уразливості", – встановити, яка атака використовує які уразливості.

"Уразливості – Об'єкти захисту", – встановити, яка уразливість належить до якого об'єкту захисту.

"Заходи протидії – Загрози", – встановити, який захід протистоїть якій загрозі.

Після аналізу відносин між елементами множин, виділених у процесі ідентифікації, проводиться оцінка ризиків. Цей процес дозволяє мінімізувати витрати ресурсів на заходи протидії. У процесі аналізу можливих і виявлення актуальних загроз оцінюється ризик, що виникає внаслідок потенційного впливу певної загрози.

Відомо декілька різних методик аналізу та оцінки ризиків (переважно закордонних). Усі вони дозволяють отримати лише якісну їх оцінку на основі експертних методів.

Запропонована методика полягає в наступному. Оцінка ризику здійснюється за допомогою оцінки можливості реалізації загроз безпеці, пов'язаних з уразливими, властивими тим чи іншим об'єктам захисту. На основі аналізу впливу загроз, їм приписується високий, середній або низький рівень ризику по кожній зоні локалізації уразливостей.

Оцінювалися всі загрози, уразливості та ризики для забезпечення впевненості в тому, що процес оцінки ризиків в організації є повним.

При проведенні оцінювання ризиків розглядаються такі основні категорії втрат: фінансові збитки, зниження ефективності функціонування та ускладнення діяльності МО України.

Фінансові збитки визначаються збільшенням витрат на відновлення та удосконалення технічних (програмних) засобів елементів інформаційної інфраструктури МО України та Збройних Сил України.

Зниження ефективності функціонування МО України визначається неспроможністю структурних підрозділів МО України та Збройних Сил України ефективно виконувати покладені на них завдання. Це відбувається внаслідок:

- зниження морально-психологічного стану співробітників, а також зміни в стані психіки (психічного здоров'я);
- зниження мотивації співробітників до військової служби та їх невпевненість у завтрашньому дні;
- зниження боєздатності військових колективів (зниження службової активності, дезертирство, симуляція хвороб, відхилення від виконання наказів начальників, зрада, подавлення волі, неадекватна поведінка);
- порушення функціонування системи управління структурними підрозділами;
- несправності (виведення з ладу) технічних (програмних) засобів інформаційної інфраструктури;
- порушення властивостей інформації, яка циркулює в кібернетичному просторі МО України та Збройних Сил України (конфіденційність, доступність, цілісність, спостережність).

Ускладнення діяльності МО України стосується ситуацій, що впливають на втрату суспільної довіри до МО України та Збройних Сил України, погіршення їх іміджу.

Оцінка рівнів ризику може здійснюватись за такими ознаками:

високий: значна грошова втрата, втрата продуктивності або значне ускладнення діяльності, що є результатом реалізації загрози, внаслідок наявності відповідної уразливості;

середній: номінальна грошова втрата, втрата продуктивності або виникають певні ускладнення діяльності;

низький: або мінімальна можливість грошової втрати, втрати продуктивності мінімальні або не існують.

Таким чином, стає зрозумілою картина розподілу загроз і втрат від їх можливої реалізації за всіма об'єктами безпеки. Подальшим етапом оцінки ризиків є своєрідне підбиття підсумку – складання таблиці оцінки ризиків, яка заповнюється за допомогою додання об'єднаного рівня ризику кожної із зон уразливості.

----------***----------

***Костенко І. В., к**.ю.н., доцент кафедри публічного права ФСП КПІ ім. Ігоря Сікорського.*

ГІБРИДНА ВІЙНА, ЯК ІНФОРМАЦІЙНЕ НАСИЛЬСТВО У СУЧАСНОМУ СВІТІ

Гібридна війна – це військова стратегія, яка об'єднує звичайну війну, малу війну і кібервійну, вона включає в себе комбінацію партизанської та громадянської воєн, а також заколоту і тероризму. [1].

Автором терміну був американський генерал Д. Маттіс у вересні 2005р., після подій 9 вересня 2000 р. Після заяви Маттіса, його ідею розвинуто науковим співробітником Національного університету оборони США Френком Гофманом у монографії «Конфлікт у XXI столітті: походження гібридних воєн» у 2007 р. Сьогодні термін набув загального визнання, він застосовується різними країнами з різними, іноді прямо протилежними цілями. Вважаю необхідним розібратися хто я як використовує термін гібридна війна і з якою метою, чому ця стратегія перетворюється у інформаційне насильство у сучасному світі.

Гібридна війна з точки зору американських військових аналітиків це в першу чергу війна зі світовим тероризмом. Політика «космополітичних гуманітарних інтервенцій», у боротьбі з «релігійними фанатиками» вимагала нових підходів, зміни характеру військових конфліктів. У його рамках дослідники вивчали літературу й перевіряли дані про нові способи ведення війни, зокрема теорії «війни четвертого покоління», «комплексної війни», а також знамениту книгу сучасних китайських стратегів «Необмежена війна» [2].

Після анексії Криму Росією, термін гібридна війна, на той час трохи забутий, тріумфально повернулася. Його поверненню випадково сприяла стаття начальника російського генштабу генерала Валерія Герасімова, перед Академією військових наук, опублікованої в лютому 2013р. у газеті «Военно-промышленный курьер» і передрукована у англомовному журналі Military Review. Співробітник «Радіо Свобода» Роб Коулсон у червні 2014 року назвав статтю Герасімова «російською військовою доктриною» «нелінійної війни». Основною метою нелінійних бойових дій Герасимов вважав досягнення потрібних стратегічних і геополітичних результатів шляхом використання явної і тайної дипломатії, економічного тиску, завоювання симпатії населення країни, яку потрібно ввести у коло своїх інтересів. [3].

Винахідник терміна Гофман підтвердив, що саме така війна триває в Україні (а також точилася в Грузії 2008 році). Знищення малазійського літака влітку 2014 року він навів як приклад «катастрофічного тероризму», що в його теорії є однією з тактик гібридної війни.

Яку мету переслідують апологети російського світу у гібридній війні?

Після розпаду Радянського Союзу, Росія, всіма можливими засобами намагається взяти реванш за поразку і відвоювати місто світового лідера, відродити Радянський Союз. Але ідея Руського світу вже показала свій руйнівний вплив. Стагнація економіки, зубожіння населення, тоталітарна ідеологія, репресії все це є непривабливим для населення пострадянських країн. І лише власне населення, лідеру країни віртуозно вдається зомбувати вже протягом десятиліть. Хоча і там тривають протести. П'ятого травня 2018 р., напередодні інавгурації Путина, пройшли протести під гаслом «Він нам не цар» у Москві. Під час акції протесту заарештовано понад 1500 учасників.. Після невдалої спроби приєднати Україну до Митного Союзу, Росії, яка має великий досвід «холодної війни», довелось розпочати проти неї гібридну війну.

Разом із тим, директор Українського інституту національної пам'яті Володимир В'ятрович заявив, що Кремль веде в Україні не гібридну, а "більшовицьку" війну[66, с. 43]. Світ говорить про якійсь новий тип війни, який застосовується проти України, так звану гібридну війну, але мені здається, насправді, цей тип не новий – це типовий більшовицький тип ведення війни, який вівся проти України ще в 1918 році", – зазначив В'ятрович. Суть цього методу полягала в тому, що "на певній території створюється якась паралельна, альтернативна влада, як Раднарком Радянської України у Харкові в 1918 р., на противагу УНР, створюються збройні формування, які визнаються Москвою, ведеться активна інформаційна, пропагандистська компанія серед населення для його підтримки, а потім вже розгортається безпосередня агресія – вторгнення на територію України регулярної армії. [4].

Захоплення території противника не є головною метою гібридної війни. На перше місце встає моральне знищення ворога. Так учасники Майдану (майданівці) у свідомості зомбованих російською пропагандою росіян стали фашистами, а кольорові революції у світі росіяни вважають гібридними війнами США проти Росії. А з іншого боку Кремль стає символом світового зла, а Путин кровавим диктатором. Народи двох країн зробили ворогами на підсвідомому рівні. Олеся, яка проживає у Москві ненавидить брата Ореста за те що він у Києві вживає новонароджених. І, як не дико це чути, знадобляться десятиліття щоб вивітрити цей дурман.

Але українцям боляче чути, що іноді у наший країні критика сприймається як «російська загроза і гібридна війна». Під час поїздки до США, Президент України назвав редакційну статтю в "New York Times" , яка викриває корупцію в Україні, елементом гібридної війни, що ведеться проти України через поширення інформації, яка дискредитує державу. На що журналіст газети відповів, що «українські посадовці намагаються позбутися будь-якої критики, представляючи її «гібридною війною» з боку Росії». [5].

Теорія гібридної війни знає багато заходів протидії руйнівного впливу інформаційного насильства. Це, у випадку України, заборона трансляції російського телебачення, яке дійсно зомбує населення прифронтових територій. І це нарешті вже зроблено і жителі мають змогу бачити українські канали.

Але нам здається, що більш переконливою буде ситуація коли покращитися життя українців, коли з нашого життя зникне недовіра до уряду, піде у минуле такі виразки сьогодення як корупція, олігархіям і на зміну їх прийде повага і довіра. Саме на цьому її паразитує так звана російська пропаганда.

Список використаних джерел:

1.Чекаленко Л. Про поняття "гібридна війна" / Л. Чекаленко // Віче. – 2015. – № 5. – С. 41-42. – Режим доступу: http://nbuv.gov.ua/

*2.*Володимир Артюх Туман «гібридної війни»: чому шкідливо мислити гібридно. [Електронний ресурс] / В. Артюх . – Режим доступу: https://commons.com.ua/ru/tuman-gibridnoyi-vijni-chomu-shkidlivo-misliti-gibridno/

3.Герасимов, В., 2013. «Ценность науки в предвидении». *:* Военно-промышленный курьер, 27 февраля – 5 марта 2013, стр. 1–3. . – Режим доступу : www.vpk-news.ru/articles/14632

4.Володимир В'ятрович: Росія веде в Україні більшовицьку війну[Електронний ресурс] /В. В'ятрович. – Режим доступу : https://espreso. tv/article/2014/11/29/volodymyr_vyatrovych_rosiya_vede_v_ukrayini_bilshovycku_viynu

5.Непереможна українська корупція. повний текст статті у New York Times. Режим доступу : https://ua.112.ua/mnenie/neperemozhna-ukrainska - koruptsiia-povnyi-tekst-rezonansnoi-statti-the-new-york-times-301986.html

----------***----------

Забара І. М., *к.ю.н., доцент кафедри міжнародного права Інституту міжнародних відносин Київського національного університету ім. Тараса Шевченка.*

ПРАВО ЛЮДИНИ НА ІНФОРМАЦІЮ: ДОКТРИНАЛЬНІ ПІДХОДИ В МІЖНАРОДНОМУ ПРАВІ

Доктринальні дослідження, що проводились протягом останніх більш ніж сімдесяти років, значною мірою охопили питання, пов'язані із категорією *«свобода інформації»* у міжнародному праві. Чималу увагу їй було приділено у низці вітчизняних і іноземних досліджень.

Разом з тим, використання раніше накопичених обсягів різноманітної інформації, викликає низку теоретичних і практичних питань, серед яких – гарантована можливість доступу і отримання такої інформації, дотримання

балансу між «правом знати» і необхідністю забезпечення таємниці для захисту ключових державних і приватних інтересів. Окремі дослідники – Ф. Ла Руе, А. Лігабо, Т. Мендел, Г. Крішнан, А Фігарі, А. Хуссейн та інші, звернули увагу і на іншу категорію, яку почали визначати як *«право на інформацію»*.

Зауважимо, що словосполучення «право на інформацію», «право на вільний пошук інформації», «право на пошук і отримання інформації» і «право на доступ до інформації» на першому етапі становлення і розвитку концепції (1990-2003 рр.) використовувались як синонімічні (тотожні) поняття. У подальшому стали використовувати словосполучення «право на інформацію», зокрема у щорічних Доповідях Спеціального доповідача ООН з питань сприяння і захисту права на свободу переконань та їх вільне волевиявлення, а також у спільних щорічних деклараціях, що приймається ним спільно з Головою Організації із співробітництва і співробітництва в Європі (ОБСЄ) з питання про свободу засобів масової інформації, Спеціальним Доповідачем Організації американських держав (ОАД) з питань про свободу висловлювання думок і Спеціальним доповідачем Африканської комісії з прав людини і народів (АКПЛН) з питань про свободу висловлювання думок і доступу до інформації (1999-2010 рр.).

Для розуміння суті права на інформацію, необхідно звернути увагу на низку основних аспектів, на яких акцентують свою увагу її прихильники.

Загальне розуміння права на інформацію базується на положенні, що людині повинно бути забезпечено захист її права на отримання інформації та ознайомлення з різними ідеями (п. 35) [1]. Така початкова теза була аргументована постійно зростаючою соціальною і політичною роллю інформації в сучасному суспільстві. Саме вона стала однією з базових положень для системи поглядів, що складались навколо неї, а з часом – і концепції права на інформацію (п. 36) [2].

Прихильники концепції права на інформацію обґрунтовують свій підхід виходячи із закріпленої в міжнародно-правових актах свободи шукати інформацію. Підставою виступають відповідні положення ст. 19 Загальної декларації прав людини 1948 р. і ст. 19 Міжнародного пакту про громадянські і політичні права 1966 р. та інших актів.

Аргументуючи свою позицію, вони виходять з наступних постулатів:

1. Свобода шукати інформацію *«тягне за собою право шукати інформацію в тій мірі, в якій ця інформація є загальнодоступною»* (п. 34) [1], (п.38) [2].

Вперше ця позиція була висловлена у 1994 році (п. 34) [1] і до нашого часу є базовою.

2. *«Право шукати та мати доступ до інформації є одним з важливих елементів свободи слова та вираження поглядів. Свобода буде позбавлена будь-*

якої ефективності, якщо позбавити людей доступу до інформації» (п. 35) [1], (п.38) [2], (п. 35) [3].

Фактично такий підхід дає можливість його прихильникам говорити про «дві складові» права на інформацію:

1) гарантовану відповідь на запит про надання інформації, і

2) гарантований доступ до інформації.

Крім цього, варто звернути увагу і на те, що це положення дає підстави прихильникам вказувати і на необхідність захисту такого права. На їх думку, оскільки право на інформацію «представляє собою один із суттєвих елементів права на свободу слова і вільне вираження їх переконань, захист цього права повинен бути правилом, а його обмеження – лише виключенням із загального положення (п.5) [4].

Зауважимо, що в кінцевому рахунку реалізація права на інформацію спрямована на отримання необхідної інформації. Цей підхід залишається незмінним протягом усього періоду формування концепції і знаходить підтримку в ООН і інших міжнародних організаціях.

Варто звернути увагу на те, що в теперішній час в доктрині і практиці увага почала концентруватись на «другій складовій» – питанні гарантованого доступу до інформації (або «праві на доступ до інформації»).

3. Реалізація права на інформацію спрямована на отримання гарантованого доступу виключно до державної інформації.

Підкреслюючи важливість права на інформацію як фундаментального елементу демократії і свободи, а також реалізації права на розвиток (п. 42) [5], послідовники цієї концепції досить принципово наголошують і на тому, що «доступ до інформації є основою демократичного образу життя. Тому тенденцію утримувати інформацію від широких верств населення необхідно рішучо припиняти» (п. 35) [1], (п.38) [2]. Розвиваючи цю тезу, прихильники наполягають на необхідності гарантованого доступу саме до державної інформації. Необхідність такого доступу вони аргументують наступним: «при відсутності поваги до права на свободу вираження поглядів, яке включає в себе право шукати, отримувати і поширювати інформацію і ідеї, неможливо здійснювати на практиці право голосу, відкрито казати про порушення прав людини і викривати корумповані і неефективні уряди» [6, с. 8].

Т. Мендел, характеризуючи цей аспект, зазначає, що «державні органи зберігають інформацію не для себе, а заради суспільного блага. По суті, ця інформація повинна бути доступною для громадськості за тієї умови, що її зберігання не є для суспільства більш пріоритетним. В цьому відношенні закони про отримання доступу до інформації відображають основну ідею державності, де держава слугує народу» [6, с. 4].

А.В. Хан, в свою чергу, характеризуючи такий підхід, зауважує, що «державні органи володіють величезним обсягом інформації, і зберігати її в таємниці означає серйозно порушувати право на свободу вираження поглядів, гарантоване міжнародним правом, а також більшістю конституцій» [6, с. 1].

4. Право на інформацію накладає на державу позитивний обов'язок забезпечити доступ до інформації (п.14) [7], (п.12) [8], (п.39, п.44) [2].

Варто відмітити, що цей позитивний обов'язок держави розглядався спочатку виключно як забезпечення доступу до матеріальних носіїв інформації.

З розвитком концепції ця позиція уточнювалась. Сьогодні, на думку прихильників концепції, доступ до державної інформації не обмежується тільки доступом і ознайомленням з інформацією на носіях, які знаходяться в державних установах. Вказується і на можливість отримання інформації безпосередньо від державного органу, як першоджерела. Так, А. Лігабо зазначає, що «у тих випадках, коли мова йде про уряди, за будь-яких можливих обставин громадськість повинна отримати доступ до «державної діяльності», наприклад до роботи різних нарад і форумів (п. 14) [7], (п. 40)[2]. В свою чергу, А. Хусейн вказує і на умови такого доступу, підкреслюючи, що «право на доступ повинно реалізовуватись в усіх, а не у виключних випадках» (п. 12) [7], (п. 39) [2]. Враховуючи такий підхід, можна говорити про достатньо широке коло випадків, коли держава повинна надавати інформацію.

Разом з тим, необхідно вказати і на випадки його обмеження. Так, на думку А. Лігабо, позитивний обов'язок держави забезпечити доступ до інформації може бути обмежений тільки тими положеннями, які містяться в п. 3 ст.19 Міжнародного пакту про громадянські і політичні права (п. 12) [8], (п. 47) [2]. Нагадаємо, що йдеться про обмеження, які спрямовані на захист поваги прав і репутації інших осіб, охорону державної безпеки, громадського порядку, здоров'я та моральності населення.

Вважається, що «системи засекречування інформації варто використовувати лише для засекречування такої інформації, розголошення якої «неминуче» завдасть шкоди державі» (п.12) [7].

5. Суттєвим аспектом, на якому загострюють свою увагу прихильники права на інформацію, є зміст інформації, до якої повинно бути надано гарантований доступ. За минулі півтора десятка років, це питання пройшло в своєму розвитку кілька періодів.

Спочатку мова йшла тільки про доступ до суспільної інформації. Ф. Ла Руе, зауважував, що «в умовах демократії право доступу до суспільної інформації є основоположним фактором забезпечення транспарентності. Для того, щоб демократичні процедури були ефективними, люди повинні мати доступ до суспільної інформації, яка визначається в якості інформації, що відноситься до усіх видів діяльності держави. Це дозволить їм приймати

відповідні рішення, здійснювати своє політичне право обирати та бути обраним; ставити під сумнів державну політику або здійснювати вплив на неї; слідкувати за якістю системи державних витрат і укріплювати систему підзвітності. Все це в свою чергу, дозволяє здійснювати контроль з метою не зловживання владою» [9, с. 7].

В подальшому, розвиток питання, пов'язаного із змістом інформації, пішов шляхом надання гарантованого доступу вже до окремих видів інформації. Мова йде про доступ до інформації, що знаходиться у держави і яка стосується проблем екології, ВІЛ/СНІД, тероризму, а також прав людини.

Актуальними і перспективними називаються «екологічні дослідження і дослідження впливу на здоров'я людини, національні бюджети і соціальні витрати, проекти промислового розвитку і торгівельна політика», доступ до історичних даних і архівів, які містять інформацію про порушення прав людини (п. 34) [9].

Варто врахувати, що сьогодні склалось два підходи, які враховуються на глобальному, регіональному і національному рівнях. Перший – полягає в тому, щоб закріпити право на інформацію в цілому, другий – закріпити право на доступ до інформації певного змісту.

Найбільш активно цей процес протікає на регіональному і національному рівнях, про що свідчить кількість прийнятих національних законодавчих актів. Відмічається, що сьогодні їх вже нараховується більше шістдесяти. Як правило, вони враховують положення про забезпечення доступу до інформації, включаючи: дотримання принципу максимального розголошення, презумпцію публічного характеру нарад і ключових документів, широке визначення типів доступної інформації, розумну плату і розумні терміни, незалежний аналіз відмов у розголошення інформації, санкції в випадку недотримання режиму доступу (п. 32) [9]. Не є виключенням і законодавство України (Закон України «Про доступ до публічної інформації від 13.10.2011 (№2939-VI).

Враховуються і положення прийнятих раніше конвенцій, що визначають обов'язки держав щодо надання доступу до інформації. Зокрема, Конвенції про оцінку впливу на навколишнє середовище у транскордонному контексті 1991 р., Конвенції про доступ до інформації, участі громадськості в процесі прийняття рішень і доступі до правосуддя з питань навколишнього середовища 1998 р., Конвенції Ради Європи про доступ до офіційних документів 2009 р. та інших.

6. Право на інформацію носить самостійний характер («має самостійне значення»).

В цьому питанні необхідно звернути увагу на зміни у трактуванні природи права на інформацію. Спочатку воно розглядалось прихильниками концепції подвійно: як похідне і як самостійне право. Зазначалось, що право на інформацію є «суттєвим елементом права на свободу слова і вільне

висловлювання своїх переконань (п. 35) [1], а також, що воно «грає не тільки допоміжну роль у справі передачі інформації, але й має самостійне значення» (п. 5) [4]. Підставою для визнання права на інформацію в якості похідного, називалась ст. 19 Міжнародного пакту про громадські і політичні права 1966 р., що закріплювала право на вільне вираження своїх думок, яке включає серед інших, саме свободу шукати інформацію. Саме вона слугувала підставою для широкого тлумачення, виокремлення і обґрунтування його похідного характеру. Разом з тим підкреслюючи значимість і необхідність права на інформацію, прихильники вказували і на його самостійний характер.

З часом, таке трактування природи права на інформацію було змінено: право на інформацію почали розглядати виключно як право, яке носить самостійний характер. Зазначалось, що «це право існує само по собі. Як таке, воно є одним із прав, на яких базуються вільні і демократичні суспільства» (п. 42) [8].

Таким виступають концептуальні засади права на інформацію в науці міжнародного права, що сприяють обґрунтовуванню необхідності його визнання і закріплення не тільки в національних законах, а і у конституціях держав.

Список використаних джерел:

1. 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 [Електронный ресурс] – Режим доступа: http://daccess-ods.un.org/TMP/7821679.71134186.html.

2. Резолюция Комиссии по правам человека. Гражданские и политические права, включая вопрос свободы выражения мнений. Право на свободу мнений и их свободное выражение. Доклад Специального докладчика г-на Амбейи Лигабо, представленный в соответствии с резолюцией 2003/42 Комиссии. 12 декабря 2003 г. E/CN.4/2004/62 [Електронный ресурс]. – Режим доступа: http://ap.ohchr.org/documents/dpage _e.aspx?m=85.

3. Резолюция Комиссии по правам человека. Гражданские и политические права, включая вопрос свободы выражения мнений. Доклад Специального докладчика г-на Абида Хуссейна, представляемый в соответствии с резолюцией 1999/36 Комиссии. 18 января 2000 г. E/CN.4/2000/63 [Електронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/4718434.21459198.html.

4.) 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 1996/53 Комиссии по правам человека. 4 февраля 1997 г. E/CN.4/1997/31 [Електронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/5678730.60703278.html.

5. Резолюция Комиссии по правам человека. Гражданские и политические права, включая вопрос свободы выражения мнений. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное их выражение г-на Абида Хуссейна, представляемый в соответствии с резолюцией 1999/36 Комиссии по правам человека от 18 января 1999. [Електронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/4718434.21459198.html.

6. Мендел Т. Свобода информации: сравнительно-правовое исследование. / Т. Мендел; – Изд. 2-е, доп. – Париж, ЮНЕСКО,2008.– 176 с.

7. 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 1997/27 Комиссии по правам человека от 28 февраля 1998 E/CN.4/1998/40 [Електронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/9652923.3455658.html.

8. Резолюции Комиссии по правам человека. Гражданские и политические права, включая вопрос свободы выражения мнений. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное их выражение г-на Абида Хуссейна. 29 января 1999 г. E/CN.4/1999/64 [Електронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/980569.422245026.html.

9. Резолюция Совета по правам человека. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное их выражение Франка Ла Руе от 20 апреля 2010 [Електронный ресурс]. – Режим доступа: http://daccess-ods.un.org/TMP/4187773. 16808701.html.

----------***----------

Дзьобань О. П., *д.ф.н., професор, г.н.с., НДІ інформатики і права Національної академії правових наук України м. Харків.*

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ ВІТЧИЗНЯНОГО ДЕРЖАВОТВОРЕННЯ ЯК ФАКТОР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Розвиток у напрямку інтеграції у європейську спільноту – це цивілізаційний вибір України. У системі зовнішньополітичних пріоритетів нашої держави він посідає особливе місце. Активізація євроінтеграційних процесів означає також її більш інтенсивне включення у міжнародну співпрацю щодо врегулювання конфліктів та протидії новітнім загрозам у сфері безпеки. Основними ж напрямами забезпечення інформаційної безпеки у сфері міжнародної співпраці є інтеграція в міжнародну систему забезпечення інформаційної безпеки і співпраця стосовно запобігання протиправних дій в інформаційній сфері.

Першочерговим у цьому плані є повернення українців до власної історії, уникнення історичного безпам'ятства українського народу, розвиток його самосвідомості до рівня усвідомлення себе як народу історичного, самобутнього, державо- та культуротворчого. Людина, яка втрачає пам'ять, втрачає й саму себе. Вона перетворюється на сліпого виконавця чужої волі, субстрат, додатковий матеріал чужої соціальної творчості, політичних маніпуляцій. Те саме стосується й народу. Лише той народ має майбутнє, який пам'ятає свою історію, зв'язок зі своїм корінням, постійно звертається до витоків і водночас творить нову історію цивілізованими засобами.

Така постановка питання вимагає особливого звернення до проблеми забезпечення безпеки, оскільки проблеми національної ідентичності, національної культури й ментальності завжди знаходяться в епіцентрі смислового ядра національної безпеки. У сучасному українському контексті питання підтвердження власної європейської ідентичності безпосередньо пов'язані з проблемами інтеграції до Європейського Союзу.

На противагу традиційному підходу до безпеки, який асоціюється у першу чергу з воєнною складовою, із застосуванням військових засобів, європейське бачення виходить із цілісного розуміння безпеки як взаємної залежності політичного, соціально-економічного, екологічного, культурного, військового та, передусім, інформаційного вимірів. Цьому відповідає трактування ЄС себе як цивільної структури, що прагне здійснювати стійкий і довготерміновий вплив на міжнародне оточення шляхом створення відповідного інформаційного середовища, а не за допомогою методів силового тиску або захоплення. Саме тому європейський вектор вітчизняного державотворення є одним з основних об'єктів інформаційної безпеки України.

У Європі є розуміння того, що заходи у боротьбі із глобальними загрозами будуть по-справжньому дієвими лише за умов налагодження відповідної структури обміну інформацією між її членами. Україна, яка вживає усіх можливих заходів стосовно євроінтеграційного державотворення, за таких умов неминуче зіткнеться з проблемою узгодження безпекових підходів з ЄС і з забезпеченням власної інформаційної безпеки.

Створення планетарного інформаційного простору за допомогою глобальних комп'ютерних мереж може мати серйозні наслідки для національної, зокрема економічної безпеки. Інформаційний простір не має державних кордонів, не має таких інститутів захисту державних інтересів, якими є прикордонна й митна служби, поки що відсутні способи і засоби контролю цінності і важливості інформаційних ресурсів, що «перевозяться» через кордон. Поки що державний кордон є практично прозорим для інформаційних ресурсів.

Якщо протягом перших двох третин XX ст. війна переважно впливала на інформаційну сферу, то останнім часом цілком очевидно спостерігається зворотний зв'язок як на макро-, так і на мікрорівні.

На сьогодні Україна, здійснюючи складні демократичні та соціально-економічні трансформації, перебуває в зоні ризику з точки зору інформаційної безпеки, оскільки цій сфері тривалий час не приділялась належна увага, що стало однією з причин посилення внутрішніх протиріч та конфліктів, інспірованих ззовні за допомогою передусім інформаційно-комунікаційних засобів. Агресивного інформаційно-психологічного впливу з боку Російської Федерації зазнає не лише українське та російське суспільства, громадяни країн пострадянського простору, а й населення США, країн ЄС. Для реалізації цього впливу застосовується арсенал засобів, передусім телебачення та інтернет-ресурси. Оплотом російського іномовлення є заснований у 2005 р. одіозний телеканал Russia Today (RT), що транслюється у понад 100 країнах світу, має 700 млн аудиторію, цілодобове мовлення. Наприкінці 2014 р. було додатково запущено Інтернет-портал «Sputnik», який використовує інформаційний потік телеканалу RT, що значно збільшує можливості доступу до інформації, яку створює та поширює RT. Російські пропагандистські ресурси вдало експлуатують ідею свободи слова та інформації для поширення дезінформації в європейському суспільстві з метою не просто викликати довіру аудиторії або переконати її у власній правоті (на відміну від класичної публічної дипломатії), а, розповсюджуючи теорії змови та неправдиві чутки, викликати сумніви, розгубленість, відчуття зневіри.

Актуальною є також проблема методів захисту існуючих інформаційно-телекомунікаційних систем і технологій. Розвиток інформаційних і телекомунікаційних систем, їх широке впровадження у всі сфери життєдіяльності суспільства призводить до зростання залежності суспільства, окремої людини від безперебійного функціонування даних засобів, від гарантій використання накопичуваної в них інформації в інтересах громадян, що не суперечить законним інтересам, суспільства і держави. Очевидно, що помилки в роботі інформаційних систем управління повітряними перевезеннями, рухом залізничного транспорту тощо можуть послужити причиною великих трагедій і величезного матеріального збитку, не говорячи вже про системи управління небезпечними виробництвами, АЕС, стратегічною ядерною зброєю. Все це дозволяє констатувати, що складові інформаційної безпеки є центральними для національної безпеки.

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у

життєво важливих сферах суспільної державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою не лише суверенітету України, функціонуванню життєво важливих сфер суспільної й державної діяльності, що реалізовується на інформаційному рівні, а й процесу інтеграції України у європейську спільноту.

Разом з тим, безсистемність процесів формування інформаційної інфраструктури України зумовлює складність розв'язання проблеми інформаційної безпеки, захисту інформаційних ресурсів на усіх рівнях.

Результати аналізу зовнішніх впливів на інформаційний медіа- і кіберпростір України дозволяють констатувати існування реальних загроз для нашої держави. Ґрунтуючись на традиційних підходах, можна виділити декілька їх основних груп. Перша група загроз пов'язана з бурхливим розвитком нового класу зброї − інформаційної, яка здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії. Друга група загроз для особистості, суспільства й держави − це новий клас соціальних злочинів, заснованих на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство тощо). Третя група загроз − електронний контроль за життям, настроями, планами громадян, політичних організацій. Четверта група загроз – використання нових інформаційних технологій у політичних цілях.

Сьогодні ефективність євроінтеграційного процесу безпосередньо залежить від того, наскільки швидко буде «розміновано» свідомість щодо вирішення проблеми узгодження національної самоідентифікації з самоідентифікацією європейською, каталізатором чого має бути задоволення усього комплексу економічних, соціальних та інформаційних (духовних) інтересів та цінностей громадян України. Причому, якщо розглядати євроінтеграційний процес з ціннісного боку, то саме аксіологічне підґрунтя інформаційної безпеки України є квінтесенцією ментальних, цивілізаційних, політичних, правових, культурно-історичних цінностей і традицій, які повинні забезпечувати ефективність згадуваного процесу.

Головна функція європейської інтеграції – консолідація українського суспільства. Традиційно в Україні були чіткі регіональні відмінності у ставленні населення до зовнішньополітичних пріоритетів. Новий формат відносин із ЄС – Угода про асоціацію – передбачає зміну як самої моделі, механізмів поглиблення двосторонніх відносин, так і інформаційного забезпечення цих феноменів. Процес інтеграції набуде прикладних форм, а ефективність можна буде визначати за цілком конкретними критеріями та індикаторами. Це зміна законодавчої бази, впровадження стандартів та норм ЄС, зміна в системі вироблення та реалізації державної політики, рівень та характер української економіки. Все це відкриває нові можливості для зміни суспільної думки. Якщо

для пересічних українців наслідки євроінтеграції будуть ефективними й позитивними, то варто очікувати збільшення кількості прихильників європейського курсу в українському суспільстві. Якщо ж реформи будуть проводитися неефективно, то підтримка євроінтеграційної ідеї може зменшитися, а регіональні розколи – посилитися.

Історичний шлях наочно демонструє, що в ментальному просторі українського народу, як в об'єкті інформаційної безпеки, завжди поєднувались індивідуалізм, універсалізм, «гнучкість», відкритість, тяжіння до новацій і здатність їх самобутньої адаптації, що дозволяє оптимістично оцінювати перспективи України під кутом зору сприйняття нею парадигмальних змін у світі взагалі і змін, зумовлених євроінтеграційними процесами зокрема. Тож роль інформаційних аспектів безпеки у цих процесах важко переоцінити.

----------***----------

Корж І. Ф., д.ю.н., с.н.с., зав. науковою лабораторією, НДІ інформатики і права НАПрН України.

ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ, ВКЛЮЧАЮЧИ ПРАВОВУ, – НЕВІД'ЄМНЕ КОНСТИТУЦІЙНЕ ПРАВО ГРОМАДЯН

Як зазначала у свій час Уповноважений Верховної Ради України з прав людини В. Лутковська, прийняття Закону України «Про доступ до публічної інформації» [1] стало важливим кроком у сфері дотримання конституційних прав та свобод людини в Україні. Водночас, особливістю доступу до публічної інформації є набуття органами влади більшої відкритості та прозорості для громадян, що значно зменшує можливість зловживань та порушень [2, с.6].

Право на доступ до інформації є конституційним правом людини, яке гарантоване Конституцією України (ст.34) і базується на міжнародному праві. Так згідно з положенням Рекомендацій Парламентської Асамблеї Ради Європи Раді Міністрів (81) 19 [3], були визначені основні принципи доступу до інформації, яка знаходиться у розпорядженні органів державної влади. До них можна віднести:

– усі громадяни мають право робити запит на інформацію, яка знаходиться у розпорядженні державних органів, за винятком законодавчих і судових органів;

– для доступу необхідно забезпечувати ефективні та належні засоби;

– забороняється відмовляти у запиті на інформацію на підставі того, що вона не стосується особистих інтересів зацікавленої сторони;

– доступ забезпечується на основі рівності;

– кожен запит має бути розглянутий у визначений термін, а у випадку відмови у її надання, має бути надано чітке пояснення зазначеному;

– доступ до інформації може бути обмежений у випадках, зазначених у законі, які стосуються захисту інтересів національної безпеки, громадського порядку, розслідування кримінальних злочинів, або які можуть порушувати право на приватність;

– обмеження реалізації права на доступ має бути роз'яснено причину відповідно до закону чи практики;

– кожна відмова у наданні інформації може бути оскаржена.

Чинним законодавством України визначено основні принципи інформаційних відносин загалом, до яких віднесено [4]: гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об'єктивність, вірогідність інформації; повнота і точність інформації; законність.

Однак у науковій літературі зазначаються більш широкі підходи до зазначеного, з урахуванням міжнародних стандартів [5, с.185], а саме:

має діяти принцип максимального розкриття інформації, тобто державні органи повинні бути зобов'язаними публікувати ключову інформацію;

винятки повинні бути виписані зрозуміло і обмежувально;

інформаційні запити повинні бути оброблені швидко і справедливо;

осіб не повинні стримувати від подання інформаційного запиту надмірні витрати;

засідання державних органів повинні бути відкритими для громадськості;

закони, що суперечать принципу максимального розкриття інформації, повинні бути змінені або відмінені;

особи, які повідомляють інформацію щодо правопорушень – ті, хто «виносять сміття з хати» – свистуни (whistleblowers - інформатори) – повинні бути захищені.

Один з основних принципів – максимальне розкриття інформації, витікає з припущення, що вся публічна інформація, так чи інакше, належить людям. Член суспільства не повинен обгрунтовувати своє право мати доступ до будь-якої інформації. Тому органи державної влади повинні вживати активних заходів для поширення ключових типів інформації.

Якщо державна влада намагається заборонити доступ до інформації, вона повинна нести відповідальність щодо обгрунтування відмови . Саме відкритість є основним принципом доступу до офіційної інформації, тому інформація про діяльність органів влади всіх рівнів повинна бути відкритою й загальнодоступною.

З метою забезпечення конституційного права громадян на доступ до правової інформації, як різновиду публічної, та створення належних умов

користування чинними актами законодавства, на Міністерство юстиції України покладено функції офіційного видавця збірників актів законодавства України, а також їх оновлення. Публікація підзаконних нормативних актів, які пройшли процедуру державної реєстрації, відбувається відповідно до п. 6.7 Наказу Міністерства юстиції України «Про вдосконалення порядку державної реєстрації нормативно-правових актів у Міністерстві юстиції України та скасування рішення про державну реєстрацію нормативно-правових актів» [6].

Згідно з Указом Президента України [7] «Офіційному віснику України» та газеті «Урядовий кур'єр» надано статус офіційних друкованих видань, у яких підлягають оприлюдненню державною мовою акти Верховної Ради України, Президента України, Кабінету Міністрів України. Пізніше до Указу були внесені відповідні зміни щодо розширення переліку офіційних друкованих видань. Нині офіційними друкованими виданнями, в яких здійснюється офіційне оприлюднення законів та інших актів Верховної Ради України, є також газета «Голос України», «Відомості Верховної Ради України», а також офіційним друкованим виданням, в якому здійснюється офіційне оприлюднення законів, актів Президента України, є також інформаційний бюлетень «Офіційний вісник Президента України».

Ще одним актом, положення якого забезпечують право доступу громадян до інформації, є Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» [8]. Прийнятий відповідно до Конституції України, Закон визначає порядок всебічного і об'єктивного висвітлення засобами масової інформації діяльність органів державної влади та органів місцевого самоврядування, захисту їх від монопольного впливу органів тієї чи іншої гілки державної влади або органів місцевого самоврядування. Його положення регулюють порядок одержання, збирання, створення, поширення, використання і зберігання інформації про діяльність органів державної влади та органів місцевого самоврядування, задоволення інформаційних потреб громадян, юридичних осіб про роботу цих органів.

Таким чином на сьогодні питання доведення нормативно-правової інформації до громадян регулюється рядом нормативно-правових актів, включаючи підзаконні. Однак зазначене не відповідає положенням статті 57 Конституції України, згідно з якою закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення у порядку, встановленому законом. Не доведенні у такому порядку акти є нечинними. Тому, на нашу думку, є нагальна необхідність у прийнятті комплексного закону, положеннями якого б регулювалися зазначені питання.

Ще однією проблемою сьогодення у зазначеній сфері є той факт, що нормативно-правові акти органів місцевого самоврядування, які не підлягають

державній реєстрації, і які є джерелом національного права, не убезпечені від наявності в них неконституційних чи незаконних положень. Відповідність таких актів Конституції України чи законам України забезпечується лише внутрішнім «аудитом», а згадана невідповідність може бути оскаржена у судовому порядку.

Прокуратура функції загального нагляду позбавлена, інститут префектів, який передбачений проектом закону «Про внесення змін до Конституції України (щодо децентралізації влади)» (№ 2217а від 01.07.2015 р.) [9] і на яких покладена функція державного нагляду і контролю за додержанням Конституції і законів України органами місцевого самоврядування, повноваження яких виписані в ст. 119 документа, ще не запроваджений. Таким чином, утворилася прогалина у механізмі контролю за конституційністю та законністю прийняття актів органів місцевого самоврядування.

Необхідно зазначити, що рівень інформатизації українського суспільства постійно зростає, що вимагає швидкого доступу до актуальних текстів нормативно-правової інформації, забезпечуючи тим самим конституційне право громадян на участь в управління державними справами, в реалізації своїх прав і свобод. Водночас зазначене створює проблему визначення правового статусу інформації, яка розміщується на офіційних веб-сторінках державних органів. Зокрема розміщені на таких веб-сторінках тексти нормативно-правових актів в більшості випадків не мають вказівки на їх офіційне оприлюднення, тому немає простої можливості перевірити їх правильність.

В останні роки було підготовлено декілька законопроектів, метою яких було врегулювання нормотворчої діяльності, в тому числі і питань оприлюднення нормативно-правових актів. Деякі з них враховували можливість опублікування нормативно-правових актів не тільки в друкованому варіанті але й в електронному. Однак дана проблема до цього часу не вирішена.

Висновок: Роль інформації в житті нинішнього суспільства дуже значима. Завдяки їй збільшується обсяг виробництва, спрощується випуск продукції, використання матеріалів, технологічного обладнання, розширюються зовнішні та внутрішні зв’язки підприємства тощо. Більше того, інформація – тепер об’єкт купівлі та продажу. Особливо в нинішніх умовах зростає роль правової інформації, як різновиду публічної. Рівень доступу громадян до даної інформації є показником рівня впровадження принципів демократії в державі.

В Україні, як зазначалося в доповіді, існує ряд проблемних питань у даній сфері, які вимагають невідкладного вирішення з боку державної влади.

Список використаних джерел:

1. Про доступ до публічної інформації : Закон України від 13 січня 2011 року // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

2. Доступ до публічної інформації: найчастіші запитання та відповіді / За заг. ред. В. Андрусіва, Д. Котляра ; Укр. незалеж. центр політ. дослідж., – К.: [Агентство «Україна»], 2012. – 64 с.
3. Про доступ до інформації, що знаходиться в розпорядженні державних органів: Рекомендації Ради Європи № R (81) 19 від 25 листопада 1982 р. – Режим доступу : http://ippi.org.ua/sites/default/files/recr8119.pdf.
4. Про інформацію : Закон України від 02 жовтня 1992 р. // Відомості Верховної Ради України. – 1992, № 48. – Ст. 650.
5. Марущак А. І. Інформаційне право: Доступ до інформації : Навчальний посібник. – К. : КНТ, 2007. – 532 с.
6. Про вдосконалення порядку державної реєстрації нормативно-правових актів у Міністерстві юстиції України та скасування рішення про державну реєстрацію нормативно-правових актів : Наказ Міністерства юстиції України від 12 квітня 2005 р. № 34/5 // Офіційний вісник України. – 2005. – № 15. – Ст. 799.
7. Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності : Указ Президента України від 10 червня 1997 року № 503/97 // Офіційний вісник України. – 1997. – № 24. – Стор.11.
8. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації : Закон України від 23 вересня 1997 р. // Відомості Верховної Ради України. – 1997. – № 49. – Ст. 299.
9. Проект Закону про внесення змін до Конституції України (щодо децентралізації влади) : проект Закону від 1 липня 2015 р. № 2217а // http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55812.

----------*----------**

Ткачук Н. І., *к.ю.н., головний спеціаліст Департаменту інформаційно-аналітичного забезпечення Служби безпеки України.*

ОКРЕМІ ПИТАННЯ ЩОДО ПРАВОВИХ ФОРМ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД ЛЮДИНИ І ГРОМАДЯНИНА

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 в 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 передує 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.

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.

Список використаних джерел:

1. Конституція України від 28 червня 1996 року: [Електронний ресурс]. – Режим доступу: 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: [Електронний ресурс]. – Режим доступу: 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/ Ю.Сидорчук// Науковий вісник Чернівецького університету. – 2013, Випуск 682: Правознавство. – С.33-35

----------***----------

Луферeнко В. М., *аспірант Науково-дослідного інституту інформатики і права НАПрН України.*

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ У ФОРМІ ВІДКРИТИХ ДАНИХ В УКРАЇНІ.

У сучасному світі відкриті дані є не лише інструментом підвищення прозорості та ефективності роботи органів державної влади, а й потужним джерелом для стимулювання розвитку економіки країни. Нажаль, більшість українських урядових топ-менеджерів на сьогодні ще не повністю уявляють потенціал та можливості відкритих даних саме в економічному аспекті.

Публічна інформація у формі відкритих даних в Україні – це інструмент для реалізації конституційних прав і свобод людини на інформацію та участь громадськості в керівництві державою.

Тема відкритих даних на сьогоднішній день досить актуальна, нова, знаходиться в стадії розвитку. З впровадженням відкритих даних, підвищиться

прозорість та ефективність роботи органів державної влади, а також прискориться впровадження реформ, які призведуть до покращення соціально-економічного розвитку в Україні.

Нормативно-правове регулювання наборів даних, що підлягають оприлюдненню у формі відкритих даних.

9 квітня 2015 року Верховна Рада України ухвалила Закон України № 319 «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних». Зазначеним Законом внесені зміни до Закону України «Про доступ до публічної інформації» (стаття 10-1) з метою визначення базових норм та засад розвитку відкритих даних в Україні, а саме:

1.Публічна інформація у формі відкритих даних – це публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання;

2.Розпорядники інформації зобов'язані надавати публічну інформацію у формі відкритих даних на запит, оприлюднювати і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних та на своїх веб-сайтах;

3.Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації.

Відповідно до статті 10-1 Закону України «Про доступ до публічної інформації», Кабінет Міністрів України Постановою від 21 жовтня 2015 р. № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних», затвердив Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних (далі – Положення).

Цим Положенням визначено вимоги до формату і структури наборів даних, а також затверджено перелік пріоритетних наборів даних, які підлягають оприлюдненню (більше 300 наборів). Постановою чітко визначений перелік форматів для оприлюднення відкритих даних в залежності від їх виду:

Оприлюднення набору даних здійснюється розпорядником інформації наборів даних на офіційному веб-сайті розпорядника інформації або на Єдиному державному веб-порталі відкритих даних.

Створення та забезпечення функціонування Єдиного державного веб-порталу відкритих даних здійснюється Державним агентством з питань електронного урядування, яке є його держателем.

Адміністратором Єдиного державного веб-порталу відкритих даних є державне підприємство, яке належить до сфери управління Державного агентства з питань електронного урядування.

Єдиний державний веб-портал відкритих даних призначений для забезпечення надання доступу до публічної інформації у формі відкритих даних та передбачає доступ до інформації органів влади з можливістю її наступного використання.

Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації.

Цілі створення Порталу:

– забезпечення своєчасного розміщення органами влади інформації, яка підлягає оприлюдненню, а також будь-яких інших даних, що відповідають визначенню публічної інформації у формі відкритих даних;

– оприлюднення та регулярне оновлення розпорядником інформації відкритих даних на Порталі;

– забезпечення для всіх користувачів інформаційного простору спільних правил щодо оприлюднення інформаційних матеріалів у формі відкритих даних;

– забезпечення своєчасного розміщення повної та достовірної інформації;

– забезпечення ефективних двосторонніх комунікацій і каналів зворотного зв'язку.

Вимоги до структури наборів даних оприлюднених на Порталі:

Структура набору відкритих даних включає опис складу (елементів) набору даних, їх формат, параметри та призначення. Структура набору відкритих даних оприлюднюється у форматах XSD, JSON, CSV або інших аналогічних форматах.

Створення та забезпечення функціонування єдиного державного веб-порталу відкритих даних здійснюється Державним агентством з питань електронного урядування України за підтримки Кабінету Міністрів України, Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України, Громадянської платформи SocialBoost, Програми розвитку ООН в Україні, Міжнародного фонду «Відродження» та Представництва Microsoft в Україні.

Хартія відкритих даних.

Наразі Україна приєдналася до міжнародної Хартії відкритих даних.

Розробка зазначеної Хартії була ініційована представниками урядів Канади, Мексики, Великобританії, впливових міжнародних організацій до травня 2015 року під час міжнародної конференції з питань відкритих даних в Канаді. Міжнародну хартію відкритих даних було представлено під час Генеральної Асамблеї Організації Об'єднаних Націй, і, згодом, під час саміту G20 в Туреччині (листопад 2015) і COP21 у Франції (грудень 2015).

На сьогодні понад 17 урядів прийняли Міжнародну Хартію відкритих даних, серед яких уряди Великобританії, Канади, Франції, Італії, Мексики, Південної Кореї та ін..

Головною метою Міжнародної Хартії відкритих даних є покращення та сприяння співпраці та взаємоузгодженості для прийняття та реалізації спільних принципів, стандартів та кращих практик відкритих даних по всьому світу. Цілями Хартії є поширення демократії, боротьба з корупцією та сприяння економічному зростанню по всьому світу.

Хронологія впровадження в Україні наборів даних, які підлягають оприлюдненню у формі відкритих даних.

21 жовтня 2015 року Кабінет Міністрів України Постановою № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних», затвердив Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних.

16 серпня в Києві відбулась презентація спільного проекту Громадянської мережі ОПОРА та TechSoup щодо відкритих даних міст України, який було реалізовано за партнерської підтримки Державного агентства з питань електронного урядування України. Під час заходу було оголошено про старт конкурсу сервісів для міст на основі відкритих даних, а також презентовано спеціально розроблений Портал відкритих міських даних «Дані міст/ Apps4Cities».

22 вересня 2016 року Кабінет Міністрів України прийняв розпорядження № 686-р «Деякі питання приєднання до Міжнародної хартії відкритих даних».

Цілями зазначеної хартії є поширення демократії, боротьба з корупцією та сприяння економічному зростанню. Головною метою хартії є покращення та сприяння співпраці під час прийняття та реалізації спільних принципів, стандартів та кращих практик відкритих даних.

6-7 жовтня у Мадриді відбулась Міжнародна конференція з відкритих даних «InternationalOpenDataConference 2016», де зустрілись експерти з відкритих даних зі всього світу. В рамках заходу було офіційно оголошено про приєднання України до Міжнародної Хартії відкритих даних.

Проблемні питання:

– Відсутній контроль за достовірністю, постійним оновленням, повнотою оприлюдненої публічної інформації у формі відкритих даних.

----------***----------

Сніцаренко П. М., *д.тех.н., с.нс., пров. науковий співробітник Національного університету оборони України імені Івана Черняховського.*
Саричев Ю. О., *к.тех.н., с.н.с., провідний науковий співробітник Національного університету оборони України імені Івана Черняховського.*
Ткаченко В. А., *к.військ.н., начальник відділу Національного університету оборони України імені Івана Черняховського*

АКТУАЛЬНІ ПЕРЕДУМОВИ НЕОБХІДНОСТІ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА УКРАЇНИ

Статтею 17 Конституції України визначено, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу. Про інше стосовно інформаційної сфери в Конституції України не йдеться. У зв'язку із цим можна стверджувати, що інформаційна політика України має бути спрямована на реалізацію якраз цієї конституційної функції, а не будь-якої іншої. В той же час поняття державної інформаційної політики України не визначене чинним законодавством України. Тому її базовий наратив, яким, на наш погляд, має бути забезпечення інформаційної безпеки держави, не звучить та не імплементується у наслідкових законодавчих і нормативно-правових актах та практичній діяльності, що порушує системність у державному управлінні інформаційною сферою. Зазначене вже є приводом для удосконалення інформаційного законодавства України, але важливо розглянути цю проблематику у деяких деталях, зокрема з позиції забезпечення інформаційної безпеки держави.

Зауважимо, що в законодавчому полі України також відсутній рамковий закон про інформаційну безпеку держави, а законодавство визначило сутність інформаційної безпеки лише в "тілі" Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" [1], ніяк не рамкового по відношенню до всеохоплюючого феномена інформаційної безпеки держави. Іншого тлумачення цього визначення в законодавчих актах України немає, отже подальші теоретичні напрацювання та практичні дії, у тому числі законо- та нормотворчість, повинні опиратися на це визначення. Нажаль, в Україні цього немає, про що свідчать численні приклади, які узагальнено розглянемо.

Так, останнім часом, зокрема і під впливом військової агресії Російської Федерації, в законодавчому полі України прискорено з'явилася низка важливих

актів, покликаних, поряд з іншим, покращити інформаційне законодавство України щодо забезпечення інформаційної безпеки держави, серед яких Стратегія національної безпеки України [2], Воєнна доктрина України [3], Стратегія кібербезпеки України [4], Доктрина інформаційної безпеки України [5], Закон України "Про основні засади забезпечення кібербезпеки України" [6], Стратегічний оборонний бюлетень України [7] та ін. Разом з тим, імплементація основних положень цих актів в практичну інформаційну діяльність свідчить, що існують об'єктивні методологічні проблеми, які пов'язані із наявністю суперечливих норм у цих чинних актах України, зокрема щодо базових понять в інформаційній сфері, з причини, здебільшого, суб'єктивного розуміння їх розробниками сутності самої інформаційної безпеки. Це свідчить про ігнорування законодавчого визначення сутності інформаційної безпеки, що гальмує загальний процес створення повноцінної теорії цієї предметної області та не дозволяє в сучасних динамічних умовах протікання інформаційних процесів найбільш раціонально втілювати в життя практичні заходи, в тому числі сприяти розвитку інформаційного законодавства держави з єдиних позицій. Таким чином, окреслюється актуальне проблемне питання становлення інформаційного законодавства України – недосконаліть та нестабільність термінологічної бази як основи будь-якого законодавчого акту.

Сьогодні, на жаль, продовжує існувати неоднозначність у формулюванні сутності одних і тих же термінів з питань забезпечення інформаційної безпеки і в науковому середовищі, про що, зокрема, свідчить найбільш пізній авторизований тематичний словник [8], у якому досить часто зустрічається множинне тлумачення одного ж терміну. Цей стан в теоретичному секторі є ознакою загальної недосконалості напрацьованої термінологічної бази інформаційної сфери, наслідком чого практична діяльність дезорієнтується, що призводить до довільного розуміння та використання термінів, їх ситуативної модифікації, ігнорування у випадках, коли таке недоцільне. Особливо негативні наслідки таке ставлення матиме у випадку формування чи розвитку теорії і практики за напрямами державної інформаційної політики, що концентровано визначається нормами національного законодавства.

На підтвердження зазначеного стану розглянемо характерні особливості існуючої законодавчої та нормативно-правової бази, зокрема щодо термінології, на прикладі фундаментального поняття "інформація" як єдиного для сфер біологічної, технічної та соціальної [9], яке власне є кореневим в проблематиці інформаційної безпеки в її широкому розумінні. Це поняття зустрічається принаймні у трьох нині чинних загальнодержавних документах прямої дії [10 – 12], проте усі визначення терміна "інформація" є різними, що, зокрема, є найбільш яскравим свідченням термінологічного нігілізму, характерного сьогодні для усієї інформаційної сфери в Україні. Причиною такого стану можна вважати довільне розуміння терміна

“інформація” та його плутанина з іншими спорідненими з ним поняттями: “відомості” та “дані”. Тому у визначеннях терміну “інформація”, які містяться у цих законодавчих актах, фактично відсутні ознаки, характерні для інформації [13]. Отже, ці усі визначення терміну “інформація” є некоректними та потребують суттєвого уточнення і єдиного формулювання.

Вагомою причиною стану неналежної визначеності у законодавстві України поняття “інформація” як базової категорії для усієї інформаційної сфери слід вважати вільне ставлення як теоретиків, так і практиків до цього поняття, визначень якого зустрічається кілька десятків у фаховій літературі, що спричинене певними теоретичними і світоглядними позиціями різних авторів. Цей стан відкриває широкі можливості для маніпуляцій, в тому числі в інформаційному законодавстві України. Практичним наслідком є те, що за різними напрямами забезпечення інформаційної безпеки України розуміння сутності інформації, як правило, неоднакове. Це призвело до труднощів системного характеру, пов’язаних із неузгодженістю на загальнодержавному рівні позицій різних зацікавлених сторін, що не дозволило вибудувати в Україні єдину та чітку державну інформаційну політику і механізми її реалізації, зокрема з питань забезпечення інформаційної безпеки. Більше того, у чинному законодавстві України з питань регулювання інформаційної сфери відсутні визначення окремих важливих інформаційних понять, а ті, що присутні, часто-густо є недосконалими та потребують уточнення. Це, зокрема, стосується багатьох взаємопов'язаних понять інформаційної сфери: “державна інформаційна політика”, “інформаційний ресурс”, “інформаційна безпека”, “загроза інформаційній безпеці”, “кібернетична безпека”, “кіберзагроза”, “кіберпростір”, “кіберудар”, “стратегічні комунікації” тощо.

Із-за суперечливих норм у чинних законах України щодо базових понять в інформаційній сфері наступні нормативно-правові акти, що регулюють питання, зокрема інформаційної безпеки держави, розроблялися, скоріш за все, виходячи із суб’єктивного розуміння як сутності інформації, державної інформаційної політики, так і власне інформаційної безпеки або шляхом не зовсім вдалого калькування зарубіжного досвіду. З причини зазначеного в Україні маємо новітню практику адміністративного (формального) розмежування інформаційної та кібернетичної сфер в нормативно-правовій базі України, що функціонально (фізично) реалізувати неможливо, а для практики є недопустимою методологічною помилкою. При цьому в Стратегії національної безпеки України [2], зокрема, не уточнено поняття інформаційної безпеки України, а також не показано взаємовідношення інформаційної безпеки та кібербезпеки України, а інші чинники, що можуть бути серед стратегічних загроз для інформаційної безпеки України з невідомих причин у цій Стратегії відсутні, хоч вони реально існують.

Наслідком вищезазначеної методологічної помилки стало введення в чинне законодавче поле України ряду принципових положень державних актів [2 – 5], суперечливих за змістом для інформаційного законодавства держави. Суперечливість положень названих актів полягає, по-перше, у відсутності їх підпорядкованості єдиній державній інформаційній політиці, яка в Україні, як зазначено вище, ще не визначена на законодавчому рівні, а отже несформована, а по-друге, у слабкості термінологічної бази як теоретичної основи сутності нормативних положень, викладених у цих документах.

Подібні особливості і порівняння можливо продовжити. При цьому заради справедливості слід зауважити, що ряд термінологічних понять зазначених документів є самодостатніми і вони можуть бути офіційно стандартизовані та впроваджені в теорію і практику забезпечення інформаційної безпеки України. Покращення існуючого стану потребує законодавчого визначення сутності державної інформаційної політики України на основі чіткого і коректного понятійного апарату та уточнення напрямів її реалізації, головним із яких має бути забезпечення інформаційної безпеки держави. Вищенаведене сьогодні спричиняє загальнотеоретичні передумови необхідності удосконалення чинного законодавства України, передусім в інтересах забезпечення інформаційної безпеки держави.

Список використаних джерел:

1. Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” від 09.01.2007 р. № 537-V // Законодавство України [Електронний ресурс]. – Режим доступу: http: // zakon3.rada.gov.ua.

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу: http: // zakon5.rada.gov.ua.

3. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 р. № 96/2016 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

4. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 р. № 47/2017 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

5. *Закон* України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 р. № 2163-VIII // Законодавство України [Електронний ресурс]. – Режим доступу: http: // zakon2.rada.gov.ua.

6. Воєнна доктрина України, затверджена Указом Президента України від 24.09.2015 р. № 555/2015 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

7. Стратегічний оборонний бюлетень України, затверджений Указом Президента України від 20.05.2016 р. № 240/2016 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

8. Попова Т. В. Стратегічні комунікації: словник / Т. В. Попова, В. А. Ліпкан / За заг. ред. В. А. Ліпкана. – К.: ФОП О.С. Ліпкан, 2016. – 416 с.

9. Словарь по кибернетике: Св. 2000 ст. / Под ред. В.С. Михалевича. 2-е изд. – К.: Гл. ред. УСЭ им. М.П. Бажана, 1989. – 751 с.

10. Закон України "Про інформацію" в редакції від 13.01.2011 р. № 2938-VI // Законодавство України [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua.

11. Закон України "Про телекомунікації" від 18.11.2003 р. № 1280-IV // Законодавство України [Електронний ресурс]. – Режим доступу: http: // zakon2.rada.gov.ua.

12. Державний стандарт України. Автоматизовані системи. Терміни та визначення. ДСТУ 2226-93. – [Чинний від 1994 – 07 – 01]. – К.: Держстандарт України, 1994. – 91 с.

13. Воройский Ф.С. Информатика. Энциклопедический словарь-справочник: Введение в современные информационные и телекоммуникационные технологии в терминах и фактах / Ф.С. Воройский . – М.: ФИЗМАТЛИТ, 2006. – 768с.

----------*----------**

Соснін О. В., *д. п. н., професор, засл.діяч науки і техніки України, Інститут держави і права ім. В. М. Корецького Національної академії наук України, , член Ради ветеранів КПІ ім. Ігоря Сікорського.*

ПРО ПОТРЕБУ ТЕРМІНОВО ОСЯГНУТИІ ВРАХУВАТИ В ПРАВІ ЗАГРОЗИ НОВОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ РЕАЛЬНОСТІ

Для кожної держави завжди було принципово важливим створити безпечні умови для ефективної інформаційно-комунікаційної діяльності своїх громадян і тому виконанню державою інформаційно-комунікаційної функції приділяється така увага.З появою комп'ютерів і новітніх інформаційно-комунікаційних технологій суттєво розширились можливості і одночасно загострилисяпроблеми такої діяльності, яка значним ступенем стала віртуальною. Як наслідок, наприкінці ХХ століттяу людства з'явилася гостра потреба у суттєвомукоригуванні існуючих адміністративно-правових норм її регулювання, змін в інформаційно-комунікаційномузаконодавстві, з'явилося – «комп'ютерне право» або «правова кібернетика».

Віртуальне інформаційно-комунікаційне середовище, або кіберпростір, про який ми сьогоднібагато говоримо, виокремлюємо йогояк надважливий сектор в структурі проблем науково-технічної і освітньої діяльності,

державотворення і державного управління.Воно більш за все вимагає нашої уваги, оскільки в ньому відбувається перетворення інформації в ресурс розвитку, який підпорядковано вирішенню завдань оновлення інженерного корпусу країни, його науково-технічних знань, освіти і інноваційної діяльності.

Кіберпростірвже виявив певні характерні особливості, які обумовлюють нові погляди на свободи і обмеження в правах для громадян. Інтегруючи в собі здобутки цивілізаційної діяльності людства іокремо науково-технічних осередків, уявлення про його можливостісьогодні бурхливо розвиваються.

Внаслідок багатьох причин комп'ютерне право у нас розпорошено в класичних галузях права, передусім в адміністративному. Невирішеність багатьох питань в інформаційно-комунікаційній сфері, безумовно, гальмує наш інноваційний розвиток і ускладнює інтеграційні процеси із іншими країнами. Реально ми бачимо, що недосконаліть наших уявлень про інформацію в площині правових відносинз появою новітніх засобів комунікації постійно генерують все нові й нові загрози, інформаційний тероризм зокрема тощо. Загрози паралізують або знищують /унеможливлюють функціонування багатьох інформаційно-комунікаційних систем в державних і науково-освітніх інституціях, дискредитують владу, звинувачуючи її у бездіяльності, тощо. Як наслідок, доводиться констатувати, що на сьогодні українське законодавство і юридична практика в сфері регулювання інформаційно-комунікаційної діяльності не відповідає вимогам часу, хоча від ефективності його роботи багато в чому залежить контроль над класичними середовищами, в яких діє наша держава. Власне їх диктує науково-технічний прогресі йому притаманна якісно нова властивістьдвоїстість – як середовище воно виступає як об'єкт і суб'єкт одночасно.

Ідеї і інформацію, яку генерує і накопичує, науково-технічне співтовариство в процесі створення нових технологій і зразків техніки, ми, нажаль, довго сприймали легковажно, невміючи їх належним чином оцінювати і захищати як надбання і ресурс для інноваційного розвитку.

Існує чимало наукових і практичних думок/міркувань щодо сенсунауково-технічної діяльності. Незаперечним серед них є таке, що це діяльність підпорядкована меті постійного інженерно-технічногодомінування країни, оновленнясвоєї реальної економіки і політики заради підтримки необхідного рівняобороноздатності в різних просторових вимірах – сухопутному, морському, в новітній час – повітряно-космічному і інформаційно-комунікаційному. Є підстави стверджувати, що вонає умовою забезпечення цілісності і загального стабільного розвиткубудь-якої країни і це давно стало аксіомою державотворення високорозвинених країн, однією з найважливіших характеристик якості їх життя і розвитку економік.

Проблеми ефективного використання/застосування новітніх знань в умовах комп'ютерної доби тісно пов'язано із захистом інформації. Самі по собіпроблеми мають більш широкий діапазон завдань порівняно із звичними традиційними способами захисту документованої інформації на паперових носіях, оскільки до суто технологічних мають величезне психологічне і політико-правове наповнення.

Взагалі право на володіння інформацією – інформаційне право (*InformationLaw або Law, RelatingtoInformation*), формувалося протягом всього розвитку нашої цивілізації, але з появою комп'ютерів проблема загострилася і вже в перших наукових публікаціях з проблем комп'ютерної безпеки стало зрозумілим, що з появою електронно-обчислювальної техніки і активного використання її в системах комунікації людство зіштовхується із новими викликами, які треба вирішувати на межі правових і технічних наук.

Інформаційне право виникало і формувалося не само по собі, а в координатах вимог науково-технічних і технологічних реалій створенняновітніх засобів комунікації. Економічна глобалізація світу, наочно висвітлила постійно зростаючий рівень їх складності, оскільки, скажімо, цифрове зберігання і методи обробки інформації постійно революціонізують, змушуючи нас постійно вдосконалювати законодавчі і нормативно-правові акти роботи з нею. Скажімо, з появою комп'ютерів в новітніх засобах комунікації з'явилася така критична загроза для людства як інформаційно-комунікаційна злочинність і навіть тероризм, іна них треба було адекватно реагувати. Розбудова безпекових засад інформаційно-комунікаційного середовища вже стала загальносвітовою суспільно-політичною проблемою, зв'язавши захист комп'ютерної інформації із самою умовою інноваційного розвитку суспільств. Все це підкреслює, що інформаційне суспільство є істотно більш вразливим за індустріальне по відношенню до інформаційних впливів.

Вивчення проблем розвитку інформаційно-комунікаційної діяльності, безумовно, є надзвичайно цікавим науковим процесом, оскільки актуалізувало багатопотреб в інженерно-технічній освіті і діяльності інженерного корпусу в умовах ринкової економіки. Зокремавимагають вирішення питання перетворення змістовної інформації в інформаційний ресурс розвитку України, що вимагаєзмін в національномуінформаційно-комунікаційному законодавстві, всебічної ревізії положень національної програми інформатизаціїі навіть радикальних змін в системі адміністративно-правового регулювання інформаційно-комунікаційної діяльності.

Проблеми державного управління системою національних інформаційних ресурсів з науково-технічного потенціалу України стають на сьогодні виключно актуальними.Безумовно, на сьогодні вони мають стати предметом наукових досліджень в багатьох галузях знань і, зокрема, для кафедр НТУУ «Київський

політехнічний інститут ім. І. Сікорського», які плідно співпрацюютьз науково-освітніми осередками багатьох країн світу і мають можливість привнести досвід такої роботи. Вивчення і систематизація такого досвіду, безумовно, нададуть нового імпульсу не тільки для розвиткунаукових і освітніх процесів, а й в розбудові нових суспільно-політичних відносин в країні.

----------***----------

Сніцаренко П. М., *д. т. н, с.н.с., провідний науковий співробітник Національного університету оборони України імені Івана Черняховського.*
Саричев Ю. О., *к. т. н., с.н.с. провідний науковий співробітник Національного університету оборони України імені Івана Черняховського.*
Хоменко Л. В., *науковий співробітник Національного університету оборони України імені Івана Черняховського.*

МЕТОДИКА ВИЯВЛЕННЯ ТА ОЦІНКИ НЕГАТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА ОСОБОВИЙ СКЛАД ЗБРОЙНИХ СИЛ УКРАЇНИ

Останнім часом в передових державах світу накопичено значний науковий потенціал та практичний досвід проведення інформаційних операцій, акцій, атак і актів при вирішенні завдань у ході воєнних конфліктів, коли об’єктом інформаційно-психологічного впливу є людина, особливо особовий склад збройних сил (військових формувань) противника. Тому для України протидія такому впливу, тим більше в період військової агресії з боку Російської Федерації, коли його наслідки гостро та відчутно проявилися, зокрема на особовому складі Збройних Сил України (далі ЗС України), є актуальним завданням першорядного значення, у першу чергу в інтересах забезпечення високого рівня морально-психологічного стану військ (сил).

Аналіз показує, що на сьогодні теорія протидії негативному зовнішньому інформаційно-психологічному впливу обмежена на рівні концептуально-декларативних положень, а тому для практики є недосконалою. У ній бракує чітких формальних методів і методик для кількісних оцінок певних аспектів цієї сфери, у тому числі щодо виявлення та оцінки рівня такого впливу на особовий склад ЗС України. З цієї причини його кількісна оцінка не проводиться, а оцінка морально-психологічного стану ЗС України, який є наслідком і такого впливу, здійснюється за якісними показниками на основі результатів моніторингу у військових частинах та підрозділах відповідно діючих інструкцій [1], тобто

постфактум до наслідків різних впливів. Зазначене означає, що реально підсистема виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України відсутня, а це унеможливлює проведення, зокрема, випереджувальних заходів протидії для стабілізації морально-психологічного стану військ (сил), що вкрай необхідно.

Найбільш ефективна протидія такому впливу повинна реалізуватися за кібернетичним принципом управління [2], де об'єктом управління є рівень морально-психологічного стану особового складу ЗС України. За законами кібернетики стійкість управління забезпечується наявністю, так званих, "прямого" і "зворотного" зв'язків. Тому, зважаючи на це, а також приймаючи до уваги ту обставину, що рівень морально-психологічного стану ЗС України спричиняється як негативним інформаційним впливом, так і його компенсаторами, загальна кібернетична схема (модель) такого соціального управління матиме вигляд, як представлено на рис.1.

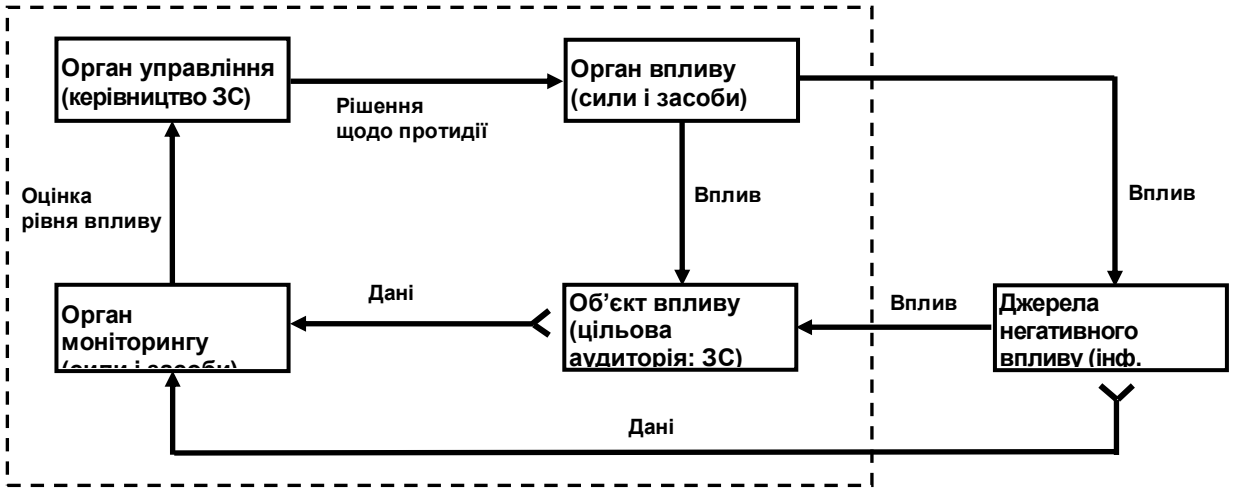

Рис.1. Кібернетична модель реалізації протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил).

Принципово важливим в контурі такого управління має бути процес своєчасного і достовірного виявлення та оцінки рівня негативного інформаційно-психологічного впливу на визначену цільову аудиторію (в нашому випадку ЗС України). Таким чином, випливає проблемна потреба в постійному підтриманні дієздатності механізму для здійснення такого моніторингу та створення відповідної підсистеми.

Пропонується методологічний підхід до створення підсистеми моніторингу інформаційного простору для виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України, який базується на основі відповідної методики, за допомогою якої визначаються необхідні кількісні показники впливу [2]. Ця методика забезпечує можливість

своєчасно та кількісно оцінити рівень такого негативного впливу на особовий склад ЗС України, а також зрозуміти тенденцію до його зміни, що якраз і дозволяє реалізувати кібернетичну модель системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) та випереджено реагувати на розвиток негативного інформаційного процесу.

Особливості цієї методики полягають у наступному:

1.класифіковано та зведено в єдиний реєстр найбільш характерні види інформаційних процесів (дій, фактів), які можуть впливати на свідомість, а отже, на морально-психологічний стан військовослужбовців;

2.визначено "вагу" кожної класифікаційної позиції за видами інформаційних процесів;

3.рівень впливу визначається через "зважену" інтенсивність сукупного інформаційного процесу, що спостерігається в інформаційному просторі держави та доступного до особового складу збройних сил;

4.частковими показниками негативного інформаційно-психологічного впливу на особовий склад військ (сил) можуть бути наведені (на рис.2) рівні інтенсивності сукупного інформаційного процесу:

5.експериментальним та експертним методами визначено діапазон "вагової ціни" кожного часткового показника негативного впливу на особовий склад ЗС України за період спостереження інформаційних процесів в інформаційному просторі України ΔT = 1 рік (опорна шкала, критерії χ_1, …, χ_5).

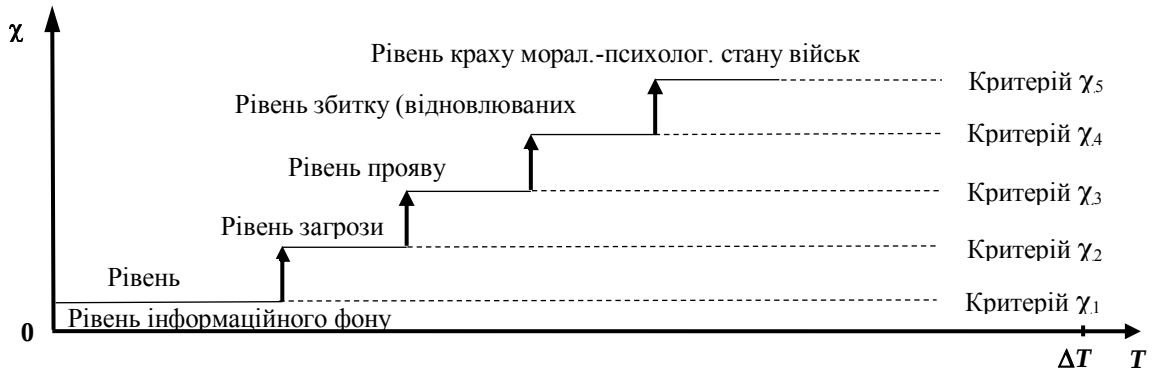

Рис. 2. Динаміка ескалації інтенсивності загального деструктивного інформаційного процесу

Отриманий результат дозволяє доволі просто реалізувати методику виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України шляхом процедури масштабування в часі спостереження, тобто через набір статистики інформаційних процесів та їх обробки не за період ΔT = 1 рік, а за значно менший термін Δt ($\Delta t << \Delta T$), наприклад за місяць чи тиждень, та їх приведення до часу ΔT = 1 рік.

Висновки.

1. Застосування вищенаведеного теоретичного підходу дозволяє реалізувати методику, яка створює можливість оцінити в кількісному вимірі рівень інформаційно-психологічного впливу на особовий склад збройних сил за відносно короткий проміжок часу. Це забезпечить створення умов для відповідного органу військового управління аби найбільш об'єктивно прогнозувати можливі наслідки та адекватно і на випередження реагувати (протидіяти) на негативні процеси.

2. Запропоновану методику слід розглядати як невід'ємний елемент підсистеми моніторингу ситуації у загальному кібернетичному контурі системи протидії негативному інформаційно-психологічного впливу на особовий склад, зокрема ЗС України, – головному механізмі управління процесом стабілізації морально-психологічного стану військ (сил).

3. Запропонований методичний підхід має універсальний характер, а тому може бути застосований при розробці аналогічних методичних засобів не лише стосовно воєнної сфери, але і до усієї соціальної системи держави, включаючи людський фактор органів державного управління, зокрема в інтересах забезпечення внутрішньополітичної стабільності.

Список використаних джерел:

1. Методичні основи виявлення та оцінки негативного інформаційно-психологічного впливу на особовий склад військ (сил) / П.М. Сніцаренко, Ю.О.Саричев, Ю.І. Михєєв, М.В.Праута // Наука і оборона. – № 3-4. – 2017. – С. 18-25.

2. Наказ ГШ ЗС України від 29.04.2017 № 153 "Про затвердження Інструкції з оцінювання морально-психологічного стану особового складу ЗС України" (зі змінами, внесеними наказом ГШ ЗС України від 16.08.2017 № 287).

----------***----------

Колотило М. О., *к. ф. н., викладач кафедри філософії КПІ імені Ігоря Сікорського.*

БЕЗПЕКА І СВОБОДА ОСОБИСТОСТІ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Світове суспільство нині перебуває на шляху трансформації, модернізації та важливих соціально-політичних змін, в результаті яких відбувається переосмислення усіх сфер його життєдіяльності. Ми є свідками переходу суспільства до цілковито іншого етапу в своєму розвитку – інформаційного, що характеризується, з одного боку, новими функціональними можливостями, з іншого – суттєвими потрясіннями для системи суспільних відносин в ньому.

Результат цих процесів може негативним чином вплинути на індивідуальну безпеку особистості, що закономірно відобразиться на її соціетальному рівні, а тому актуальним стає питання захисту прав та інтересів особистості в суспільстві, особливу роль у забезпеченні яких традиційно відіграє політичний інститут держави.

Дослідження моделі «інформаційне суспільство» та співвіднесення його з моделлю «суспільство, базоване на Інтернет-технологіях» демонструє низку протиріч в їх сутності та механізмах функціонування. Якщо взяти до уваги уявлення більшості теоретиків концепції інформаційного суспільства (Д. Белл, А. Турен, Е. Тофлер, М. Маклюен, З. Бжезінський), то увиразнюються три основоположні критерії інформаційного суспільства: наукове знання як провідний фактор суспільного життя; рівень знань як ознака соціальної диференціації (на відміну, від власності в індустріальному суспільстві); «симбіоз» соціальної організації та інформаційних технологій.

Моделі інформаційного суспільства, запропоновані вищезазначеними дослідниками, виявилися актуальними у визначенні сучасної соціальної дійсності насамперед тому, що їх автори ототожнювали інформацію і знання. Проте сучасний інформаційний простір заснований не на знанні, а на комунікації та інтерпретації. Безпосередній факт не несе смислового навантаження, натомість значущості набуває його інформаційне представлення та подальша трансляція учасникам інформаційного обміну. Отож, Інтернет-середовище у функціональному вимірі не стільки створює нове знання, скільки багатократно збільшує можливості здійснення комунікацій.

Людина усе більше занурюється у віртуальне середовище, характерною рисою якого в антропологічному аспекті стає принципова відсутність тілесності. І оскільки кожен творець «віртуальної особистості» зазвичай лишається анонімним, то постає питання про можливість стверджувати факт існування такої «особистості» як особистості? Життя людини у віртуальному світі трансформується в набір створених нею ж ролей (аватарів), що несе реальну загрозу втрати особистістю власної ідентичності.

Питання відсутності/недостатності механізмів регулювання електронного підприємництва у віртуальній мережі, методів боротьби з кіберзлочинністю, що несуть безпосередню загрозу для безпеки особистості, є дійсно актуальним та широко обговорюваним на різних дискусійних майданчиках. Разом з тим, сам по собі Інтернет як технічний засіб є етично нейтральним, оскільки може застосовуватися для розкриття творчого потенціалу особистості, розширення меж її свободи у процесі самореалізації тощо. Вочевидь, проблема є поліаспектною за змістом та потребує застосування багатовимірного підходу до свого осмислення.

Почнімо зі з'ясування особливостей функціонування сучасного інформаційного простору, що, відповідно до філософської традиції, онтологічно пов'язане з феноменом віртуального. Спроби створення філософських моделей опису сучасності на базі концепту віртуальності були здійснені практично одночасно німецькими дослідниками А. Бюлем та М. Паетау, а також канадськими фахівцями А. Крокером та М. Вайнштейном.

Теорія віртуального суспільства **Ахима Бюля**, представлена в роботі ***«Віртуальне суспільство. Економіка, політика та культура під знаком кіберпростору»***, постулює те, що з розвитком технологій комп'ютери з виключно обчислювальних машин перетворилися в універсальні пристрої, що створюють «дзеркальні світи» віртуальні аналоги усіх підсистем сучасного суспільства. Німецький дослідник стверджує, що саме вони визначають функціонування «віртуального суспільства», простір якого конституює новий віртуальний спосіб виробництва, а той в свою чергу формує класову і соціальну структуру дійсного суспільства [2].

Теорія віртуалізації **Артура Крокера** та **Міхаеля Вайнштейна**, представлена в роботі ***«Відходи інформації. Теорія віртуального класу»*** доводить багатоаспектний вплив віртуальної реальності на сучасні трансформаційні процеси в суспільстві, та безпосередньо пов'язує його з появою низки загроз для безпеки особистості в інформаційному просторі. Зміст концепції може бути представлений наступним алгоритмом: формування нового віртуального класу «кіберкапіталістів» (власників компаній, що створюють і застосовують комп'ютерні технології) перетворення віртуальної реальності «віртуальною виробничою силою» в капітал розвиток віртуального капіталу, сформованого на базі віртуальної ідеології, через професійну діяльність особистості дійсна загроза відчуження людини від дійсності в умовах занурення в штучно сконструйовану реальність [2].

Модель «віртуалізації соціального» **Міхаеля Паетау**, базована на теорії суспільства як системи комунікацій німецького філософа Н. Лумана, постулює виникнення гіперпростору віртуальної мережі в результаті «використання» суспільством нових форм комунікації для самовідтворення «аутопоєсиса» (термін Н. Лумана). Німецький дослідник серед іншого зазначає, що суспільство використовує нові форми комунікації для самовідтворення, а останні в свою чергу впливають на суспільство, здійснюючи внесок у виробництво соціальності. Очевидною постає суттєва загроза безпеці особистості неконтрольованість переходу віртуальних комунікацій в простір соціальної дійсності[2].

На сьогодні у науковому дискурсі існує декілька традицій розгляду проблеми безпеки особистості в інформаційному суспільстві: теорії, що пов’язують поняття безпеки з обмеженням особистої свободи індивіда;

ліберальні теорії безпеки, що постулюють повну свободу людини в інформаційному просторі.

Згідно з першим підходом, безпечну поведінку особистості можливо визначити як санкціоновану можливість останньої в правових межах/межах суспільних норм реалізувати себе в тій чи іншій сферах при умові наявності гаранта у формі суспільства чи держави. Таким чином, декларованe право на безпеку передбачає наявність обмежувачів особистої свободи, що сприяє його здійсненню. Показовим прикладом подібного роду теорій в інформаційному суспільстві є ***«Декларація прав цифрової людини»*** **Андре Сантіні** [3], в якій серед іншого зазначається, що не протиставлення державі, а співпраця з нею, в тому числі через відмову від принципу індивідуальної свободи заради безпеки роботи в цифровому просторі, має гарантувати свободу індивіда.

Натомість ліберальні теорії безпеки особистості постулюють її повну свободу в інформаційному просторі через неможливість здійснення жодного контролюючого/регулюючого впливу на принципи та засади функціонування останнього. Зокрема, концепція **Джона Перрі Барлоу**, представлена в роботі ***«Декларація незалежності кіберпростору»*** [1], вказує на те, що в кіберпросторі організуючим принципом культурного життя людини стає принцип трансформації (перманентного хаосу), і свобода особистості виступає гарантом безпеки самого індивіда в ситуації наростання розриву між умовами реального світу й можливостями закону по їх регулюванню.

Інструментально концепція П. Барлоу дозволяє протистояти «електронному тоталітаризму», проте її основна ідея подолання цифрової нерівності та досягнення електронної демократії, на даний час залишається нездійсненною. Утопічність концепції в її праксеологічному вимірі підтверджується низкою актуальних загроз безпеці особистості у віртуальному світі, до числа яких слід віднести: проблему суспільної нерівності у доступі до інформаційних ресурсів; поширення в мережі інформаційних матеріалів, що дезорієнтують особистість в реальному світі; поширення маніпулятивного контенту, використовуваного для нав’язування певного образу та стилю мислення (формування «інформаційних зомбі») тощо.

В який же спосіб можливий захист особистості в інформаційному просторі від втрати нею своїх прав та свобод? Адже в погоні за невпинним технологічним прогресом важливо «не проглядіти» особистість, її право на безпеку, з однієї сторони, та свободу дій з іншої. На сьогодні проблема подолання протиріччя між свободою особистості та її безпекою в інформаційному просторі стає ключем до розуміння вектора подальшого суспільного розвитку. Держава та суспільство покликані здійснювати захист вітальних інтересів людини, її основних прав і свобод. Більше того, функція правової держави саме й полягає в забезпеченні гарантій цих прав і свобод з

використанням принципу «розумної достатності», зміст якого полягає у недопущенні як загроз для безпеки суспільства та держави, так і диктату по відношенню до окремої особистості.

З наукової точки зору обидві теорії мають право на розвиток, але чи може котрась з них стати універсальним засобом сказати доволі складно. «Закрити» питання щодо прав та безпеки особистості в інформаційному просторі на рівні держави, що є властивим для частини пострадянських країн, звісно простіше аніж звертатися до людини, проте чи відповідає це сучасним загальнолюдським цінностям? Концепція ліберальної безпеки більшою мірою реалізована в країнах Західної Європи, де з багатьох причин, і в першу чергу завдяки уже досягнутому рівню безпеки, людині простіше зорієнтуватися у питаннях інформаційного захисту і особистої свободи. Ця концепція була виплекана інтелектуальною елітою, і тому можливо слід шукати відповідь в соціалізації особистості «безпечного типу», в культурному та моральному розвитку суспільства?

Список використаних джерел:

1.Барлоу Ж. Декларация независимости киберпространства [Электронный ресурс] http://www.telecomlaw.ru/articles/declaration.html

2.Иванов Д. Виртуализация общества / Д. Иванов. Санкт-Петербург: Петербургское востоковедение, 2000. 96 с. [Электронный ресурс] - http://lib.ru/POLITOLOG/ivanov_d_v.txt

3.Santini A. Declaration of the digital human rights [Electronic resource] http://www.ddhn.org/index-en.html

----------***----------

Цирфа Г.О., *к.і.н., доцент кафедри господарського та адміністративного права ФСП КПІ ім. Ігоря Сікорського.*

КОМЕРЦІЙНА ЦІННІСТЬ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

В Україні термін «комерційна таємниця» у правовий обіг був введений із прийняттям 27 березня 1991 року Закону «Про підприємства в Україні». Як відомо цей закон втратив чинність з прийняттям у 2003 році Цивільного і Господарського кодексів і набуттям їх чинності з 1 січня 2004 року.

З того часу до відповідних законодавчо-нормативних актів було внесено багато змін, проте і на сьогодні в українському суспільстві немає впевненості у захисті як персональних даних так і комерційних, пов’язаних із цінною інформацією.

Не дивлячись на те, що на міжнародному рівні важливе значення у регулюванні захисту комерційної таємниці відіграють Угода ТРІПС та деякі

інші важливі міжнародні стандарти, зокрема, Регламент № 772/2004 від 24 квітня 2004 року, в державах – членах Європейського союзу на сьогодні існують значні відмінності в правових системах. Інформаційні об'єкти, що являють собою комерційну цінність у різних країнах мають різні визначення. Рівень надійності захисту від незаконного заволодіння, використання і розголошення комерційних таємниць в кожній країні залежить від різних чинників і, в першу чергу, від державно-політичних та економічної моделі господарювання.

8 червня 2016 року Європейський Парламент та Європейська Рада прийняли Директиву 2016/943 (далі Директива) про захист нерозголошених «ноу-хау» та комерційної інформації (комерційні таємниці) від незаконного заволодіння, використання та розголошення [1].

За цією Директивою (ст. 2) під «комерційною таємницею» розуміється інформація, що відповідає всім зазначеним нижче вимогам, а саме: – є таємницею у тому сенсі, що не є відомою чи доступною для кола осіб, які, як правило, обізнані з інформацією подібного характеру; – має комерційну цінність, оскільки є таємницею; – з обґрунтованих підстав є такою, що має триматися у таємниці особою, яка на законних засадах здійснює над нею контроль.

До 9 червня 2018 року Держави-члени ЄС повинні привести норми національного законодавства у відповідність до вимог цієї Директиви. Та, на нашу думку, деяким державам майже не потрібно вносити зміни, оскільки їх законодавство практично відповідає вимогам Директиви 2016/943. Так, захист комерційної таємниці у Німеччині надійно здійснюється за кримінальними положеннями §§ 17-19 Закону про недобросовісну конкуренцію (UWG) [2], а також § 823 та 826 Цивільного кодексу (BGB) [3], як правило, у поєднанні з § 1004 BGB.

В Україні питання застосування і захисту комерційної таємниці відбувається за нормами Цивільного, Господарського кодексів та нормами інших законів, зокрема, Закону України «Про науково-технічну інформацію». Окремо слід відмітити заходи, що здійснює у цьому напрямі така державна інституція в Україні, як Антимонопольний комітет (АМКУ) за допомогою спеціального законодавства. Так, глава 4 Закону України «Про захист від недобросовісної конкуренції» має назву «Неправомірне збирання, розголошення та використання комерційної таємниці». За порушення норм (ст. 14-19) цієї глави настає відповідальність, передбачена статтями 20-24 зазначеного Закону. Також за законодавством про захист економічної конкуренції суб'єкти господарювання на вимогу АМКУ повинні надавати точну і повну інформацію, що непокоїть представників українського бізнесу. Підприємці незадоволені тим, що АМКУ має повноваження на законодавчому рівні перевіряти інформацію, в тому числі з обмеженим доступом. Проте, така інформація за Законом не

підлягає розголошенню з боку органів АМКУ. Відповідно до Законодавства України повноваження на отримання подібної інформації мають і органи слідства та суду. Та чи можна вважати що норми українського законодавства у даному випадку відповідають вимогам, що випливають з контексту ст. 2 Директиви?

Важливо звернути увагу і на інформацію, що стосується об'єктів інтелектуальної власності. Така інформація має надійний захист, якщо об'єкт інтелектуальної власності захищений у встановленому порядку за допомогою патенту або свідоцтва на певний об'єкт. Проте, в зоні риску тут залишається технічна інформація, яка не захищена патентом або свідоцтвом. Це можуть бути: технічні проекти, незапатентовані науково-технічні розробки, промислові зразки, різні види «ноу-хау», тощо. Цю проблему слід вирішувати якнайшвидше на рівні законодавства, з огляду і на те, що в Україні не існує єдиного спеціального законодавчого акта, норми якого б врегулювали питання щодо застосування та захисту комерційної таємниці. Такий стан речей вимагає продовження імплементації національного законодавства у цій сфері до відповідних європейських норм.

Відомо, що більшість норм законодавства розвинених країн дозволяють не тільки зберігати комерційні секрети, але і переслідувати тих, хто на них зазіхає. Проте далеко не в кожній, навіть розвиненій, країні існують норми, які чітко визначають що є законним придбанням інформації а що ні. У цьому повинно бути чітке розмежування.

Окремі норми Директиви мають роз'яснювальний характер. Так, з контексту ст. 20 випливає, що заходи, процедури та засоби правового захисту, передбачені Директивою, не повинні використовуватися для обмеження операцій з інформування. Тобто, захист комерційної таємниці не повинен поширюватися на випадки, коли розголошення комерційної таємниці служить інтересам суспільства та виявленню неправомірної поведінки чи діяльності.

Аналізуючи норми Директиви, наприклад, можна зрозуміти що за їх вимогами, якщо власник комерційної таємниці отримав інформацію за власним дослідженням, спостерігаючи за загальнодоступними продуктами або іншими процедурами відповідно до серйозної ділової практики, такий бізнес-секрет вважається законними. Натомість отримання інформації буде незаконним у разі несанкціонованого копіювання документів, несанкціонованого доступу до документів або порушень договорів конфіденційності.

Отже, дотримання вимог Директиви дозволить суттєво нівелювати існуючи розбіжності правового регулювання відносин, пов'язаних із застосуванням комерційної таємниці в національних законодавствах держав – членів ЄС. Україна так само повинна поступово переходити до послідовного захисту від незаконного придбання, незаконного присвоєння та розголошення

комерційної таємниці, аж до судового розгляду, де також повинні бути встановленні чіткі правила секретності, що допоможе захистити цінну комерційну інформацію сторін і в суді.

З метою наближення до створення сприятливих умов для українського бізнесу на спільному ринку Євросоюзу та на ринках країн, які визнають стандарти ЄС, Україна повинна імплементувати норми цієї важливої Директиви що дасть можливість ще на крок наблизитися до виконання зобов'язань Угоди про асоціацію між ЄС та Україною і більш надійно захистити інформаційні об'єкти, що являють собою комерційну цінність як на національному так і на міжнародному рівнях.

Список використаних джерел:

1. Директива Европейского Парламента и Совета Европейского Союза 2016/943 от 8 июня 2016 г. о защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия. – Електронний ресурс: http://base.garant.ru/ 71615160/
2. Gesetz gegen den unlauteren Wettbewerb (UWG). - Електронний ресурс: https://www.gesetze-im-internet.de/uwg_2004/BJNR141400004.html
3. Bürgerliches Gesetzbuch (BGB). – Електронний ресурс: https:// www. gesetze -im-internet.de/bgb/BJNR001950896.html

----------***----------

Ніколенко Д. М., *студентка ФСП КПІ м. Ігоря Сікорського.*
Науковий керівник: ***Фурашев В. М.,*** *к.т.н., с.н.с., доцент ФСП КПІ ім. Ігоря Сікорського.*

ЗАХИСТ КОНСТИТУЦІЙНИХ ПРАВ І СВОБОД ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ УКРАЇНИ

Розвиток інформаційних технологій призвів до виникнення нових реалій суспільного життя, коли інформація та операції з нею стали елементом прибутку. На сьогодні інформація активно використовується фізичними та юридичними особами в сімейному житті, бізнесі, політиці, творчості. Інформація є важливим продуктом, за який окремі компанії готові викласти мільярди доларів. Отож, питання захисту інформації виходить на якісно новий рівень.

Людина як біосоціальна істота не є відмежованою від соціуму, в якому інформація стала важливим ресурсом та продуктом. Щодня ми маємо справу з величезним обсягом даних, передаваючи їх банкам та фінансовим установам,

навчальним закладам та роботодавцю, провайдеру та юридичній особі, що володіє соціальною мережою. Так чи інакше, але ми ділимося частинкою інформації про себе з третіми особами, іноді не розуміючи можливі наслідки. Зрештою, ми надаємо інформацію про себе органам держави: при оформленні соціальних виплат, сплаті податків, реєстрації підприємства тощо.

Інформація про нас може бути різного характеру. Це можуть бути ідентифікаційні дані (ПІБ, вік, стать, дата народження, місце реєстрації), особисті дані (політичні, релігійні переконання, світоглядне установки, коло знайомих тощо), ділові дані (інформація про стан рахунків, доходи та витрати, зміст діяльності, раціоналізаторські ідеї, промислові зразки тощо). Отримання відомостей сторонніми особами може завдати шкоди нам як основним власникам такої інформації. Так, відомості про ноу-хау можуть бути використані конкурентами й ми втратимо прибуток, відомості про особисте життя – використані нашими ворогами, які знайдуть можливість скомпрометувати нас. Зрештою, інформація щодо стану рахунків або взагалі ключи доступу до них є загрозою для нашої фінансової безпеки. [4]

Отже, захист нашої інформації є актуальним та болючим питанням, яке лежить в площині державних функцій. Конституція України визначає інформаційну безпеку справою Українського народу, а також передбачає захист прав та законних інтересів людини в інформаційній сфері. [1]

Визначення терміну **«захист інформації»** є досить різним. У літературі цей термін визначається як сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією. [3]

Захист прав та свобод людини в інформаційній сфері має різні аспекти. На наш погляд, це поняття слід розуміти як напрям державної політики, сукупність заходів, спрямованих на забезпечення інформаційної безпеки громадян, захист їх інформації (та інформації, яка стосується таких осіб) та забезпечення права доступу до інформації. Отже, захист прав та свобод людини в інформаційні сфері, на нашу думку, складається з таких елементів:

А) право на доступ до інформації – передбачене законом право особи на отримання, користування інформацією. Особа може володіти та користуватися будь-якою інформацією, що має відкритий (публічний характер). Окрім того, особа може звернутися до розпорядника інформації із запитом на неї без роз'яснення причин. [2]

На нашу думку, право на доступ до Інформації в сучасному суспільстві має й передбачати право на доступ до Інтернету, зокрема до найбільш важливої інформації. Держава має вжити заходів щодо створення відповідної інфраструктури, аби кожен міг отримати доступ до Інтернету та важливих

ресурсів на безоплатній основі. Це є також складовою захисту прав людини в інформаційній сфері.

Б) право на захист інформації – право особи на захист даних, що знаходяться в її власності, а також даних про неї. Мова йде про захист персональної, конфіденційної інформації про особу, інформації, що складає зміст банківської інформації тощо;

В) право на інформаційну безпеку. Це поняття є досить складним та потребує окремої уваги. Законодавство України більше спрямоване на захист інформації, однак недостатньо приділяє увагу розділу інформаційної безпеки, спрямованому на захист її від руйнівного впливу інформації. Так, захист особи від маніпуляцій свідомістю, інформаційного насильства, захист людини та суспільства від інформаційного тероризму є завданнями держави на сьогодні. На жаль, цьому питанню сучасне законодавство приділяє недостатньо уваги, хоча право на захист людини від інформаційних загроз слід також усвідомлювати як захист прав людини в інформаційній сфері. [5]

Отже, у сучасних умовах захист прав людини в інформаційній сфері є досить актуальним. На жаль, чинне законодавство поки що недостатньо приділяє цьому питанню увагу. Так, положення Кримінального кодексу України щодо злочинів в інформаційній сфері є дещо застарілими та не охоплюють сучасні інформаційні загрози. Крім того, відсутній закон щодо інформаційної безпеки та кодифікований акт у сфері інформаційних відносин.

Зрештою, спрямованість законодавства виражена в бік захисту інформації, а не людини. Такі проблемні питання потребують ефективних заходів з боку держави.

По-перше, варто прийняти Інформаційний кодекс та Закон «Про інформаційну безпеку», які регламентують захист прав людини в інформаційній сфері.

По-друге, серед принципів конституційного захисту прав людини в інформаційній сфері слід передбачити спрямованість на захист людини від інформаційних загроз. Це має мати вираження у змінах до законодавствах, вжитті конкретних заходів щодо покращення державної політики у сфері протидії маніпуляції свідомістю, інформаційному насильству та інформаційному тероризму.

Зрештою, захист прав людини в інформаційній сфері має нерозривний зв’язок з інформаційно-правовою грамотністю населення. Держава має проводити тренінги, лекції, семінари, підвищувати рівень такої грамотності людей. Тоді й права людини в інформаційній сфері будуть захищені.

Список використаних джерел:

1. Конституція України [Електронний ресурс] // Відомості Верховної Ради (ВВР). – 1996. – Режим доступу до ресурсу: http://zakon5.rada.gov.ua/ laws/ show/254%D0%BA/96-%D0%B2%D1%80
2. Закон України «Про доступ до публічної інформації»
3. Наказ Ліцензійної палати Міністерства економіки України "Про затвердження Положення про порядок та умови видачі інформації з Єдиного ліцензійного реєстру" від 15 листопада 1996 року № ЛП-37
4. Єфімчук О. Проблеми захисту прав людини в інформаційному суспільстві [Електронний ресурс] // Юридична газета. – Режим доступу: http://yur-gazeta.com/publications/practice/inshe/problemi-zahistu-prav-lyudini-v-informaciynomu-suspilstvi-.html
5. Шишка Ю.М. Захист прав та свобод людини в інформаційній сфері [Електронний ресурс]. – Режим доступу: http://ippi.org.ua/sites/default/ files/14sumlis.pdf

----------*----------

Кархут О. Я., *к. ю. н., доцент кафедри теорії та історії держави і права факультету політології та права НПУ ім. М. П. Драгоманова.*

Галенко Т. М., *студентка 2 курсу спеціальності «Право» факультету політології та права НПУ ім. М. П. Драгоманова.*

КОНСТИТУЦІЙНА СКАРГА ЯК ГАРАНТІЯ ЗАХИСТУ ПРАВ ЛЮДИНИ ТА ГРОМАДЯНИНА

Становлення незалежної України як правової, демократичної держави неможливе без системи гарантій основних прав, свобод та законних інтересів людини та громадянина. У ст. 55 Конституції України передбаченотак звану юридичну гарантію, яка полягає у тому, що кожному гарантується право на оскарження в суді рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб. Також відповідно до конституційної судової реформи, яка була проведена в Україні 2 червня 2016 року до Конституції України були внесені зміни, відповідно до яких запроваджено конституційну скаргу в Україні [1].

ЇЇ зміст полягає в закріпленні на рівні Основного Закону держави права громадян, іноземців та осіб без громадянства на оскарження в суді рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб.Крім того, Закон України «Про Конституційний Суд України» було доповнено статтею 151^1:«Конституційний Суд України вирішує

питання про відповідність Конституції України (конституційність) закону України за конституційною скаргою особи, яка вважає, що застосований в остаточному судовому рішенні в її справі закон України суперечить Конституції України». Конституційна скарга може бути подана в разі, якщо всі інші засоби юридичного захисту вичерпано. Тобто, у законі здійснено посилання на те, що особа тільки тоді може подати конституційну скаргу, коли всі інші, передбачені Конституцією та законами України юридичні гарантії прав, свобод та законних інтересів були використані особою без досягнення бажаного нею результату – захисту прав та свобод.

Дослідженням проблем конституційної юстиції займались такі правники як В. Шаповал, В.Скомороха, М. Савенко, О. Марцеляк, М. Кельман, С. Д. Владиченко, О. В. Константий, Ю. Баулін та інші.

Серед основних гарантій прав людини та громадянина, які закріплені на законодавчому рівні, актуальною нині є конституційна скарга. З огляду на офіційні дані, станом на сьогоднішній день, за період з 02.01.2018 по 19.04.2018 року Конституційний Суд України отримав 142 конституційні скарги. Це свідчить про активність громадян у їх подачі та у використанні конституційної скарги саме як засобу гарантії власних основних прав та свобод[3].

Зауважимо, що конституційна скарга займає особливе місце в системі юридичних гарантій, оскільки вона передбачає відповідальність держави в особі державних органів (їх посадових осіб), органів місцевого самоврядування перед людиною та громадянином за порушення ними основних прав, свобод та законних інтересів.

Дослідники з галузі конституційного права вважають, що інститут конституційної скарги є альтернативою інтерпретаційній діяльності суду стосовно тлумачення законів України. Втім запровадження конституційної скарги втілено і доцільно було б розглянути її особливості, які б визначили її місце серед інших конституційних гарантій.

По-перше, як зазначає Ю. Баулін, запроваджена модель конституційної скарги є неповною нормативною конституційною скаргою, що пов’язана з розглядом конкретної справи. За нею оскарженню підлягає тільки один із чисельних видів нормативно-правових актів, а зокрема – закон України, який був використаний в остаточному судовому рішенні. І відповідно нормою якого порушується конституційне право особи – суб’єкта подання конституційної скарги[2].

Предметом конституційної скарги є закон або його окремі положення, який був застосований в судовому рішенні по конкретній справі судом загальної юрисдикції, апеляційним судом чи судом касаційної інстанції.

Суб’єктом права конституційної скарги, відповідно до Конституції України, є «кожний». В законі це поняття визначено як «особа», але уточнення

законодавець не надає. Зі змісту даних нормативно-правових актів ми можемо зрозуміти, що суб'єктом права на подання конституційної скарги в Конституційний Суд України є громадяни, іноземці та особи без громадянства.

Нині актуальною проблемою є реалізація особами права на конституційну скаргу. Більшість громадян подають вищезгаданий документ не дотримуючись процедури та умов подання. Відповідно до доктрини конституційного права, умовами подання громадянами, іноземцями, особами без громадянства конституційної скарги є такі положення:

1. Твердження особи про те, що закон, застосований судом при вирішенні її справи, не відповідає (суперечить) Конституції України;

2. Наявність остаточного судового рішення у справі, тобто такого рішення, яке не підлягає оскарженню, є остаточним у цій справі та обов'язковим до виконання саме стосовно тієї особи, яка звертається до Конституційного Суду із відповідною конституційною скаргою (тобто особа, яка зверталася до суду всіх трьох інстанцій, якщо це передбачено законом, відповідно до процедури, та з остаточним судовим рішенням, може звернутися до Конституційного Суду);

3. Використання автором конституційної скарги всіх інших національних юридичних гарантій та засобів захисту прав, свобод та законних інтересів. Також слід зазначити, що вимога вичерпання всіх національних способів захисту також є умовою не тільки для подання конституційної скарги, а й для звернення особи до міжнародних судових установ[2].

Таким чином, можна вважати, що конституційна скарга в Україні є важливою гарантією захисту прав людини та громадянина і найвищою в ієрархії національної системи гарантій. Основні права та свободи людини закріплені в Конституції України і є невідчужуваними та непорушними можливостями особи для нормального її існування та розвитку.Конституція України в ч. 2 ст. 3 проголошує, що 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.

На нашу думку, одним із таких засобів їх забезпечення і виступає конституційна скарга.

Список використаних джерел:

1. Конституція України : закон України від 28 червня 1996 р. № 256к/96 // Відомості Верховної Ради України. – 1996. - № 30. – Ст. 141;

2. Баулін Ю. Новий конституційний формат діяльності Конституційного Суду України: конституційна скарга [Текст] / Ю. Баулін // Право України. – Київ, 2016. – № 7. – С. 19 – 23.

3. Офіційний сайт Конституційного Суду України [Електронний ресурс] – Режим доступу: www.ccu.gov.ua

Радзієвська О. Г., *науково-дослідний інститут інформатики і права НАПрН України.*

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДИТИНИ В УМОВАХ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ

Загострення інформаційного протистояння у глобалізованому інформаційному просторі призводить до підвищення рівня інформаційних загроз для особи, суспільства та держави. Маніпулювання з інформацією стає засобом проведення спеціальних інформаційних операцій, інформаційного тиску та елементом міжнародної політики. Забезпечення інформаційної безпеки кожного громадянина за умов глобального інформаційного протистояння стає дедалі складнішим через неможливість вчасного визначення інформаційних загроз та відсутності механізмів управління ними. Така ситуація призводить до зниження рівня захищеності кожної особи в інформаційній сфері.

Складність превентивного виявлення фактів маніпулювання свідомістю не дозволяє суб'єктам забезпечення інформаційної безпеки вчасно виявляти та протидіяти подібним операціям. Особливим об'єктом маніпулятивного інформаційного впливу є свідомість дитини, як така, що знаходиться в процесі формування та становлення. Саме свідомість дитини є найлегшим для маніпулювання об'єктом, та водночас, найбажанішою ціллю, яка здатна принести суттєві дивіденди у майбутньому. Вдале маніпулювання з інформацією дозволяє не лише формувати громадську думку, впливати на формування політики у державі, управляти певними групами громадян, але й закладати необхідні патерни на майбутнє. Маючи можливість корегувати інформаційні посили під час формування особистості дитини, можна закладати бажані змісти, погляди, переконання у її свідомість. У майбутньому це дозволить управляти як індивідуальною, так і масовою свідомістю для досягнення певних цілей.

Яскравим прикладом подібної стратегії інформаційного маніпулювання у дії можна спостерігати на тимчасово непідконтрольній Україні території Донецької, Луганської областей та у Криму. Доволі часто там фіксуються випадки пропагування антиукраїнських цінностей та залучення молоді до антиукраїнських організацій, утому числі, до збройних формувань, що є порушення норм національного та міжнародного права. Інтегрування цієї молоді в українське суспільство може стикнутися з низкою складностей. Зокрема, система цінностей, закладена російською пропагандою, конфліктуватиме з культурними та національними цінностями Української держави, що призведе до культурної відособленості, соціальної ізоляції, та врешті решт до маргіналізації певних категорій громадян. Очевидно, що чим

вища кількість таких членів у суспільстві, тим вища його нестабільність та вірогідність виникнення розколів. Цілеспрямований інформаційний вплив на свідомість молоді іншою державою, або певними групами впливу всередині держави є дуже небезпечним для існування самої держави, оскільки створює фактор нестабільності системи на майбутнє.

Спостерігається також залучення вчителів та викладачів до пропаганди певних меседжів для молоді та інформаційного маніпулювання їх свідомістю, у тому числі, регламентованого на державному інституційному рівні. Підтвердженням цього є нещодавній випадок у місті Полтава, коли напередодні травневих свят місцеве управління освітою зобов'язало вчителів забезпечити явку учнів на репетицію урочистої ходи з нагоди 73-ї річниці перемоги над нацизмом у Другій світовій війні так званій акції «Безсмертний полк», яку організовує одна із політичних сил України. Це є наглядним прикладом залучення освітньої системи до пропагування певних цінностей та маніпулювання свідомістю дітей для досягнення певної мети і реалізації поставлених завдань.

Окремого вивчення та урегулювання потребує ситуація, яка виникла довкола мовного питання в освітянській сфері на Закарпатті. Позиція керівництва Угорщини щодо питання навчання в українських школах лише угорською мовою, повністю відмовившись від української, лишає молодь угорської меншини можливості продовжувати освіту у вищих навчальних закладах України та ставить під загрозу їх успішну інтеграцію в українське суспільство. Виникає ситуація, коли цілий регіон України не володіє державною мовою, не розділяє національні цінності та має низький освітній рівень. Усі ці фактори вказують на підвищену загрозу для населення цього регіону потрапити під інформаційний вплив сусідньої держави та стати об'єктом маніпулювання, а для держави є викликом національній безпеці.

Основними об'єктами деструктивного інформаційного впливу є: ідеологічно-психологічне середовище суспільства; система формування суспільної свідомості та громадської думки; система розроблення та прийняття політичних рішень; свідомість і поведінка людини; інформаційні ресурси та інформаційна інфраструктура [1, с. 29].

За Е. Богатовою і В. Константиновим особиста стійкість індивіда до різного роду інформаційних впливів – це інтегральне психологічне утворення, яке є результатом адаптації психіки людини до розширення інформаційного середовища. Стійкість індивіда до інформаційно-психологічного впливу складається з індивідуальних особливостей (інтелектуальний рівень, особливості психіки, виховання, досвід, мислення, вік та інше.) та змінюється в залежності від місця людини у соціумі та її активності у суспільно-політичному житті. Чим освіченіша особа, чим більша залученість її у суспільні процеси –

тим вищий рівень її індивідуальної інформаційно-психологічної стійкості, а відповідно, і вищий рівень убезпеченості від різного роду інформаційних впливів. [2]. Тому основним елементом убезпечення дитини в інформаційному просторі є формування її стійкості до інформаційно-психологічного впливу та маніпулювань з інформацією та активне залучення її до суспільного життя.

В рамка протидії інформаційним загрозам та убезпечення дитини в інформаційно просторі необхідно якнайшвидше створити дієву систему заходів, про які йдеться у п. 4.11 Стратегії національної безпеки України [3] з активним залучення державних інституцій та громадянського суспільства. Основну відповідальність за їх реалізацію, крім силових структур, доцільно покласти на інститути соціалізації дитини, зокрема на навчально-виховні заклади та інші структури державного та місцевого рівня. Науковим закладам слід долучитися до створення методологічних основ для проведення заходів попередження та протидії інформаційним загрозам для дитини.

Однак, описана проблема не є сугубо українською, хоча і носить більш виражений характер через протистоянням на Сході країни. Проблема маніпулювання свідомістю молоді має глобальний характер та в певній мірі є притаманною усім країнам в умовах формування інформаційного суспільства. Зокрема, на подібний факт звернув увагу генеральний директор поліції безпеки Естонії (КАПО) Арнольд Сінісалу (Arnold Sinisalu) у щорічній доповіді за 2017 рік [4]. На його думку, численні російські установи, у тому числі посольство Росії в Естонії, разом з благодійним фондом «Русский мир», намагаються впливати на молодь російської меншини, яка проживає на території держави. Особлива увага зосереджена на молоді, яка перебуває у складній життєвій ситуації. Посадовець не виключає можливості вербування підлітків для роботи на спецслужби Росії, у тому числі, із залученням до цього процесу освітніх закладів країни. На переконання Арнольд Сінісалу це призведе до того, що виросте покоління, орієнтованих на проведення кремлівської політики розколу, що заважатиме молоді інтегруватися в культурно-ціннісний простір Естонії та у подальшому може спричинити складності всередині держави.

На даний час в Україні є чітке розуміння небезпечності інформаційних та інформаційно-психологічних впливів на свідомість людини з використання сучасних інформаційно-комунікаційних засобів та масштабів цього небезпечного явища. Є також розуміння необхідності об’єднання зусиль на міжнародному рівні у справі протидії негативним інформаційним впливам на свідомість людини. Про особливості застосування спеціальних інформаційних операцій сьогодні та можливі наслідки їх застосування в умовах активного розвитку інформаційного суспільства йдеться у доповіді постійної делегації Верховної Ради України в Парламентській асамблеї НАТО «Російські підривні інформаційно-психологічні операції в соціальних медіа», представленої на

засіданні Міжпарламентської Ради Україна-НАТО 28 листопада 2017 року. Цілеспрямовані негативні інформаційні впливи можуть зашкодити психіці людини, викликати зміни її психічного чи морально-психологічного стану, призвести до тимчасової девіації у суспільній поведінці. Проте, як підкреслюється у доповіді, використання інформаційних та інформаційно-психологічних впливів на даний час застосовується у реалізації більш амбітних цілей: як то руйнування державних та міжнародних інституцій.

Подібна небезпека вимагає від держави комплексного підходу до питань забезпечення безпеки дитини в інформаційній сфері. Нагальним питанням постає необхідність розроблення Концепції інформаційної безпеки дитини в Україні, у якій повинні бути чітко відображені основні принципи забезпечення безпеки дитини в інформаційному середовищі, а також прописані пріоритетні завдання та механізми реалізації інформаційної політики у державі. Положення Концепції повинні будуватися на визнанні дітей активними учасниками інформаційного процесу, які потребують особливого піклування та захисту згідно із Законом України «Про охорону дитинства» [5], тобто особливим суб'єктом інформаційних відносин.

Серед основних принципів Концепції повинні стати:

– вільний доступ дітей до інформації та знань;

– дотримання принципу рівності в інформаційній сфері;

– відповідальність держави за дотриманням законних інтересів дітей в інформаційному середовищі;

– створення безпечного інформаційного середовища для дитини;

– виховання у дітей самостійного критичного мислення та навиків убезпечення власного інформаційного простору.

До пріоритетних завдань держаної політики щодо забезпечення інформаційної безпеки дитини слід віднести питання підвищення її інформаційної грамотності та культури, а також виховання у дітей почуття відповідальності за дії в інформаційному просторі при задоволенні своїх пізнавальних потреб та інтересів, поваги до інших учасників інформаційного процесу, до права інтелектуальної власності та авторського права. Обов'язком держави є мінімізація ризиків десоціалізації, розвитку та закріплення у суспільстві девіантних та протиправних дій через усунення факторів зовнішнього і внутрішнього маніпулювання з інформацією та активної протидії негативним інформаційним впливам на несформовану дитячу свідомість.

Положення Концепції інформаційної безпеки дитини повинні враховуватися при формуванні та реалізації інформаційної політики як в Україні так і на міжнародному рівні, а також у законодавчому процесі та при реалізації програм щодо забезпечення інформаційної безпеки у державі.

Результатом реалізації Концепції інформаційної безпеки дитини в Україні повинно стати формування молодого покоління громадян, які зможуть вільно та самостійно орієнтуватися в інформаційному середовищі, забезпечувати безпеку власного інформаційного простору та стати успішними членами глобалізованого інформаційного суспільства.

Список використаних джерел:

1. Жарков Я. М. та ін. Інформаційно-психологічне протиборство (еволюція та сучасність) : Монографія. / Я. М. Жарков, В. М. Петрик, М. М. Присяжнюк та ін. - К.: ПАТ "Віпол", 2013. - 248 с.

2. Богатова Е.Б., Константинов В.В. Устойчивость личности к информационному воздействию как центральное психологическое образование эпохи глобализации // Известия ПГПУ им. В.Г.Белинского. 2012. № 28. С. 1154-1155.

3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287/2015 // База даних Законодавство України / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/287/2015 (дата звернення: 05.05.2018).

4. РФ пытается активно манипулировать русской молодежью в Эстонии // Інтерфакс-Україна від 12.04.2018. URL: https://interfax.com.ua/ news/general/498354. html (дата звернення: 05.05.2018).

5. Про охорону дитинства: Закон України від 26.04.2001 № 2402-III. // База даних Законодавство України / ВР України. URL: http://zakon5.rada. gov.ua/laws/ show/2402-14 (дата звернення: 05.05.2018).

----------***----------

Чернишина Г. Г., *завідувач лабораторії ФСП КПІ ім. Ігоря Сікорського.*

ТАРГЕТОВАНА РЕКЛАМА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

З розширенням можливостей доступу до Інтернету пересічних громадян, компанії, що пропонують товари, послуги використовують інформаційний простір для реклами своєї продукції найбільш вразливій аудиторії. Для цього рекламодавці вдаються до збору інформації на основі якої і створюється таргетована реклама. Кожна аудиторія має певні персональні риси, знаючі які можна створити цільову рекламу. Такими рисами можуть бути расова або етнічна приналежність, стать, соціальний статус, вік, рівень освіти, місце роботи. Також збираються і аналізуються психологічні портрети такі як, індивідуальність, життєві цінності або інтереси.

Таргетована реклама або будь-яка реклама міцно пов'язана з пропагандою і піаром (зв'язки з громадськістю). Одним із засновників сучасного піару і пропаганди був американець Едвард Бернейс. Бернейс був племінником

австрійського психолога Зигмунда Фрейда, чиї роботи з психоаналізу він активно використовував у своїй діяльності. Клієнтами Бернейса були такі компанії як General Electric, Procter & Gamble та American Tobacco Company. Фундаментальною працюю Едварда Бернейса стала книга "Пропаганда", опублікована в 1928 році, на основі своєї успішної роботи в рекламному бізнесі він описав процеси маніпуляції свідомістю споживачів. Ідеї і заповіти Бернейса досі становлять основу рекламної стратегії [1].

Перші прояви таргетованной реклами в інтернеті з'явилися в 1990-х роках. Але вона була лімітованою за рахунок обмеженого поширення персональних комп'ютерів серед звичайних громадян, також були складності зі зберіганням інформації про користувачів. З приходом нульових років, та поліпшенням інформаційних технологій, стало можливо більш успішно збирати, систематизувати і зберігати персональну інформацію про користувачів.

Також з’явилися можливості створення ефективної таргетированной (цільової) реклами на основі поведінкових алгоритмів користувачів [2].

Інтернет став важливим елементом у житті кожної людини. Користувачі стали більш досвідченими та розвиненими в використанні інформаційного простору. Одна з найважливіших проблем, що несе таргетована реклама, це використання персональних даних користувачів для інших потреб. В цілях регулювання системи реклами в інтернеті багато країн стали створювати різні закони та акти для регулювання подачі реклами користувачам та використання інформації про користувачів у рекламних цілях. В США, де проблема регулювання реклами в Інтернеті зрозуміла досить давно, працює регуляторна система Federal Trade Commission "Федеральний комітет по Торгівлі" (FTC). FTC встановлює чіткі правила, як компаніям так и рекламним агентствам які пропонують свої товари та послуги. Що їм можна робити в рамках закону а що, не можна. Перший документ FTC для Конгресу США був представлений в червні 1998 року. В ньому йшлося, що 85% сайтів збирають особисту інформацію про своїх користувачів і лише 14% з них повідомляють про це своїм клієнтам. Так само важливим законом, який FTC представив на розгляд Конгресу був підзаконний акт The Childrens Online Privacy Protection Act (COPPA) в 2000 році, який зобов'язував комерційні сайти, на яких можуть зайти діти до 13 років, отримати дозвіл від їх батьків на збір інформація про дітей. Ці приклади показують, що в Сполучених Штатах Америки питання про законодавче регулювання реклами в Інтернет було розроблено майже з самого початку розповсюдження мережі серед приватних користувачів [3].

В Україні ж є проблеми з регулюванням реклами в інтернеті. Якщо в США при FTC є особливий департамент який займається тільки законами і регулюванням реклами в інтернеті, то в Україні, такий спеціальний орган відсутній. Не дивлячись на те, що у нас є багато комітетів та комісій які

займаються законами про монополії, рекламу, захист інформації, окремих органів з регулювання та імплементації законів про торгівлю, виключно для інтернету у нас немає. У 2008 році, на розгляд Верховної Ради України виносився проект закону "Про Інтернет рекламу" № 3126, але він так і не був прийнятим [4].

У підсумку, в зв'язку з низькою зацікавленістю наших законодавчих органів в розробці законодавчої системи для інтернету в Україні, наша країна має небезпечний шанс потрапити під вплив пропаганди інших держав, у відношенні реклами в інтернеті, які більш серйозно поставилися до цієї проблеми.

Список використаних джерел:

1. The manipulation of the American mind: Edward Bernays and the birth of public relations.-URL: http://theconversation.com/the-manipulation-of-the-american-mind-edward-bernays-and-the-birth-of-public-relations-44393 (дата звернення 20.05.2018)

2. Targeting of Online Advertising.-URL: https://aaltodoc.aalto.fi/bitstream/handle/123456789/27250/bachelor_Tupam%C3%A4ki_Kalle_2017.pdf?sequence=1&isAllowed=y (дата звернення 18.05.2018)

3. Advertising and Marketing on the Internet.-URL: https://www.ftc.gov/system/files/documents/plain-language/bus28-advertising-and-marketing-internet-rules-road2018.pdf (дата звернення 22.05.2018)

4. ЗУ Про Інтернет рекламу. – URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JF2EU00A.html (дата звернення 22.05.2018)

----------*----------**

Фарадж Д. Ю., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник: ***Фурашев В.М.,*** *к. т. н., доцент ФСП КПІ ім. Ігоря Сікорського.*

НЕГАТИВНИЙ ВПЛИВ СМАРТФОНІВ НА СВІДОМІСТЬ ТА ІНТЕЛЕКТУАЛЬНИЙ РОЗВИТОК МОЛОДІ

На сьогоднішній день можна помітити, що молоде покоління дуже багато часу проводить з телефонами, замість так званого живого спілкування, і це є дуже поганим фактором.

Було б доцільно розпочати з поняття телефону та його початкове признаення, а потом перейти до дослідження даної проблеми.

Телефон поняття іншомовного походження, складається з двох слів: «Теле», що означає далеко і «Фон», що означає звук, на сьогодні це апарат для

прийому та передачі звуку на відстані за допомогою електричних сигналів. Телефон, як і все інше має свою давню історію. Можна виділити три етапи призначення телефонів, а саме:

– Перший етап – називають початком ери телефонів, тому що створювався пошук засобу, який би міг оперативно передавати інформацію, даний період припадає на 60-і роки XIX століття.

– Другий етап – широке впровадження нових технологій, активно розвиваються мобільні мережі зв'язку, започатковується масове виробництво телефонів та їх впровадження, даний період припадає на 70-і роки XX століття.

– Третій етап – телефон стає універсальним засобом спілкування між людьми не залежно від відстані, а також впровадження безлічі додатків мультимедіа, що вміщують в собі функції телевізора, комп'ютера, тощо, і з кожним роком в телефон додають все більше і більше функцій, що і є негативним для впливу на свідомість та інтелектуальний розвиток молоді та населення в цілому, даний етап припадає на кінець XX століття і до сьогодні.

Користувачі смартфонів зазвичай свій день починають та закінчують з перегляду стрічок у соціальних мережах, тим самим не підозрюючи те, що з кожним днем вони становляться заручниками деградації. Так звані «Розумні гаджети» стали невід'ємною частиною життя молоді, так, як їх початкове призначення, а саме передача та прийом звуку через електронні сигнали вже не є одиничною функцією. На сьогодні люди використовують телефони не тільки для дзвінків, а й для перегляду погоди, пошуку роботи, здійснення покупок через інтернет, тощо.

Використання смартфонів негативно впливає на свідомість людини та на її інтелектуальний рівень. Дуже знижується уважність при цілодобовому користуванні смартфонами, вона може знижуватись навіть коли гаджет лежить поруч, це несвідомо відволікає увагу. Смартфони є так званим «вікном у світ», а тому мозок людини автоматично приділяє їм увагу. Найбільшою проблемою молоді є дуже часте покладання на так званий «Кишеньковий інтернет» в пошуках відповідей на будь-яке поставлене їм запитання, замість того, щоб самостійно подумати над відповіддю, таке покладання значною мірою знижує спроможність мозку запам'ятовувати будь-якого роду інформацію.

Хотілося б звернути увагу на таке поняття, як « Покоління iGen»- це підростання нового покоління, яке народилося в період між 1995 та 2012 роками і стало першопроходцями , які не уявляють світ без смартфонів та інтернету. Дане покоління, які дуже часто користуються смартфонами психологічно є більш уразливе, ніж їх попередники. Надмірне користування смартфонами дуже часто призводить до дипресивної поведінка та навіть до суїциду, причиною є нестача живого спілкування молоді, вони спілкуються через гаджети навіть не виходячи з домівки. Також надмірне користування смартфонами дуже затримує

вік дорослішання у молоді, наприклад 20-річні зараз поводять себе, як колись поводили себе 16-річні, а 16-річні поводяться, як 12 річні, таким чином дуже затягується дитинство.

Смартфони впливають на фізичний та психічний стан людини, але це не зобов'язує людину відмовитись від сучасних технологій, виникає потреба проводити більше часу на свіжому повітрі і бажано подалі від гаджетів. Також, якщо відкладати гаджети подалі від ліжка то це покращить якість сну, дехто може задати питання, а як, же будильник ?, будильник краще використовувати годинниковий. Що стосується навчання, то телефон взагалі не бажано брати з собою. Виникає дуже велика проблема телефонної залежності у молодого покоління, вони вже не представляють свого життя без смартфонів, на сьогоднішній день учні, які навчаються у першому класі вже заражені такою залежністю, а виною цьому є їх батьки, які з раннього дитинства привчають своїх дітей до смартфонів за для відволікання тих від інших потреб, або, щоб не приділяти їм багато уваги, але такий спосіб виховання зовсім не є ефективним а тільки погано вплине на майбутнє дитини. Найкращим способом запобігти телефонної залежності у молоді є розповсюдження для них інформації щодо можливих наслідків надто тривалого користування телефонів, але це може бути не зовсім ефективно, так, як діти дуже часто беруть приклад з своїх батьків, а тому, батькам самим слід менше часу проводити з гаджетами та стати прикладом для своїх дітей.

На сьогодні існує велика кількість додатків для телефонів, які нічим не шкодять, а навпаки служать для покращення здоров'я людини, слід користуватись такими додатками, вони не викликають залежність. Молоді слід менше проводити часу в соціальних мережах переглядаючи стрічки, а також рекомендовано не гратись у сучасні ігри, які ще більше псують їх розвиток. Якщо раніше ігри на телефони створювали де потрібно було хоч трохи подумати, то на сьогоднішній день розробники ігор випускають такі ігри, де все, що потрібно просто натискати одну кнопку, що призводить до великого зниження інтелекту людини.

Тому молоде населення має самостійно обирати свій шлях життя та використовувати смартфони для покращення свого самопочуття та майбутнього.

Список використаних джерел:

1. Електронний ресурс: https://www.radiosvoboda.org/a/28705680.html
2. Електронний ресурс: https://24tv.ua/ru/pokolenie_igen_kak_smartfony_izmenili_celoe_pokolenie_n950658

----------***----------

Петряєв О. С., *аспірант Національного інституту стратегічних досліджень; викладач ФСП КПІ ім. Ігоря Сікорського.*

ЄВРОПЕЙСЬКІ СТРАТЕГІЇ ПОЛІТИЧНОЇ ДЕРАДИКАЛІЗАЦІЇ ІСЛАМСЬКОЇ МОЛОДІ

В ЄС багато десятиліть проживає чимало мусульманського населення. А в таких європейських країнахяк Боснія і Герцеговина, Косово і Албанія, мусульманське населення є абсолютною більшістю, що пов'язано з османськими завоюваннями.

Дедалі більше ісламізується ФРН, куди із-за дефіциту чоловічої робочої сили в повоєнний період масово рекрутувалося турецьке населення. Водночас, турки мігрували також до Бельгії, Нідерландів, Австрії. Так само, після закінчення війни в Алжирі, до Франції масово мігрували алжирські мусульмани.

Другий етап масової міграції став наслідком Арабської Весни: війн в Лівії, Сирії, Іраку, Ємені, Афганістані та в ряді Африканських країн. З 2015 року, арабські біженці почали масово мігрувати до ЄС, перетинаючи Середземне море або через сухопутний кордон Туреччини з країнами ЄС.

За даними на 2016 рік, мусульманське населення Європейського Союзу плюс Норвегії та Швейцарії склало 4,9% від усього населення Союзу (25,8 млн.). Це певне зростання порівняно з 2010 р., коли в ЄС було тільки 3.8% мусульман (19,5 млн.). Наразі найбільше мусульман проживає у наступних країнах ЄС [1]:

- Франції (8,8% від загалу населення; 5,720 млн.);
- Німеччині (6,1%; 4,95 млн.);
- Великобританії (6,3%; 4,13 млн.);
- Італії (4,8%; 2,87 млн.);
- Нідерландах 7.1% (1,21 млн.);
- Іспанії 2.6% (1,18 млн.).

За даними Pew Research Center, за умови збереження нинішнього рівня народжуваності у мусульманських сім’ях (одна жінка народжує одну дитину) й збереження нинішніх міграційних трендів до 2050 р. мусульманське населення ЄС становитиме від 11,2% до 14% від загалу населення ЄС (якщо він на той час існуватиме в нинішньому вигляді) [2].

Політика ЄС щодо мусульманської міграції будувалася на основі соціальних стратегій, які праворадикальні елементи вважають «помилковими». По-перше, уряди держав ЄС робили ставку на відносну дешевизну робочої сили мусульманського походження, ігноруючи при цьому специфічний менталітетом

мігрантів, заснований на релігії і сприйнятті європейців як колишніх колонізаторів. Друга помилка європейських урядів нібито полягала на перенесенні на європейський грунт американської «плавильного котла», згідно якої мігранти мали змішатися з європейським населенням. Тут дійсно містилася недооцінка поняття «мусульманська умма» (мусульманська нація), відповідно до якої мусульманське населення протиставляє себе корінному населенню Європи в релігійному і культурному плані, що вже призвело до створення мусульманських районів (гетто) в основних європейських містах, що, зрештою, типово не тільки для мусульманського населення.

У 2014 році на тлі війни в Сирії активізувався Ісламський Халіфат (ІДІЛ; ДАІШ), який пробував з терористичної організації перетворитися на «повноцінну» державу, що контролює великі території Сирії та Іраку, має інститути влади, армію і економіку. Стратегічною метою ІДІЛ обрав побудову нової ісламської імперії XXI століття. За допомогою Інтернету (особливо YouTube та соціальних мереж) ісламські пропагандисти вели агітацію серед європейських послідовників ісламу молодшого віку, не задоволених життям в Європі, мусульман-мігрантів та корінних європейців, які зацікавилися радикальним ісламом. Результатом стала участь європейців і європейських мусульман в громадянській війні в Сирії на боці ІДІЛ й терористичні атаки радикалів-ісламістів в містах ЄС.

Важливо враховувати еволюцію свідомості індивідуума, коли він зі звичайної людини перетворюється на терориста. Першим етапом тут є радикалізація свідомості, коли людина подумки підтримує використання насильства для досягнення політичних або релігійних цілей. На другому етапі радикал перетворюється на екстреміста, який потрапляє під вплив ідей, які сповідують радикальні політичні рухи, які завдяки використанню насильства хочуть змінити суспільство. На третому етапі зміни людину цілеспрямовано використовують для здійснення актів насильства, залякування суспільства для досягнення «вищих» політичних цілей.

На тлі загострення терористичної загрози не тільки наукові інститути, але й держані агенції ініціювали програми дерадікалізації мусульманського населення. У 2014 р. Рада безпеки ООН ухвалила Резолюцію 2178 щодо протидії насильницькому екстремізму (Countering Violent Extremism (CVE). Відтак різні країни світу почали розвивати індивідуальні і спільні програми для дерадікалізації населення, на підтримку неурядовим агенціям, які працюють в цьому напрямі. Програми CVE акцентують увагу на боротьбі з розповсюдженням екстремістської інформації в соціальних мережах, які є наразі чи не найголовнішою платформою радикальної пропаганди в Інтернеті. [3]

Завданням дерадикалізації є зміни аттитюдів щодо екстремістської ідеології, відмова від своїх переконань та участі у насильницьких політичних

акціях. Існує щонайменше шість форм програм дерадикалізації: освітні, професійні, соціокультурні, релігійно-ідеологічні, психологічні та громадські [4].

Доцільно також виокремлювати підходи до роботи з населенням на рівнях макро- мезо- й мікросоціальних. Макро-соціальний рівень передбачає реалізацію програм національного, регіонального та міського масштабів. Мезо-соціальний рівень – це робота із сім'ями, на робочих місцях, у школах та громадах. Мікро-соціальний рівень – це індивідуальні підходи [3].

Так само доцільно виокремлювати три форми роботи з дерадикалізації: запобігання, тлумлення та втручання, кожна з яких використовується на різних етапах радикалізації, індивідуума чи групи осіб, залежно від стану, у якому вони наразі перебувають: радикальному, екстремістському чи терористичному і залежно від того, наскільки вони готові вдатися до актів [3].

Великий досвід боротьби з насильницьким екстремізмом має Великобританія, де подібні програми діють уже впродовж десяти років. Проте, попри помітну користь від реалізації таких прогаром, вистачає і їх критики. Зокрема, орієнтація цих програм на мусульманські громади сприяє їх відчуженню, творенню довкола них «атмосфери страху». Існують також звинувачення у заохоченні різноманітного «шпигунства», починаючи від моніторингу електронної пошти та акаунтів соціальних мереж й закінчуючи використанням компетентними правоохоронними органами (Скотландом-Ярдом тощо) інсайдерів («кротів») з відповідних радикальних й екстремістських угрупувань. У відповідь представники правоохоронних органів звинувачують своїх критиків у «невігластві», відкидаючи при цьому звинувачення у «шпигуванні», але підкреслюючи натомість моменти, пов’язані з «профілактикою» [4].

Британська програма дерадикалізації PREVENT була започаткована у 2003 р. тодішнім урядом лейбористів як складова ширшої урядової програми протидії терористичній загрозі – CONTEST. У 2011 р. ці програми були пролонговані урядом консерваторів й ліберальних демократів (лібдемів). В одному лише 2015 р. завдяки програмі PREVENT вдалося попередити відправку в ІДІЛ 150 молодих людей [5].

Превентивні заходи будуються за трьохчленною пірамідальною схемою: (а) інокуляція (інформаційне «щеплення» проти тероризму); (б) цільове втручання (targeting interventions); (в) наставництво (mentoring) [5].

Отже, боротьба з радикалізмом, екстремізмом та теоризмом повинна проводитися переважно превентивними методами, для чого слід виявляти ознаки радикалізму у різних людей або соціальних груп на якомога ранніх етапах і ліквідувати засобами «інформаційного щеплення» задовго до того, як він увійшов у термінальну стадію тероризму.

Список використаних джерел:

1. Europe's Growing Muslim Population. // Pew Research Center. 29 листопада 2017 р. – URL: http://www.pewforum. org/2017/11/29/europes-growing-muslim-population/
2. Countering violent extremism. // The United Nations Security Council Counter-Terrorism Committee. – URL: https://www. un.org/sc/ctc/focus-areas/countering-violent-extremism/
3. Koelher D. A typology of 'de-radicalisation' programmes. // De-radicalisation' Scientific insights for policy. Flemish Peace Institute. Brussels. Sept. 8. 2017. Pp. 63-69. – URL: https://www.flemishpeace institute.eu/sites/vlaamsvredesinstituut.eu/files/files/reports/deradicalisering_eng_lowres.pdf
4. Baird, Roger. Prevent: Police chief says critics of Home Office counter-terrorism scheme are ignorant // The International Business Times. August 7, 2017. – URL: https://www.ibtimes.co.uk/prevent-police-chief-says-critics-home-office-counter-terrorism-scheme-are-ignorant-1633810
5. De Silva, Richard. Is the UK counter extremism model working? // Defence IQ. 08/11/2017. URL: https://www. defenceiq.com/cyber-defence-and-security/news/is-the-uk-counter-extremism-model-working

----------***----------

Головатий А. А., *студент ФСП КПІ імені Ігоря Сікорського.*
Науковий керівник: ***Фурашев В. М.,*** *к. т. н, доцент ФСП КПІ ім. Ігоря Сікорського.*

ПРОБЛЕМА ДОТРИМАННЯ КОНСТИТУЦІЙНИХ ПРАВ І СВОБОД У ІНТЕРНЕТІ

В наш час важко знайти людину, яка б не користувалася Інтернетом. В останні десятиліття він став невід'ємною частиною життя кожного з нас. Та правда в тому, що з часом Інтернет перетворюється на справжній смітник, в якому важко знайти корисну інформацію, а таке поняття як цензура вже давно нічого не вартує. Аби зрозуміти, що зумовило такий розвиток подій, варто пригадати, що саме зробило його настільки привабливим для людей.

Інтернет – це наразі єдине доступне всім у світі місце, де свобода є насправді абсолютною. Тільки там ти можеш сказати будь-що, не боячись наслідків – не обов'язково навіть використовувати своє власне ім'я. В Інтернеті фактично не існує такого поняття як контроль, що дозволяє людям безкарно робити ті речі, які в реальному світі вони робити не можуть. Інтернет - це місце, в якому практично все базується на найбільш примітивних інстинктах і потребах людини. І все це не тільки працює, а й активно розвивається надалі

лише через одну причину – це приносить великі гроші. Справді, все, що в реальному світі є забороненим, але реалізується в Інтернеті приносить надзвичайний прибуток і так триватиме до тих пір, поки цей прибуток буде надходити.

Кожний громадянин або підданий у будь-якій цивілізованій країні світу володіє певним набором прав і свобод. Вони гарантуються конституціями кожної з таких держав і поширюються, як на своїх людей, так і на іноземців. Всі ці документи в першу чергу закріплюють такі демократичні основи суспільства як свобода слова, рівність, свобода творчої діяльності та багато інших. Здавалось би, Інтернет має бути місцем, де наявність всіх цих прав зрозуміла сама по собі, але що ж ми маємо насправді? Неповага до чужих честі та гідності, расизм, сексизм, шовінізм – і це тільки перше, що кидається у вічі, коли вмикаєш будь-який сайт. На жаль, дотримання більшості конституційних прав і свобод у Інтернеті тепер залежить лише від моралі тих, хто володіє тими чи іншими сайтами, медіа, соціальними спільнотами і іншими подібними речами. Існує кілька серйозних проблем, які ставлять під сумнів можливість виправити курс на деградацію людства. Перша з них полягає в тому, що станом на сьогодні просто не існує суб'єкту, здатного неупереджено виконувати в Інтернеті контрольно-наглядову функцію на міжнародному рівні. Основний недолік конституційних прав людини – це те, що вони безпосередньо прив'язані до конкретних країн. Взагалі, конституція – найперший спосіб взаємодії держави з особою, яка проживає на її території. Тому, враховуючи чисельні відмінності у конституціях різних країн, створення компетентного органу на даний момент виглядає мало вірогідним. Справа навіть не у відмінностях в самих документах – розділ, що стосується прав і свобод людей мало чим відрізняється у всіх демократичних державах. Проблема полягає у розподілі відповідальності, адже сама сутність будь-якої конституції полягає в тому, що вона діє виключно на територіях, що належать до юрисдикції тієї чи іншої країни.

Одне з основних прав людини, яким активно нехтують в Інтернеті є таємниця листування. В електронному вигляді воно є, мабуть, найпопулярнішим способом спілкування в «міжнародній павутині». Та і взагалі безпека персональних даних сьогодні є доволі сумнівною. Майже ні для кого не є таємницею, що такі служби як ЦРУ постійно тиснуть на відомі компанії та соціальні мережі з метою отримати доступ до інформації людей, підозрюваних у скоєнні злочинів.

Отже, станом на сьогодні дотримання багатьох конституційних прав і свобод людей у мережі Інтернет є практично неможливим, враховуючи чисельні й серйозні недоліки сучасного суспільного устрою.

----------*----------**

Сказко О. М., *аспірантка, Науково-дослідний інститут інформатики і права НАПрН України.*

ПРАВОВЕ РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН ПОВЯЗАНИХ З ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ

Розвиток інформаційних технологій призвів до їх широкого використання у всіх сферах життєдіяльності людини, суспільства та держави. Використання мережі Інтернет та Інтернет технологій для обміну інформацією у будь якому вигляді та форматі стало звичайним явищем сьогодення. Проте особливості застосування комп'ютерних та Інтернет технологій, що обумовлюють виникнення певної анонімності суб'єктів такого інформаційного обміну, невизначеності місця їх знаходження та часу відправлення та отримання інформаційних повідомлень, транскордонний характер інформаційної взаємодії, призводить до виникнення високого рівня недовіри, щодо використання таких технологій, що значно ускладнює процес взаємодії людей будь якого виду діяльності, в бізнесі, в банківській сфері, в державному управлінні та в інших сферах суспільних взаємовідносин. На сьогодні це є однією з основних проблем невирішення якої створює бар'єри для подальшого використання мережі Інтернет та Інтернет технологій, тому що нейтралізація негативних наслідків цих технологій потребує вжиття додаткових заходів щодо фіксації певних юридичних фактів, які в умовах чинного законодавства іноді неможна здійснити.

Джерелом розходжень змісту підходів до вирішення проблеми правового регулювання суспільних відносин, пов'язаних з використанням інтернет-технологій, очевидно є різне розуміння предмета правового регулювання й об'єкта правовідносин. Також методологічно ключовим для предмета дослідження є визначення дефініції терміна «Інтернет» [1]. Так В.О. Копилов зазначав, що Інтернет являє собою нове середовище перебування людства, нове середовище діяльності особистості, суспільства, держави [2]. С. В. Малахов стверджує, що поняття Інтернет «визначається як а) інформаційна комп'ютерна система, що складається із сукупності окремих інформаційних комп'ютерних мереж, об'єднаних на основі єдиного міжмережевого протоколу, б) інформаційний простір, в) середовище перебування суб'єктів суспільства, г) сукупність інформаційних суспільних відносин у віртуальному середовищі» [3].

Об'єктами ж правовідносин у мережі Інтернет є: 1) телекомунікаційні мережі та інше технічне обладнання; 2) комп'ютерне програмне забезпечення; 3) інформація, інформаційні ресурси, інформаційні продукти, інформаційні послуги; 4) доменні імена; 5) права та свободи в сфері інформації; 6) інформаційна безпека.

При всьому різноманітті об’єктів відносин в Інтернеті потрібно зазначити, що основним об’єктом відносин, що складаються в мережі, є інформація (технічна, економічна, соціальна, юридична та ін.). Сьогодні інформація стирає грані між продуктом і послугою, що знаходить своє втілення в сучасних технологіях, які об’єднують інформаційні продукти і послуги в єдине ціле [4].

Пріоритетними методами та способами правового регулювання суспільних відносин, що виникають з приводу використання всесвітньої комп’ютерної мережі Інтернет, є публічно-правовий та приватно-правовий методи (метод юридичної рівності сторін), позитивне зобов’язання та дозвіл, оскільки вони є засобами юридичного стимулювання поведінки учасників згаданих суспільних відносин [5].

Правовідносини у віртуальному середовищі виступають юридичною формою взаємодії користувачів мережі Інтернет з приводу обміну різноманітною інформацією, мають вольовий характер та у сукупності складаються з комплексу абсолютних і відносних, регулятивних і охоронних правовідносин. Потрібно зауважити, що багато вчених, відносини у мережі Інтернет називають інформаційними відносинами, а це дає змогу зробити висновок, що відносини у мережі Інтернет є різновидом інформаційних відносин. Головною особливістю цих правовідносин є те, що суб’єктивні права в них, в першу чергу, розкриваються через власні дії користувачів мережі Інтернет, які спричиняють виникнення, припинення або зміну прав та обов’язків інших учасників мережі Інтернет, а не тільки через обов’язки третіх осіб (інформаційних провайдерів та власників Інтернет-сайтів).

Правове регулювання суспільних відносин що виникають в процесі використання мережі Інтернет може бути необхідною у наступних випадках:

– в процесі розгляду доменних спорів;

– при захисті прав правовласників у сфері промислової власності;

– при захисті честі гідності та ділової репутації фізичних та юридичних осіб;

– неправомірного використання об’єктів авторського права (текстів, аудіо, відеоматеріалів, тощо);

– у випадках розповсюдження реклами зміст якої суперечить положенням закону України «Про рекламу»;

– фіксації перекрученні чи зміни цілісності переданих повідомлень.

Зазначені проблеми мають не тільки внутрішньодержавний характер, але й міжнародний, завдяки тому, що інформаційний обмін, в останні часи, стає більше глобалізованим, а суб’єкти цього обміну можуть мати різнодержавну юрисдикцію.

Але недосконаліть, а в більшості випадків, відсутність усталеного правового механізму не дозволяє як на національному, так і на міжнародному ефективно вирішити проблему зміцнення довіри до використання інформаційних технологій, дієвого захисту порушених прав та інтересів осіб, які використовують ці технології, а також забезпечити її більш широке використання у всіх сферах життєдіяльності суспільства.

З урахуванням вищезазначеного, особливо актуальним є формування теоретико-методологічних засад регулювання суспільних відносин та забезпечення фіксації юридичних фактів в умовах використання мережі Інтернет та напрацювання практичних рекомендацій щодо удосконалення національного законодавства.

Список використаних джерел:

1. О.А. Баранов «Інтернет і право: об'єкт і предмет регулювання».
2. Копылов В.А. «Информационное право».
3. Малахов С. В. «Гражданско-правовое регулирование отношений в глобальной компьютерной сети Интернет».
4. Еннан Р.Є. «Правове регулювання відносин у мережі Інтернет».
5. Жилінкова І. В. «Правове регулювання Інтернет – відносин».

----------***----------

Полевий В. І., *к.ю.н., с.н.с., завідувач кафедри загальнотеоретичних правових дисциплін та філософії Бердянського університету менеджменту і бізнесу.*

ФЕЙКОВІ НОВИНИ ЧИ ФЕЙКОВИЙ МЕДІАПРОСТІР: ПОСТАНОВКА ПРОБЛЕМИ

Сьогодні багато говоримо про інформаційну агресію проти України з боку Росії, про феномен «фейкових» новин, про загибель класичних медіа.

Мабуть, протягом цієї конференції багато буде сказано та написано про кількісні та якісні характеристики російського впливу, про російську пропаганду та проросійські медіа чи журналістів тут, в Україні.

Я ж хочу звернути ваші погляду в Україну, її читачів, чи, ба, більше, у голови кожного з нас. А також поставлю такі запитання:

Які внутрішні передумови сприяють агресору в інформаційному просторі?

Що можемо з цим зробити?

Інформація для людини не є самоціллю, а лише необхідним інструментом для прийняття рішення. Ми відкриті до інформації, потребуємо її, і лише фізичні можливості обмежують нас у її споживанні.

Тому теза перша. Для прийняття рішення потрібно обмежити споживання інформаційного шуму, нерелевантної інформації та вміти фільтрувати нерелевантні інформаційні потоки і концентруватися на ваших задачах.

Іншими словами, я говорю про правила інформаційної гігієни, про яку вже починають говорити, але яка ще не стала нормою, як гігієна побутова, фізична. Громада лише стоїть на шляху до усвідомлення її важливості, а особистість ще не навчена простим діям на її підтримку: мити руки, не їсти з землі, їсти приборами, а не руками. В частині споживання інформації це можуть бути правила: обмеження розважального контенту, рестрикція комерційного контенту, лімітованість часу у віртуальному просторі, споживання інформації з надійних джерел, навчання та саморозвиток, а лише тоді розваги тощо.

Далі. Прийняття рішення передбачає співставлення отриманої інформації, а потім і проекту дії з усталеною системою цінностей особистості. Системою, яка має існувати і бути частиною зрілої особистості. Зрілість, в даному випадку, означає здатність приймати відповідальні (системі цінностей, особистим, родинним, громадським інтересам) рішення самостійно. Цінності мають бути наочними та певним чином канонізовані. Знаємо про християнські чесноти, про духовні скрєпи руського міра, про моральний кодекс будівника комунізму (такі дідугани як я його пам‘ятають), а що можемо сказати про цінності українця?

Цінності особистості в її індивідуальному та колективному розрізі? Демократія, секуляризація, свобода слова не є цінністю, а лише інструментом для формування світогляду. Україна і без війни знаходиться на зламі соціальних парадигм. Ринок формує з нас споживача, Інтернет із простору свободи став маркетинговим інструментом та ринковою платформою, тому тут, у загальній масі, ми також споживачі інформації, а не її творці. Страх перед зовнішньою загрозою штучно згуртував нас навколо патріотизму, навколо держави, Патріотизм є товаром та гаслом, яке продають нам політичні партії, що змагаються за право бути найбільш патріотичними.

Чому це об’єднання штучне? Тому що в його основі лежить страх, який гуртує нас у зграю, орду, у тваринний натовп, який діє за своїми законами психології мас, що так влучно сформував Гюстав Ле Бон. Натовпу потрібен лідер, він мислить у чорно-білих тонах, відкидає індивідуальну відповідальність за вибір, він потребує публічного «спалення» ворогів тощо.

У сухому підсумку, українці – ірраціональна (у владі емоцій та зовнішніх впливів), інфантильна (незріла, не готова брати на себе відповідальність), перелякана зграя наляканих тварин.

Якщо розглядати проблему через призму п‘яти стадій емоційної реакції особистості на зміни (заперечення, гнів, торг, депресія, прийняття) , то українці лише у незначній своїй частині дійшли до стадії депресії, або розчарування змінами, що на нас навалилися, і про які ми, загалом, нікого не просили.

Торг та депресія – дуже нестійкі стани та чудова передумова до подальших маніпуляцій. Демократія та вибори – конституційні інструменти, які роблять маніпуляції неминучими для України. Медіа та Інтернет – канали маніпуляції натовпом.

Це проміжний висновок з першого питання, яке я задав на початку доповіді. Він вам не подобається? Тоді у мене для вас погана новина – зараз ви знаходитеся лише на першій емоційній стадії: заперечення.

Що означає стадія прийняття для нашого суспільства?

Усвідомлення того, хто ми є (див. вище), прийняття факту важкої боротьби на десятиліття (потреба терпіння), розуміння відсутності швидких рішень (відмова від інфантилізму популістів до відповідальності), внутрішньо усвідомлена потреба почати з себе та з власного кола впливу.

Таким колом впливу традиційно є не друзі (вторинне коло), колеги по роботі (штучна ринкова спільнота), френдифейсбука (віртуальна спільнота), а сім‘я. Повноцінні особистості батька, матері, дітей та старших членів родини. Усвідомлення нашого місця – не як вінця творіння і самоціллі, а лише частки у безперервному коловороті зміни поколінь. Місця, яке знецінює ваше Я, його емоції, але возвеличує ваші Дії на нескінченому шляху Творіння.

Звідси й назва цих тез. Фейковими є не новини, а наш інформаційний простір в цілому. Нажаль, він не той і не про те. Він про гроші, страхи та емоції, а не про те, що зробить з нас особистість, а вже потім згуртує нас в українців на основі спільних цінностей.

Список використаних джерел:

1. Psychologie der Massen. 15. Aufl. — Stuttgart: Kröner, 1982. ISBN 3-520-09915-2
2. Елисеева Е. 5 стадий принятия неизбежного, изменений и управленческих решений /веб-сайт NRG[Електронний ресурс] . -2018. – 20 квіт. – Режим доступу: http://newrealgoal.com.ua/5-stadij-reagirovaniya-sotrudnikov-na-izmeneniya.html.

----------***----------

Сірик А. О., *провідний науковий співробітник в/ч А1906*

НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ІНФОРМАЦІЙНОЇ ЕКСПАНСІЇ РФ

Агресія Росії проти України, яка розпочалась в лютому 2014 року з анексії Криму та триває нині на Донбасі, не є другорядним, локальним конфліктом на кордонах Європейського континенту. Ця війна несе не лише загрозу державності України, а й Західному світу. Європейці стали критично вразливими як від внутрішніх проблем, так і від

силової "гібридної" політики Кремля. Головною складовою якої є потужна інформаційна експансія, що набула рис агресивного характеру.

Особливостями інформаційних заходів РФ проти країн ЄС та НАТО останнім часом стали: використання з пропагандистською метою Російської православної церкви в країнах Заходу та інших регіонах спрямоване на об'єднання православних віруючих, російськомовного населення; використання проросійських агентів впливу у міжнародних організаціях, які можуть відстоювати необхідну позицію для вирішення суперечок та лобіювання інтересів Кремля; публікація фейкових новин через соціальні мережі (Facebook, Twitter), форуми та інші інтернет-ресурси з метою дискредитації опонентів РФ та розповсюдження дезінформації, провокативних повідомлень; кібернетичні атаки на об'єкти критичної інфраструктури.

Свідченням масштабності заходів у кіберпросторі стали кібератаки хакерських угруповань (червень 2016 року) на головний офіс Демократичної партії США, які підтримувалися спецслужбами РФ та призвели до витоку тисяч електронних листів, призначених для внутрішнього користування, а також ситуація із втручанням у президентські вибори США.

Спроби втручання РФ у внутрішньополітичні процеси країн ЄС і НАТО шляхом здійснення інформаційного впливу на населення та об'єкти інфраструктури спонукають міжнародне співтовариство до пошуку нових механізмів та інструментів для забезпечення інформаційної безпеки (ІБ) і насамперед правового регулювання цих питань. Значна увага при цьому приділяється проблемі кібербезпеки (КБ) як складової ІБ.

На Варшавському саміті НАТО (8–9 липня 2016 року) кіберпростір визначено як четвертий операційний простір поряд з морською акваторією, суходолом і повітряним простором. Міжнародними експертами на цьому саміті були визначені такі основні проблемні питання правового забезпечення у сфері КБ:

– у керівних документах Альянсу з КБ не передбачена відповідна норма, яка б давала змогу здійснювати превентивний кібернетичний вплив на мережі та системи, що використовуються хакерськими угрупованнями для кібератак як на об'єкти інфраструктури Альянсу, так і на окремі країни-члени НАТО;

– не врегульована проблема розробки механізмів, завдяки яким можна ефективно використовувати сили і засоби Альянсу для протидії кібератакам на об'єктах критичної інфраструктури країн-членів організації (на виконання статті 5 Північноатлантичного договору, згідно з якою напад на країну-члена НАТО розглядається як акт агресії проти всієї організації);

– окремі країни НАТО сьогодні не мають навіть базових документів у сфері КБ, які були б розроблені відповідно до стандартів Альянсу.

Необхідність протидії російському інформаційному впливу усвідомили і у ЄС. В листопаді 2017 року Європейський парламент ухвалив резолюцію щодо протидії пропаганді третіх країн, включаючи Росію, яка агресивно використовує цілий спектр засобів для атак на демократичні цінності, для розколу Європи і для забезпечення підтримки всередині країни.

Резолюція рекомендувала ЄС енергійніше боротися з проявами пропаганди, не забуваючи при цьому про принцип свободи слова. Також вона рекомендує посилити Оперативну групу зі стратегічних комунікацій на Сході, перетворивши її на повноцінне відомство у складі Європейської служби зовнішніх зв'язків (EEAS, фактично МЗС Євросоюзу) [1].

В сучасних умовах більшість країни Заходу перебувають у процесі вимушеної трансформації власних військових потенціалів, кібернетичної та інформаційно-психологічної зброї. Цей процес відбувається завдяки, насамперед розробці (удосконалення) власних нормативних документів (стратегій), які повинні забезпечити цілісність державної політики у даній сфері. На сьогоднішній день такі країни як США, Франція, Німеччина, Фінляндія, Естонія та інші вже розробили їх. Деякі країни ЄС знаходяться в процесі завершення розробки (Польща).

Найбільш вражаючих результатів у цьому досягли ***США***. Слід наголосити, що Пентагон оприлюднив п'ять комплексних стратегічних цілей. Одна з них передбачає нарощування потенціалу в кіберпросторі в тісній співпраці з іноземними союзниками, в першу чергу, взаємодію з НАТО [2].

У 2015 році Пентагон презентував нову Стратегію кібербезпеки (The Department of Defense Cyber Strategy), яка містить три головних напрями діяльності:

1) захист власних інформаційних систем від хакерських атак;

2) співпраця з іншими агентствами й зарубіжними союзниками в напрямку збору розвідувальної інформації, спільні операції ФБР, ЦРУ, АНБ з іноземними спецслужбами до створення системи автоматичного обміну інформацією;

3) кібернетична підтримка військових операцій США й залучення кваліфікованих цивільних фахівців [3].

Останнім часом, США усвідомлюючи загрозу деструктивного кібернетичного впливу РФ на національну безпеку вжили ряд кардинальних заходів, а саме Сенат США у вересні 2017 року проголосував за заборону використання програмних продуктів російської ІТ-компанії "Лабораторії Касперського" в державних установах США. Також, у січні 2018 року МО США оприлюднило відкриту частину Стратегії національної оборони, яка визначає глобальні загрози, найбільшими з яких визнано РФ, Китай, КНДР та терористичні організації. Питання розбудови кібернетичних спроможностей ЗС США та протидії кіберзагрозам є однією із складових цього документа.

Необхідно відмітити, що розвиток стратегії національної безпеки та оборони США в 2018 році передбачає окремим напрямом зосередження зусиль на упереджувальних діях у кіберпросторі. Головним суб'єктом реалізації цих планів є Кібернетичне командування ЗС США, статус якого був підвищений до окремої структури в системі Об'єднаних бойових командувань ЗС США [4].

Уряд ***ФРН*** (після серій кібератак у 2015 році) також активізував заходи з удосконалення системи КБ країни. В 2016 році була затверджена нова Стратегія кібербезпеки ФРН, в якій передбачена можливість здійснення превентивних кібератак на об'єкти противника. В рамках реалізації нової Стратегії та з метою удосконалення технічної

бази для боротьби проти тероризму, кіберзлочинів та кібершпигунства в інтересах усіх спецслужб ФРН на базі університету Бундесверу (м.Мюнхен) з 2017 року розпочав діяльність Центр інформаційних технологій у сфері безпеки при Федеральному міністерстві внутрішніх справ ФРН. Головною функцією Центру є превентивні заходи кібернетичного впливу на об'єкти хакерів [5].

Провідних позицій серед країн Центрально-Східної Європи у зміцненні КБ та правового регулювання цих питань досягла ***Естонія***. Така діяльність включає розробку правових визначень КБ та кіберзлочину; впровадження законодавства щодо питань КБ, включаючи запровадження обов'язкових заходів та стандартів безпеки і встановлення мінімальних вимог до безпеки інформаційних систем; започаткування ініціатив у законотворчій діяльності на міжнародному рівні тощо. У 2014 році затверджено нову редакцію Стратегії КБ Республіки Естонія на 2014–2017 роки, в якій, насамперед підсумовано здобутки країни у сфері забезпечення КБ за попередній період; надано ґрунтовну оцінку викликів і загроз та зазначено перелік заходів для ефективної боротьби з цими загрозами. Документ продовжує реалізацію цілей, закладених у Стратегії 2008 року та доповнений новими загрозами й викликами відповідно до реалій сьогодення [6].

Щодо ***Литовської Республіки***, то у 2014 році сейм Литви прийняв Закон "Про кібернетичну безпеку". Несподіваною нормою цього Закону стало те, що інтернет-провайдер може припинити надання послуг особам, якщо їхня діяльність суперечить ІБ держави. Також передбачено створення Національного центру кібернетичної безпеки, відкриття якого відбулось в 2016 році. У рамках своєї компетенції новостворений Центр разом із державними установами, організаціями та іншими суб'єктами вирішуватиме питання КБ державних інформаційних ресурсів та інформаційної інфраструктури особливого призначення [7].

Польща. Агресія РФ в Україні також підштовхнула і РП до удосконалення нормативно-правової бази щодо ІБ, а саме ведеться робота над Доктриною інформаційної безпеки. За цим документом, державній безпеці може загрожувати створення негативного образу Польщі на міжнародній арені, зокрема, серед членів НАТО та ЄС. У тексті доктрини зазначено, що третя сторона може стимулювати польсько-український конфлікт на тлі складного історичного минулого. У польській доктрині згадано методи, якими ведуться сучасні інформаційні війни. Окремо в документі говориться про інтернет-тролінг, спрямований на поширення дезінформації, висміювання та приниження користувачів мережі [8].

Попри очевидну необхідність розбудови законодавства, Польща може похвалитися певними здобутками в цьому контексті як одна з небагатьох держав, що вже прийняла відповідні зміни, які визначають дефініцію кіберпростору таким чином, що дає змогу запровадити надзвичайний стан в країні внаслідок проведення проти неї кібератак.

Отже, країни Заходу активно модернізують власні сектори безпеки відповідно до викликів сучасності, передусім у сфері КБ та протидії російській пропаганді і основним питанням при цьому є впорядкування нормативно-правової бази. Україні під час

формування інформаційної політики і побудови власної системи забезпечення інформаційної (кібернетичної) безпеки міжнародний досвід є вкрай необхідним та цінним.

Список використаних джерел:

1. Європарламент прийняв резолюцію про протидію російській пропаганді [Електронний ресурс] – Режим доступа: http://dt.ua/WORLD/yevroparlament-priynyav-rezolyuciyu-pro-protidiyu-rosiyskiy-propagandi-225409_.html.

2. Department of Defense Strategy for Operatingin Cyberspace. [Електронний ресурс] – Режим доступу: http://www.cfr.org/cybersecurity/department-defense-stra tegy-operating-cyberspace/p25479.

3. Кибернетический бастион НАТО в Прибалтике в действии [Електронний ресурс]. – Режим доступу: https://www.ritmeurasia.org/news-2016-11-20-kibernetiche skij-bastion-nato-v-pribaltike-v-dejstvii-26949.

4. Адміністрація президента США готує реформу кіберкомандування Пентагону. [Електронний ресурс]. – Режим доступу: https:/wartime.org.ua/28084-admnstracya-prezidenta-ssha-gotuye-reformu-kberkomanduvannya-pentagonu.html.

5. Cybersicherheitsstrategie: Bundesregierunglдsst Parlamentьber Planungenim Dunkeln [Електронний ресурс] – Режим доступу: https://netzpolitik.org/2016/ cybe rsicherheitsstrategie-bundesregierung-laesst-parlament-ueber-planungen-im-dunkeln.

6. Эстония модернизирует крупнейший в Европе киберполигон [Електронний ресурс]. – Режим доступу: https://www.ria.ee/en/about-estonian-information-system-authority.html.

7. Кибернетическая безопасность: ситуация в Литве и странах Балтии [Електронний ресурс]. – Режим доступу: https://net-artis.com/kiberneticheskaya-bezopasnost-situaciya-v-litve-i-stranax-baltii/.

8. Польща створює Доктрину інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://www.evrointegration.com.ua/news/2015/07/26/ 70 36321/.

----------***----------

Троян А. П., *аспірант Науково-дослідного інституту інформатики і права НАПрН України.*

ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АДВОКАТСЬКОЇ ДІЯЛЬНОСТІ В КРАЇНАХ ЄС ТА НАТО

Відповідно до частини 1 статті 394 Глави 14 «Інформаційне суспільство» Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони – сторони сприяють поступовому наближенню до права і нормативно-правової бази ЄС у галузі регулювання інформаційного суспільства і електронних комунікацій.

14 квітня 2016 року, після чотирьох років розробки та переговорів, довгоочікуваний Регламент ЄС щодо захисту даних ("GDPR") був прийнятий на рівні ЄС. За результатами голосування Комітету Верховної Ради з громадянських свобод, правосуддя та внутрішніх справ та парламенту ЄС на пленарному засіданні, GDPR тепер є офіційним законодавством ЄС і буде безпосередньо застосовуватись у всіх країнах ЄС, замінивши законодавство ЄС щодо захисту даних [0].

Нові правила включають положення про:

– право на забуття;

– "чітку та позитивну згоду" на обробку персональних даних відповідною особою, право передавати свої дані іншому постачальнику послуг;

– право знати, коли ваші дані були зламані;

– забезпечення того, щоб політика конфіденційності була пояснена чіткою та зрозумілою мовою;

– посилення примусу та штрафів до 4% загального річного обороту фірми як захід стримання від порушення правил.

Пакет захисту даних також включає директиву щодо передачі даних для поліцейської та судової цілей. Також вперше встановлюються мінімальні стандарти обробки даних для цілей поліцейської діяльності в кожній державі-члені.

Нові правила спрямовані на захист потерпілих від злочинів, злочинців чи свідків, шляхом встановлення чітких прав та обмежень на передачу даних з метою запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань, включаючи запобігання і захист від загроз громадської безпеки, одночасно сприяючи більш плавному та більш ефективному співробітництву правоохоронних органів.

Крім того, 17 травня 2016 р. Рада ЄС офіційно прийняла перше законодавство ЄС щодо кібербезпеки – Директиву про мережеву інформаційну безпеку - яка набрала чинності в серпні 2016 року [2].

Директива зобов’язує "операторів основних послуг" у секторах високого ризику, таких як енергетика, транспорт та фінанси, вживати заходів для мінімізації їхнього кіберризику та повідомляти про певні кіберінциденти. Ця Директива доповнює Регламент про захист даних, який був прийнятий в квітні 2016 р. і застосовуватиметься з травня 2018 р.

Як тільки Директива набере чинності, державам-членам ЄС надається 21 місяць для її перенесення до національного законодавства, однак ділові стосунки повинні готуватися вже зараз.

Відповідно до Директиви підприємства повинні приймати "відповідні та пропорційні технічні та організаційні заходи", щоб мінімізувати вплив інцидентів кібербезпеки та забезпечити безперервність своїх послуг.

Національні регулюючі органи визначать конкретні заходи, які слід вжити. Ці заходи можуть включати в себе кроки, які компаніям з інфраструктури слід прагнути здійснити, щоб мінімізувати ризики, такі як:

– забезпечення відповідного корпоративного управління та процедур дотримання;

– забезпечення належного забезпечення та моніторингу технологічних систем та мереж;

– забезпечення навчання працівників та обізнаності про кіберризики;

– забезпечення виконання плану безперервності бізнесу та плану реагування на інциденти (із залученням персоналу з інформаційних технологій, правових, кадрових та маркетингових);

– переглянути існуючі контракти, щоб забезпечити їх адекватну ревізію систем постачальників, захист від форс-мажорних обставин, обмеження відповідальності та повідомлення про кіберінциденти.

Підприємства, що підпадають під дію Директиви, також повинні звітувати – "без зайвої затримки" – про будь-які інциденти, які суттєво впливають на безперервність своїх послуг. Підприємства повинні оцінювати, чи інциденти підлягають звітуванню з урахуванням: (i) тривалості інциденту; (ii) кількість користувачів, які зазнали порушення служби; і (iii) географічне поширення території, на яку вплинув інцидент. Очікується, що національні органи влади спільно співпрацюватимуть з Європейським агентством з мереж та інформаційної безпеки для розробки керівних принципів щодо випробувань для обов'язкового повідомлення.

Директива вимагає від національних органів влади консультуватися з суб'єктом господарювання, що звітує, перш ніж публічно повідомляти про інцидент. Інциденти будуть оприлюднені лише у випадках, коли поширення такої інформації необхідне для подолання інциденту або попередження подальшого інциденту.

З недержавних організацій в країнах ЄС велику роботу проводить Рада адвокатських асоціацій та юридичних спільнот Європи (CCBE), заснована в 1960 році, яка є міжнародною некомерційною асоціацією, що з моменту її створення була на передньому краї просування поглядів європейських юристів та захисту правових принципів, таких як демократія і верховенство закону.

Рада стверджує, що конфіденційність є ключовим принципом професії адвоката, а знання основ інформаційної безпеки для адвоката є вкрай необхідними. Також Рада наполягає на обов'язковому впровадженню в адвокатських компаніях стандарту систем управління інформаційною безпекою ISO/IEC 27001 [3].

Інформаційна безпека адвокатської діяльності в країнах-членах НАТО також має чітке правове регулювання.

Так, у Канаді, яка є однією із країн-засновниць і активним членом НАТО, підприємства та організації усіх форм власності, які збирають, зберігають та поширюють персональну інформацію, – зобов'язані дотримуватися вимог Акту захисту персональної інформації та електронних документів (PIPEDA).

PIPEDA набрав чинності з 1 червня 2009 року і його поточна редакція є станом на 26 березня 2018 року. Вказаний акт по суті є пошуком балансу між правами приватності особи з повагою до її персональної інформації та потребами організацій у збиранні, зберіганні та поширенні персональної інформації для потреб своєї діяльності.

Адвокати в Канаді постійно отримують особисту інформацію про своїх клієнтів та інших осіб. Хоча адвокати вже давно підлягають юридичним та професійним обов'язкам щодо збору, використання та розголошення такої інформації, адвокати також повинні ретельно розглянути їх відповідність законам про конфіденційність, включаючи, де це можливо, PIPEDA.

У деяких випадках вимоги PIPEDA відображають існуючі професійні вимоги до адвокатів. В інших випадках слідування вимогам PIPEDA може посилити складність в юридичній практиці.

Згідно із вимогами PIPEDA канадські адвокати повинні не лише розглядати власні зобов'язання щодо конфіденційності, але також різні зобов'язання, з якими може стикнутися кожен з їхніх клієнтів. Політика конфіденційності, яка застосовується до клієнтів, іноді може обмежувати те, що адвокати можуть використовувати для особистої інформації, яку вони збирають, використовують або розголошують від імені своїх клієнтів [4].

У 2012 році Комісія з питань етики 20/20 Американської асоціації адвокатів змінила виноску {6} до правила 1.1 Типових правил професійної відповідальності стосовно рівня компетенції адвоката щодо представництва клієнтів.

Поправка, конкретно вказує: {6} Щоб зберегти необхідні знання та навички, адвокат повинен бути в курсі змін у законодавстві та його практиці, включаючи переваги та ризики, пов'язані з відповідними технологіями, займатися постійним навчанням та відповідати всім вимогам щодо юридичної освіти, які встановлені для адвоката. Хоча (штат) Нью-Йорк ще не прийняв типових правил, вони все більше стають стандартом в інших державах, і це майже напевно є провісником керівних принципів, які будуть потрібні на загальнонаціональному рівні в найближчому майбутньому. Навіть якщо формально не буде кодифіковано в Нью-Йорку в цей час, як і раніше, основні етичні заповіді щодо збереження конфіденційності чутливої інформації про клієнта – вимагається від адвокатів цього штату запобігання порушенням етики, спричиненими несанкціонованим доступом до привілейованої інформації клієнта, такої як інтелектуальна власність, інформація в очікуванні комерційної

угоди, адвокат-клієнтські повідомлення тощо, навіть якщо така інформація передається по електронній пошті. Окрім етичних вимог до адвоката, певні статути або правила можуть встановлювати додаткові зобов'язання щодо кібербезпеки для адвоката, виходячи з виду діяльності, що проводиться клієнтом [5].

З 2016 року Федеральне бюро розслідувань Сполучених Штатів Америки працює із юридичними компаніями із використанням системи InfraGard. Передумовою такої роботи стало значне зростання хакерських атак на юридичні компанії в США: від одиничних у 2009 році, двостах атак у 2011 році та десятків тисяч атак вже у 2016 році [6].

InfraGard – є некомерційною організацією, яка забезпечує партнерство між ФБР та членами приватного сектору. Програма InfraGard служить інструментом для безперервної співпраці державного та приватного секторів з урядом, що покращує своєчасний обмін інформацією та сприяє взаємній навчанню можливостей, що стосуються захисту критично важливої інфраструктури.

Список використаних джерел:

1. Data protection reform – Parliament approves new rules fit for the digital era. Press realese. – European Parliament. 14.04.2016 [Електронний ресурс]. – Режим доступу: http://www.europarl.europa.eu/news/en/press-room/20160407 IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era. – Назва з екрана.
2. EU-wide cybersecurity rules adopted by the Council. Press realese. – European Council. Council of the European Union. 17.05.2016 [Електронний ресурс]. – Режим доступу: http://www.consilium.europa.eu/en/press/press-releases/2016/05/17/wide-cybersecurity-rule-adopted/. – Назва з екрана.
3. CCBE guidance on Improving the IT Security of Lawyers Against Unlawful Surveillance. – Council of Bars and Law Societes of Europe. – 24 p. – [Електронний ресурс]. – Режим доступу: http://www.ccbe.eu/ fileadmin/ speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommentations/EN_ITL_20160520_CCBE_Guidance_on_Improving_the_IT_Security_of_Lawyers_Against_Unlawful_Surveillance.pdf – P. 2–4, 11–13. – Назва з екрана.
4. PIPEDA and Your Practice. A privacy handbook for lawyers. – Ottawa - Ontario : Office of the Privacy Commissioner of Canada, 2011– 26 p. – ISBN: 978-1-100-53540-1. P. 3–7.
5. Increasing Cybersecurity Requirements for Lawyers. – Stephen Treglia, New York Law Journal. May 30, 2017. [Електронний ресурс]. – Режим доступу: http://www.newyorklawjournal.com/printerfriendly/id=1202787639146 . – Назва з екрана.
6. Locked Down. Practical information security for lawyers. 2nd Edition. - David G Ries, John Simek, Sharon D Nelson. – American BAR Association, 2016 – 370 p. –ISBN: 978-1-63425-414-4.

----------***----------

Бежевець А. М., *старший викладач*
ФСП КПІ ім. Ігоря Сікорського.

GDPR ЯК НЕОБХІДНА УМОВА ЗАБЕЗПЕЧЕННЯ ПРАВА НА ІНФОРМАЦІЙНУ ПРИВАТНІСТЬ

В умовах формування інформаційного суспільства одним з основних завдань сучасної держави є забезпечення інтересів особистості, її прав і свобод. Будь-які трансформації в суспільстві мають відбуватися з неухильним дотриманням прав і свобод громадян, оскільки, відповідно до ст.3 Конституції України утвердження і забезпечення прав і свобод людини є головним обов'язком держави.

Повсюдне використання інформаційних технологій, великих масивів інформації, хмарних обчислень, інтернету речей, блокчейну тощо дає суспільству не тільки беззаперечне благо, але і створює нові загрози, наприклад, неконтрольоване зберігання та обробка даних про особу.

Подальше поширення сучасних інформаційних технологій може призвести до того, що сам факт існування приватного життя опиниться під загрозою.

Автором вже досліджувалося питання приватності та стан регулювання цього права за законодавством України. Зокрема, автором запропоновано одним з видів приватності визначити інформаційну приватність, яка полягає у забезпеченні безпеки при збиранні та обробці інформації про людину (персональні дані).

З урахуванням цих та інших пропозицій та висновків, зроблених автором раніше, пропонується продовжити досліджувати питання правового інституту персональних даних у зв’язку із прийняттям Регламенту ЄС 2016/679 (GDPR — General Data Protection Regulation, далі - GDPR).

Усвідомлюючи важливість інституту персональних даних як складової правового статусу особистості, європейською спільнотою 27 квітня 2016 року прийнято зазначений Регламент з метою сприяти досягненню свободи, безпеки та справедливості і економічного союзу, економічному та соціальному прогресу, зміцненню законності і зближенню економіки на внутрішньому ринку ЄС і добробуту фізичних осіб. GDPR - найважливіший законодавчий документ, який суттєво підвищує рівень захисту персональних даних громадян ЄС, як всередині країн-членів, так і за межами ЄС.

GDPR є нормативно-правовим актом, який почне діяти у країнах ЄС наприкінці травня 2018 року. Важливою особливістю GDPR є екстериторіальний принцип дії, суть якого полягає в обов’язковості виконання

GDPR всіма юридичними особами, що обробляють персональні дані резидентів і громадян ЄС, незалежно від їх місцезнаходження.

GDPR в своїй преамбулі ясно вказує, що при обробці персональних даних необхідно дотримуватися основних прав і свобод людини, зокрема поваги до приватного і сімейного життя, житла і комунікацій, захисту особистих даних, свободи думки, совісті і релігії, свободи вираження поглядів та інформації, свободи ведення бізнесу, права на ефективний засіб правового захисту і справедливий судовий розгляд, культурне, релігійне та мовне розмаїття.

Стаття 2 Закону України «Про захист персональних даних» закріплює, що персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

У статті 4 GDPR визначено, що персональними даними є будь-яка інформація, що стосується ідентифікованого або ідентифіковуваної фізичної особи («суб'єкт даних»); ідентифіковувана особа – це особа, яка може бути ідентифікована прямо або опосередковано, зокрема, за допомогою посилання на ідентифікатор, такий як ім'я, ідентифікаційний номер, дані про місце розташування, онлайновий ідентифікатор або один або кілька факторів, специфічних для фізичної, фізіологічної, генетичної, розумової, економічної, культурної або соціальної ідентичності цієї фізичної особи. Зазначене визначення широке і досить чітко дає зрозуміти, що навіть IP адреси можуть бути персональними даними.

Таким чином, порівнюючи вказані визначення, підставно стверджувати, що законодавство України про захист персональних даних потребує подальшого вдосконалення з метою уточнення (розширення) відомостей, за допомогою яких особа може бути ідентифікована (персональні дані) з метою забезпечення права особи на інформаційну приватність.

Доцільно звернути увагу на те, що статею 9 GDPR передбачено можливість заборони обробки спеціальних категорій персональних даних. До них відносяться: дані, які розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання або членство в профспілках, а також генетичні дані, біометричні дані, які використовуються з метою однозначної ідентифікації фізичної особи, дані про здоров'я або дані, що стосуються сексуального життя або сексуальної орієнтації фізичної особи.

Формування адекватного режиму правового регулювання відносин у сфері персональних даних є важливою гарантією прав особистості, що дозволяє контролювати обробку інформації про себе і, в першу чергу, визначати порядок і умови доступу до неї.

Враховуючи взятий Україною курс євроінтеграції, з метою реального забезпечення сповідуваних демократичних цінностей, підставно стверджувати, що GDPR потребує уважного вивчення та імплементації його норм у

законодавство України для дотримання права на інформаційну приватність кожної особи.

----------***----------

Солончук І. В., *ст. викладач кафедри інформаційного права та права інтелектуальної власності КПІ ім. Ігоря Сікорського.*

ОФІЦІЙНА ЕЛЕКТРОННА АДРЕСА: ПОТРЕБИ ТА ПРОБЛЕМИ ЗАПРОВАДЖЕННЯ

Дотримання прав, свобод та забезпечення безпеки людини в інформаційній сфері на сьогодні є одним із провідних завдань державної політики, оскільки не можливо уявити жодну сферу суспільного життя, яка б не була пронизана «інформативно». Сучасні інформаційні технології значно полегшують роботу державних інституцій, водночас проблема захисту інформації набуває дедалі складнішого характеру та вимагає детального наукового вивчення й аналізу. Дослідженню цього питання присвячена значна кількість наукових праць, науково-практичних конференцій та круглих столів. Але дана робота є спробою погляду на проблему дотримання прав та свобод людини в інформаційній сфері з точки зору новел цивільного судочинства.

Стрімкий розвиток інформаційного права спровокував інтеграційні інформаційні процеси у правовій системі суспільства. Не залишається осторонь і цивільне судочинство, яке на сьогодні перебуває в стані реформування та зазнає прогресивних змін, значна частина яких пов’язана із використання сучасних інформаційних технологій для досягнення загальної мети – покращення процесу відправлення правосуддя при розгляді та вирішенні судами цивільних справ.

Зі змінами в Цивільному процесуальному кодексі (далі – ЦПК) України, внесеними Законом № 2147-VIII від 03.10.2017, цивільне судочинство України відображає ряд вагомих новел, сприйнятих міжнародним співтовариством та вже існуючих в інших державах [1]. Так згідно ст. 14 ЦПК України в усіх судах нашої держави функціонує Єдина судова інформаційно-телекомунікаційна система (далі – ЄСІТС), яка прийшла на зміну Автоматизованій системі документообігу суду та представляє собою систему вищого рівня, здатну виконувати ширше коло завдань, а саме:

– обов’язкову реєстрацію позовних та всіх інших заяв, скарг, процесуальних документів, які надходять до суду,

– здійснення визначення судді або колегії суддів (судді-доповідача) для розгляду конкретної справи,

– забезпечення обміну документами (надсилання та отримання документів) в електронній формі між судами, між судом та учасниками судового процесу, між учасниками судового процесу,

– фіксування судового процесу за допомогою відео- та (або) звукозаписувального технічного засобу,

– можливість проведення участі особи - учасника судового процесу у судовому засіданні в режимі відеоконференції [2].

Особливо цікавим є нововведення, яке стосується судових повісток. Проблема вручення судової повістки є актуальною в будь-якому судовому процесі, оскільки безпосередньо впливає на рух справи. Що стосується цивільного судочинства, то в цивільному процесуальному законі з'явилося нове поняття – офіційна електронна адреса. Якщо особа має офіційну електронну адресу, то суд направляє судові повістки та інші процесуальні документи учаснику судового процесу на його офіційну електронну адресу. Але попередньо учасник цивільного процесу має зареєструвати свою офіційну електронну адресу в ЄСІТС. І тут Законодавець поділяє учасників процесу на дві категорії: ті, що реєструють офіційну електронну адресу в обов'язковому порядку, та ті, які добровільно реєструють офіційну електронну адресу в ЄСІТС. До осіб, які реєструють офіційні електронні адреси в ЄСІТС в обов'язковому порядку, ЦПК України відносить: адвокатів, нотаріусів, приватних виконавців, арбітражних керуючих, судових експертів, державні органи, органи місцевого самоврядування, суб'єктів господарювання державного й комунального секторів економіки. Всі інші учасники цивільного процесу, зокрема громадяни, добровільно реєструють свою офіційну електронну адресу в ЄСІТС.

Але слід зазначити, що на сьогодні не існує чіткого нормативного визначення поняття «офіційна електронна адреса». У Верховній раді України 26 грудня 2017 року зареєстровано проект Закону № 7443 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. В даному проекті Закону № 7443 пропонується наступне визначення: офіційна електронна адреса - адреса електронної пошти юридичної особи та фізичної особи-підприємця, що використовується для офіційного листування в електронному вигляді та є незмінною до внесення запису про державну реєстрацію припинення юридичної особи, припинення підприємницької діяльності фізичної особи; всі листи, повідомлення, які надсилаються на офіційну електронну адресу, вважаються такими, що надіслані офіційно, та не потребують додаткового документального підтвердження [3]. На основі такого розуміння можемо зробити висновок, що офіційну електронну адресу пропонується присвоювати «автоматично» під час

державної реєстрації створення юридичної особи або ж при реєстрації статусу фізичної особи-підприємця. Проаналізувавши положення зазначеного проекту Закону, можемо констатувати, що наявність офіційної електронної адреси Законодавець пов'язує виключно з юридичними особами та фізичними особами-підприємцями. Що ж стосується поняття та порядку реєстрації офіційних електронних адрес фізичних осіб, то це питання потребує негайного доопрацювання на законодавчому рівні, оскільки є неприпустимими обмеження в правах різних груп суб'єктів цивільних процесуальних правовідносин. ЦПК України передбачає, що фізичні особи мають право зареєструвати свою офіційну електронну адресу в ЄСІТС в добровільному порядку, що надає їм можливість скористатися всіма перевагами та зручностями ЄСІТС. Адже всім особам, які виконали зазначену реєстрацію, суд матиме змогу та, одночасно, зобов'язання надсилати будь-які документи у справах, в яких такі особи беруть участь, виключно в електронній формі шляхом їх направлення на офіційні електронні адреси таких осіб, що не позбавляє їх права отримати копію судового рішення у паперовій формі за окремою заявою [4, с. 169].

Підсумовуючи, можемо зазначити, що запровадження в судах ЄСТІС є вагомим кроком у реформуванні судової системи України. Водночас, є ряд недоліків, які уповільнюють прогресивні реформаційні процеси. Зокрема, Законодавцем до цього часу не визначено, коли саме або ж, принаймні, до якого саме року, має почати функціонувати ЄСІТС. Також є незрозумілим, невизначеним поняття офіційної електронної адреси для фізичної особи, а також порядок її реєстрації. Таким чином, з впевненістю та прикрістю можемо стверджувати, що права і свободи людини в інформаційній сфері в контексті цивільного судочинства зазнали прогресивних кроків лише, як кажуть, «на папері», а на практиці – продовжує функціонувати Автоматизована система документообігу суду, яка не в змозі забезпечувати всі можливості сучасних інформаційних технологій з метою покращення захисту прав, свобод та інтересів людини та належним чином гарантувати безпеку учасників цивільного процесу в інформаційній сфері.

Список використаних джерел:

1. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України ... : Закон від 03.10.2017 № 2147-VIII / Верховна Рада України. Київ: ВВРУ, 2017. № 48. Ст.436.

2. Цивільний процесуальний кодекс України: Кодекс України, Закон від 18.03.2004 № 1618-IV / Верховна Рада України. Київ: ВВРУ, 2004. № 40, 41, 42. Ст. 492.

3. 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 № 7443 від 26.12.2017 // База даних «Законодавство України» / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/498_604 (дата звернення – 09.03.2018).

4. Солончук І. В. Інформаційні правовідносини в контексті цивільного судочинства. *Інформація і право*. №1(24)/2018. С. 164 – 173.

----------***----------

Литвинова Л. А., *кандидат наук із соціальних комунікацій, с.н.с. НБУВ.*

НОВІ МЕХАНІЗИ РЕГУЛЮВАННЯ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В МЕРЕЖІ ІНТЕРНЕТ

Міжнародний альянс інтелектуальної власності (IIPA)[12] у щорічному звіті про міжнародний стан охорони прав інтелектуальної власності, відомий як «Special 301 report», опублікованому Офісом торгового представництва США (USTR), включив Україну в Priority Watch List 2017 – список «піратських» країн, де найбільше порушуються права інтелектуальної власності в світі [1]. До цього списку головних порушників потрапили ще 7 країн: Китай, Чилі, Індія, Мексика, Росія, Тайвань і В'єтнам[13]. Із країною, яка потрапила в цей список, складаються певні економічні відносини, позбавлені довіри, застосовуються санкції. Все це позначається на інвестиційній привабливості України, а українських підприємців відмовляються сприймати всерйоз.

Україна двічі очолювала список «Priority foreign country», – у 2001 та в 2013 році – в обох випадках позбавляючись членства в «Загальній системі привілеїв» (GSP) – програмі американського уряду із підтримки економічного росту країн, що розвиваються, в рамках якої в США щорічно без мита завозились українські товари на суму до $70 млн (2012 р.).

Згідно зі звітом Міжнародного альянсу інтелектуальної власності, Україну рекомендовано залишити в списку пріоритетного спостереження, оскільки будь-яких глобальних змін, щодо дотримання авторських прав, в країні не спостерігається.

Як говориться в офіційному звіті альянсу, причинами через які Україну занесено до Priority Watch List були:

[12] Міжнародний альянс інтелектуальної власності (IIPA) - коаліція приватного сектора, заснована в 1984 для подання авторсько-правових галузей виробництва США і в двосторонніх і багатосторонніх зусиллях для поліпшення міжнародного захисту матеріалів, захищених авторським правом. До альянсу входить сім торгових асоціацій, кожна з яких представляє значний сегмент авторсько-правової спільноти США

[13] Залежно від ступеня тяжкості проступку, «країни-порушники» потрапляють в одну з трьох категорій: Watch list (країни під наглядом), Priority watch list (країни під першочерговим контролем), або ж Priority foreign country (пріоритетна країна).

– несправедливе, непрозоре адміністрування системи організацій колективного управління, які відповідають за збір і передачу роялті правовласникам в США та інших країн;

– широке (і очевидне) використання неліцензійного програмного забезпечення державними органами України;

– нездатність запровадження ефективних механізмів боротьби з порушенням авторського права в мережі Інтернет в Україні.

Експерти USTR позитивно оцінили окремі заходи, прийняті Україною в напрямку поліпшення захисту прав інтелектуальної власності, проте проблеми з інтернет-піратством в Україні завдають серйозних економічних збитків США.

Окремо в Спецдоповіді відзначається прийняття Верховною Радою закону «Про державну підтримку кінематографії в Україні» (набрав чинності 26 квітня 2017 р.) як відображення нової політичної волі держави щодо вирішення проблемних питань в сфері дотримання прав інтелектуальної власності.

Цим законом було внесено досить суттєві зміни до Закону України «Про авторське право і суміжні права», а також до Кримінального кодексу, Кодексу України про адміністративні правопорушення та інших законодавчих актів. Ці зміни так чи інакше пов’язано з процедурами захисту авторських прав в Інтернет.

Головні зміни стосуються Закону України «Про авторське право і суміжні права», уточнено та визначено нові терміни: «веб-сайт, веб-сторінка, власник веб-сайту, власник веб-сторінки, гіперпосилання, електронна (цифрова) інформація, камкординг, кардшейрінг, обліковий запис, постачальник послуг хостингу».

Зокрема, дається визначення поняттю «піратство у сфері авторського права і (або) суміжних прав» – це будь-яке використання об'єктів авторського права і (або) суміжних прав, у тому числі в мережі інтернет, без дозволу суб’єктів авторського права і (або) суміжних прав з урахуванням передбачених обмежень майнових прав.

Закон України «Про авторське право і суміжні права» доповнений новими статтями 52-1, 52-2, якими встановлюється порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі інтернет (ст. 52-1) та зобов’язання постачальників послуг хостінгу щодо забезпечення захисту авторського права і (або) суміжних прав з використанням мережі інтернет (ст. 52-2). Зокрема, суб'єкт зазначених прав у разі виявлення електронної (цифрової) інформації, що порушує авторське та (або) суміжні права чи посилання на таку інформацію онлайн має право звернутися до власника веб-сайту, веб-сторінки, локальної мережі, хостинг-провайдеру з вимогою про припинення порушення авторського права і (або) суміжних прав. Такий порядок захисту авторського права і (або) суміжних прав застосовується

до відносин, пов'язаних з використанням аудіовізуальних творів, музичних творів, комп'ютерних програм, відеограм, фонограм, передач (програм) організацій мовлення. Таким чином, цей порядок не застосовується до таких творів як фотографії, об'єкти графічного дизайну, літературні твори та бази даних. Але ж права авторів цих творів порушуються в мережі, можливо навіть, частіше, ніж права авторів музики або фільмів.

Необхідно зазначити, у процесі складання заяв-претензій обов'язовим є представництво (посередництво) адвоката, який перевіряє достовірність інформації та обгрунтання порушення авторських і (або) суміжних прав в Інтернеті. Такий підхід скоріш всього привиде до закріплення нової спеціалізації «адвокат з авторського права». Проте законодавець чомусь проігнорував патентних повірених та організації колективного управління, що може привести до недобросовісної конкуренції та зловживання праволасниками запитів.

Якщо після цієї заяви контент не буде заблоковано, тоді правовласник має право звернутися до суду, де він знову зіткнеться все з тією ж адвокатською монополією.

Варто заважити, у разі невиконання вищезазнених вимог щодо видалення (блокування) контенту, власники веб-сайт несуть відповідальність за порушення авторського та (або) суміжних прав.

Тобто внесені зміни до закону передбачають досудове видалення або блокування доступу до контенту і веб-сайту, при чому найчастіше провайдерами. Таким чином, будь-який контент і веб-сайт може бути заблоковано без суду.

Необхідно відмітити, що такий досудовий порядок видалення контенту або блокування доступу до нього суперечить положенням Договору про торгові аспекти прав інтелектуальної власності (TRIPS), який передбачає судову процедуру захисту порушення прав.

У цьогорічному звіті про охорону та захист авторського права, який Міжнародний альянс інтелектуальної власності опублікував та подав Торговому представнику Сполучених Штатів Америки, Україна залишилась у списку країн із значними проблемами у сфері охорони прав інтелектуальної власності [2].

Неупереджено оцінюючи ситуацію з рівнем охорони авторського права, Міжнародний альянс інтелектуальної власності у своєму звіті зазначає, що прийняттям законодавчих актів щодо протидії Інтернет-піратству, було введено нехай і недосконалу, але процедуру повідомлень про порушення авторського права в мережі Інтернет (takedown notice) з частковою відповідальністю хостинг-провайдерів. Крім того, ІІРА вважає, що у Законі України «Про авторське право і суміжні права» слід чітко визначити поняття «тимчасові копії», надати ліцензіатам зарубіжних компаній такі ж можливості для захисту

прав, як і вітчизняним суб'єктам прав. Прирівняти несплату роялті за використання музики та відрахувань за приватне копіювання до порушення авторського і/або суміжних прав, встановити розмір фіксованих збитків або розширених збитків.

Передбачено, що ці зміни до Закону допоможуть наблизити законодавчу базу України до законодавства ЄС, що забезпечить помітне зниження Інтернет-піратства в нашій країні, і як наслідок, не тільки поліпшить наш імідж в очах Заходу, а й благодійно позначиться на вітчизняній культурі та економіці. Для Украини дуже важливо позбутися негативного іміджу, що стосується Інтернет-піратства. Тільки так наша країна може залучити діючі бізнес-активи, а отже і масштабні інвестиції.

Список використаних джерел:

1. 2017 Special 301 Report. URL: https://ustr.gov/sites/default/files/301/ 2017 Special 301 Report FINAL.PDF (дата звернення: 01.04.2018).

2. 2018 Special 301 report oncopyright protection and enforcement. URL: https://iipa.org/files/uploads/2018/02/2018_SPECIAL_301.pdf (дата звернення: 01.04.2018).

----------***----------

Куцик К. М., *ст. викладач кафедри філософії КПІ ім. Ігоря Сікорського.*

ЗАХИСТ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В СОЦІАЛЬНО-ГУМАНІТАРНИХ ДОСЛІДЖЕННЯХ (НЕЮРИСДИКЦІЙНИЙ АСПЕКТ ПРОБЛЕМИ)

Єдиним можливим способом захисту інтелектуальної власності в реаліях вітчизняної дійсності є академічна доброчесність. Для того, щоб вона стала нормою існування наукової спільноти, потрібна з'ява неформальних корпоративних об'єднань з духовно усвідомленою орієнтацією на моральний авторитет вченого, його гідність, культуру самосвідомості та спілкування, соціальний престиж професійної наукової діяльності. Якщо таке духовне самоконструювання ствердиться не лише як ціннісний ідеал, але і як умова та норма існування нових неформальних корпорацій, то вони здатні будуть творити аудиторію за власним типажом. Спробуємо аргументувати дану тезу.

Каральні заходи з позиції цивільно-кримінально-адміністративного права не дають помітних позитивних результатів у захисті інтелектуальної власності та все ще залишаються малодійними, оскільки цільна, цілісна система такого захисту в Україні все ще відсутня. І як будь яка система, правова також, не може охопити всієї повноти наявних суспільних елементів, які б відтворювали всі можливі їх взаємозв'язки та були зафіксовані

правовими законами. Правове поле залишає своєрідний люфт для дій поза законом. Тобто, всі складові тих негативних тенденцій, що створювались десятиліттями у вітчизняному академічному середовищі, не завжди можуть бути виявлені правовими нормами та законодавчими актами.

Свідченням того, наскільки соціально актуальною та болісною для академічного середовища є проблема недоброчесності, є публікації в періодичних виданнях, в мережі Інтернет, створений рух за академічну доброчесність та його діяльність, програма співпраці США та України «Проект сприяння академічній доброчесності в Україні (SAIUP)», наради у МОН та проведений круглий стіл про плагіат… Уряд ухвалив постанову, що посилює відповідальність за порушення академічної доброчесності під час отримання вчених звань [1].

А.А.Мельниченко, декан ФСП, в статті «Прояви академічної нечесності» виклав аргументовано послідовне дослідження причин та проявів форм академічної нечесності [2, с. 107-121].

Є. Ніколаєв, один з учасників руху за академічну доброчесність, критикує та негативно оцінює діяльність учасників атестаційного процесу (загальновідомий факт скасування МОН рішення про присудження наукового ступеня чотирьом дисертантам за зверненням активістів ініціативи «Дисергейт» (лист МОН № 1/11-3930 від 06.04.2018 р.)) та наголошує, що владні намагання шукати централізованих рішень «згори»- це неефективний шлях, оскільки «за поодинокими випадками (Швеція і Норвегія) розвиненим країнам взагалі не властива регламентація питань академічної доброчесності з боку органів влади, ці питання є виключно компетенцією автономних академічних спільнот» [3]. Сайт «Освітня політика» пропонує гостро критичні публікації про необхідність змін у вітчизняному академічному середовищі, розглядаються глибинні причини кризи академічної спільноти, вносяться рекомендації щодо подолання академічної недоброчесності [4].

С.Єсилевський, науковець, пропонує створити «альтернативне незалежне співтовариство вчених, на трьох базових засадах:

– беззастережне дотримання академічної чесності та професійної етики;

– інтегрованість у світову науку;

– абсолютний бойкот та розмежування з людьми та організаціями, що підтримують карго-культ, імітацію наукової діяльності та порушення академічної етики» [5].

На нашу думку, сподіватись на зовнішній чинник- чи то правовий, чи на новостворену структуру… в спробі навернення наукової спільноти до цивілізаційних норм обрамлення наукової діяльності – «марнота марнот та ловлення вітру». Ліміт даного чинника вичерпав себе. Дисциплінарна академічна спільнота, за визначенням, як спільнота еліт, за свідомою волею та

бажанням мала б обрати таке поводження, яке б стало взірцево-заразливим, ідеалом для наслідування. Умовно цей рух можна було б назвати самоорганізованим клубом, корпорацією (цехом) джентльменів. Імітатори від науки почуваються тут зайвими. Саме середовище регулює проблеми наукової доброчесності. Наукова репутація мала б стати брендом. Створюються умови, коли плагіат стає справою невигідною і не престижною.

Виникла парадоксальна ситуація: в науковому співтоваристві є цікаві творчі особистості, але допоки що корпоруватись в нову спільноту, яка б існувала за правилами цивілізованого світу, їм не вдається. І оскільки проблема усвідомлена, то розпочатий рух протидії кризовим явищам в академічній спільноті розгортається.

Список використаних джерел:

1. http://konkurent.in.ua/news/ukrayina/25865/akademichna-nedobroche snist -za-plagiat -pozbavlyatimut-vchenih-zvan.html&lang=uk

2. Академічна чесність як основа сталого розвитку університету/ За заг. ред. Т.В.Фінікова, А.Є.Артюхова – К.; Таксон, 2016. – 234 с.

3. http://education-ua.org/ua/articles/1181-kultura-akademichnoji-nedobro chesnosti-kejs-plagiatnikh-filosofskikh-disertatsij

4. https://osvita.ua/vnz/high_school/60290/

5.https://site.ua/yesint/12423-dostalo-ili-prizyv-k-samoorganizatsii-chestnyh-uchenyh/

----------***----------

Завальнюк А. М., *студентка ФСП КПІ ім. Ігоря Сікорського.*
*Науковий керівник****: Фурашев В.М.,***
к. т. н., доцент ФСП КПІ ім. Ігоря Сікорського.

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРАВА ЛЮДИНИ НА ВИНАХІД В СУЧАСНОМУ СУСПІЛЬСТВІ

Невід’ємною складовою сьогодення став бурхливий розвиток технологій. Науково-технічний процес зумовив виникнення нової суспільної реальності, в якій людська праця замінюється розумними технологіями, а на перше місце виходить людина, її інтелектуальний та творчий потенціал. Розвиток технологій дозволяє звільнити людину від рутинної, брудної роботи, надавши їй можливості для інтелектуального розвитку. Однак, у новій системі розумних технологій людина повинна знайти своє місце. Оскільки саме людині притаманна вища форма розвитку нервової системи – мислення, отож людина у цій новій системі має постати творцем [1].

Сучасне життя вимагає від кожного з нас реалізації творчого потенціалу, креативності. Інтелектуальна власність на сьогодні стала важливим об'єктом цивільного обігу, а тому питання забезпечення права людини на винахід у сучасному суспільстві вбачається актуальним.

Винахід – це результат інтелектуальної діяльності людини в певній сфері технології. Завдяки винахідництву забезпечується розвиток науки й техніки, здійснюється рух суспільства вперед. Для України питання забезпечення права на винахід є особливо важливим, оскільки саме Україна стала Батьківщиною для багатьох винахідників. Ігор Сікорський, Сергій Корольов, Сергій Глушков, Микола Амосов – це лише невелика частка видатних українців, винаходи й інтелектуальні досягнення яких стали революційними у галузі авіатехніки, космічної техніки, кібернетики та медицини. Однак, й на сьогодні в Україні існують винахідники. Проте велика частина з них вимушені шукати кращої долі за кордоном [2].

На сьогодні законодавством врегульовані питання реєстрації винаходу, встановлені правові гарантії щодо винахідників. Однак, очевидно, цього є недостатньо, оскільки тенденція відтоку мізків зберігається.

На нашу думку, правове забезпечення щодо права людини на винахід в Україні містить ряд проблемних аспектів.

По-перше, відсутність стимулів для винахідництва в Україні. Так, законом не передбачено чіткого матеріального та морального заохочення винахідників. Таке заохочення могло б мати певні привілеї щодо розміру пенсії, отримання винагороди з державного бюджету, податкові привілеї в частині використання винаходу у комерційній діяльності. Відсутня належна пропаганда корисності винахідницької діяльності. Тривалий час наука фінансується за залишковим принципом, через що втрачаються стимули до ефективної діяльності на користь Батьківщини [4].

По-друге, дещо зарегульованою є процедура реєстрації винаходу. Так, обов'язковим при отриманні патенту є проходження експертизи, яка, як правило, затягується на тривалий час, котрий для кожної людини є цінним [3].

По-третє, недостатньо розвиненою є як правова база, так і сама фактична діяльність венчурних та інвестиційних фондів. За таких умов не забезпечується комунікація між бізнесом та винахідниками, через що людина не може повноцінно реалізувати право на винахід [1].

Отже, основними проблемами в реалізації права людини на винахід у сучасному суспільстві є наступні:

– зарегульованість процедур щодо патентування винаходу;

– слабка комунікація між бізнесом та винахідниками через нерозвиненість правової бази;

– незахищеність винахідників з боку держави;

– низький рівень матеріального стимулювання: в частині соціального (пенсійного) забезпечення, податкових пільг та матеріальної винагороди за винахід;

– низький рівень пропаганди винахідництва в державі. Відсутня державна політика щодо підвищення престижу винахідників, укріплення високої ролі винахідників у суспільній свідомості.

На сьогодні є потреба у покращенні не лише правового забезпечення, а й у запровадженні цільової державної політики, спрямованої на підвищення винахідницького потенціалу в Україні.

По-перше, слід забезпечити винахідників державними матеріальними винагородами (державними стипендіями та грантами), пільговими пенсійними та податковими умовами.

По-друге, слід спростити порядок отримання патенту на винахід, прискорити цю процедуру.

По-третє, необхідно створити сприятливі умови для розвитку бізнесу, до якого залучаються винаходи, запатентовані в Україні. Це може бути створення сприятливих податкових умов (звільнення від оподаткування, пільгові податкові ставки), надання державних цільових кредитів, запровадження національної програми фінансування винаходів в Україні.

Зрештою, держава має пропагувати важливість винахідництва. Підкреслювати у свідомості підростаючого покоління значимість інтелектуальної праці людини.

Список використаних джерел:

1. Гайдедей Ю.І. Актуальні проблеми реалізації права на винахід [Електронний ресурс]. – Режим доступу: http://legalactivity.com.ua/index.php ?option=com_content&view=article&id=221%3A120223-09&catid=37%3A-3&Itemid=54&lang=ru

2. Семенок О. Проблемні аспекти правового регулювання промислової власності [Електронний ресурс]. – Режим доступу: https://www. businesslaw. org.ua/ pravove-reguluvannya-promyslovoi-vlasnosti/

3. Работягова Л. Винахід і корисна модель як об’єкти договірного регулювання [Електронний ресурс]. – Режим доступу: http://www.inprojo urnal.org/ wp-content/uploads/2016/11/Rabotiagova-216.pdf

Кук О. Молоді науковці масово емігрують з України: вчені назвали причини [Електронний ресурс]. – Режим доступу: https://24tv.ua/molodi _naukovtsi_ masovo_emigruyut_z_ukrayini_vcheni_nazvali_prichini_n924862

----------***----------

Гожій І. О., *ст. викладач ФСП КПІ ім. Ігоря Сікорського.*

ПРАВО НА ОТРИМАННЯ ІНФОРМАЦІЇ ЩОДО ЗНИКЛОГО БЕЗВІСТІ ІНОЗЕМЦЯ

18 січня 2018 року Верховною Радою України був прийнятий у першому читанні Закон «Про правовий статус осіб, зниклих безвісти» (далі - Закон) [1], який забезпечує правове регулювання відносин, пов'язаних з обліком та розшуком осіб, зниклих безвісти через збройний конфлікт в України.

Управлінням Верховного комісара ООН з прав людини було підготовлено декілька доповідей щодо ситуації з правами людини в Україні. Доповіді ґрунтуються на даних, які Моніторингова місія ООН з прав людини отримала під час роботи в Україні. Зокрема, двадцята та двадцять перша доповіді охоплюють періоди, відповідно, з 16 серпня до 15 листопада 2016 року та з16 листопада 2017 року до 15 лютого 2018 року. Серед інших питань, які розглядаються у доповідях, звертається увага на значну кількість цивільних осіб, які загинули або зникли безвісти у зв’язку зі збройним конфліктом на території України. Крім того, було наголошено на відсутності координації діяльності між державними органами щодо встановлення кількості зниклих безвісті осіб та механізму їх розшуку[2;3]. Рекомендації стосовно необхідності створення такого механізму неодноразово надавалися Україні авторитетними міжнародними організаціями. Так, Парламентська Асамблея Ради Європи ще у 2015 році ухвалила резолюцію, присвячену долі осіб, які зникли безвісти внаслідок російської агресії в Україні, в якій міститься рекомендації для української влади щодо створення ефективного механізму розшуку зниклих осіб [4]. Прес-секретар Міжнародного комітету Червоного Хреста Міладін Богетич на брифінгу, який був проведений у березні цього року, зазначив, що за весь час воєнного конфлікту зниклими безвісти вважаються 1500 осіб, причому половина з них - цивільні особи [5]. Незаперечним є той факт, що серед осіб, які зникли безвісти внаслідок збройної агресії Російської Федерації проти України, є іноземні громадяни та особи без громадянства.

Закон визначає, що іноземець та особа без громадянства, які зникли на території України, набувають правового статусу осіб, зниклих безвісти, в орядку, передбаченому законом, за умови, що такі особи постійно або тимчасово проживали на території України або якщо існує достовірна інформація, що зникнення відбулося на території України, хоча особа постійно не проживала на території України [1]. Це положення в повній мірі відповідає приписам ст.26 Конституції України [6] та ст.3 Закону України "Про правовий статус іноземців та осіб без громадянства" [7], а також статті 3 Керівних принципів/Модельного закону щодо осіб, зниклих безвісти, розроблених

Міжнародним Комітетом Червоного Хреста (далі - Модельний закон) [8], щодо правового статусу іноземців у країні перебування. Крім того, ст.7 Закону забороняє будь - яку дискримінацію як осіб, зниклих безвісті, так і їх родичів на підставі їхньої раси, кольору шкіри, статі, віросповідання, політичних чи інших поглядів, національного чи соціального походження.

Право знати про долю своїх зниклих родичів передбачено міжнародним правом прав людини та міжнародним гуманітарним правом. Женевська конвенція про захист цивільного населення під час війни [9] та Додатковий протокол до Женевських конвенцій стосовно захисту жертв міжнародний збройних конфліктів [10] вміщують норми щодо права родичів отримати інформацію стосовно зниклої особи, загальний зміст яких можна визначити наступним чином: особа має право знати про обставини зникнення рідної людини, а у випадку смерті – про обставини загибелі і місце поховання. Влада зобов'язана інформувати родичів про хід розслідування та про його результати. Відповідно до Закону, родичі зниклої безвісті особи, в тому числі іноземця, можуть реалізувати право на отримання інформації щодо зниклого безвісті шляхом подання запиту до Комісії з питань осіб, зниклих безвісті (далі – Комісія), утворення якої передбачено з метою забезпечення координації діяльності органів, уповноважених на облік та розшук осіб, зниклих безвісти. Серед основних завдань Комісії є, зокрема, з'ясування долі та місцезнаходження осіб, зниклих безвісти, комунікація з родичами осіб, зниклих безвісти та надання їм інформації про хід проведення розшуку та його результати. Відомості, необхідні для розшуку осіб, зниклих безвісті, накопичуються та зберігаються у Єдиному реєстрі даних про осіб, зниклих безвісті, функціонування якого забезпечує Комісія. Відповідно до Закону, внесення відомостей до Реєстру щодо розшуку осіб, зниклих безвісти у зв'язку зі збройним конфліктом або воєнними діями, здійснюється виключно Комісією.

Закон визначає, що Україна здійснює міжнародне співробітництво у сфері розшуку, осіб, зниклих безвісти з іноземними державами, Міжнародним комітетом Червоного Хреста в якості нейтрального посередника, міжнародними організаціями, що здійснюють заходи щодо розшуку цих осіб відповідно до національного законодавства, та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України [1]. Відповідно до Закону, у випадку, якщо особа, що зникла безвісти, є громадянином іншої держави, уповноважений державний орган в Україні, який здійснює облік та розшук таких осіб, зобов'язаний повідомити уповноважені органи держави, громадянином якої ця особа є, про включення такої особи до Реєстру та про результати її розшуку. Принагідно слід зазначити, що із запитом про надання інформації щодо зниклого безвісті іноземця можуть звернутися не тільки його родичі, а і відповідні органи іноземної держави. Згідно положень Закону,

інформація може бути надана лише у випадку, якщо ці органи та відповідний компетентний орган України можуть установити такий режим доступу до інформації, який унеможливлює розкриття інформації. На даному етапі вважаємо за потрібне зауважити, що статті 17 та 18 Модельного закону, який містить базові норми, призначені для використання будь – якою державою під час розробки відповідного законодавства, дуже детально регламентує порядок накопичення інформації про зниклих безвісті осіб, доступ до неї та її захист. Зокрема, зазначається, що мають бути прийняті заходи щодо захисту інформації та недоторканності приватного життя зниклих безвісті осіб та їх родичів та щодо попередження використання даних з метою, відміною від тієї, для якої вони були зібрані [8]. Прикро, що відповідні положення не увійшли до Закону.

Надання особі статусу зниклої безвісті не позбавляє її родичів права на звернення до суду із заявою про визнання такої особи безвісно відсутньою чи оголошення її померлою у порядку, передбаченому чинним законодавством. Відповідно до ст.20 Закону України "Про міжнародне приватне право"[11] підстави та правові наслідки визнання іноземця, який мав постійне місце проживання в Україні, безвісно відсутнім чи оголошення його померлим визначається національним законодавством, тобто Цивільним кодексом України.

Список використаних джерел:

1. Про правовий статус осіб, зниклих безвісті: проект закону від 22.11.2016 р. № 5435//Офіційний портал Верховної Ради України/ ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=60560 (дата звернення: 15.05.2018)
2. Доповідь щодо ситуації з правами людини в Україні 16 серпня - 15 листопада 2016 р. // Управляння Верховного комісара ООН з прав людини/ URL: http://www.un.org.ua/images/UKR_16th_HRMMU_Report.pdf (дата звернення 15.05.2018)
3. Доповідь щодо ситуації з правами людини в Україні 16 листопада 2017року - 15 лютого 2018 року// Управляння Верховного комісара ООН з прав людини /URL: http://www.ohchr.org/Documents/Countries/UA/ ReportUkraineNov2017-Feb2018_UKR.pdf (дата звернення 15.05.2018)
4. Зниклі особи під час конфлікту в Україні //Резолюція 2067 Парламентської асамблеї Ради Європи від 25.06.2015 р. / URL: http://w1.c1.rada.gov.ua/pls/mpz/docs/2128_rez_2067_(2015).htm (дата звернення 15.05.2018)
5. Новостной интернет – ресурс / Корреспондент.net. URL: https:// t.me/korrespondentnet (дата обращения – 24.04.2018)
6. Конституція України: Закон від 28.06.1996 № 254к/96-ВР/ Верховна Рада України. Київ: Відомості Верховної Ради України (ВВРУ), 1996, № 30, с. 141)

7. Про правовий статус іноземців та осіб без громадянства: Закон України від 22.09.2011р. №3773-VI/Верховна Рада України. Київ: Відомості Верховної Ради України (ВВРУ),2012.№19-20, ст.179.

8. Руководящие принципы/Модельный закон о пропавших без вести лицах//Международный Комитет Красного Креста. URL: https://www.icrc.org/rus/resources/documents/misc/ihl-missing-5.htm (дата обращения 15.05.2018)

9. Конвенция о защите гражданского населения во время войны. Женева, 12 августа 1949 года//Международный Комитет Красного Креста. URL: https://www.icrc.org/rus/resources/documents/misc/geneva-convention-4.htm (дата обращения 15.05.2018)

10. Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов//Международный Комитет Красного Креста. URL: https://www.icrc.org/rus/assets/files/2013/ap_i_rus.pdf (дата обращения 15.05.2018)

11. Про міжнародне приватне право: Закон України від 23.06.2005 р. №2709 – IV / Верховна Рада України. Київ: Відомості Верховної Ради України (ВВРУ), 2005. №32. С. 42

----------***----------

Богачев Р. М., *м. Київ.*

УСВІДОМЛЕНЕ ПРАВО ТА ПРАВОВА СВІДОМІСТЬ

Розглянемо основні «больові центри», причини розгортання кризи кризового способу життя сучасного світу можливо узагальнити виходячі з теоретичних постулатів О.Зіновєващодо історії, яка «випливає в соціальні дірки»: по-перше, зниження загальної ефективності світ-системи зумовлює поглиблення суспільної **несправедливості** розподілу ресурсів та результатів суспільного відтворення, їх споживання, а, відповідно, призводить до подальшого, ще більшого зниження ефективності; по-друге, культ споживацтва та високий рівень соціальних витрат зумовлює відмову від гармонійності як критерію регулювання системи суспільного відтворення, позитивним та правильним вважається все, що підтримує рівень споживання, **правда** як суспільне бачення та потенційний орієнтир для гармонізації системи стає об'єктом маніпулювання; по-третє, для зовнішнього тимчасового збалансування системи **правові норми** підлаштовуються або взагалі ігноруються.

Світ балансує на межі кординальних змін та перетворень. Ідеологічне оформлення нових Ідеалів суспільного розвитку має на меті гармонізацію векторів діяльнісних проявів та сфер ПРАВА – ПРАВДИ – СПРАВЕДЛИВОСТІ в процесі суспільної самоорганізації в форматі мережива «живого спілкування».

Саме ці сфери виступають аналогом та корелятом властивості мережевості (справедливість), процесу мережування (правда) та мережива як результату (право). Такі процеси розгортаються й на міжнародному рівні.

Нескінченні спроби основних суб'єктів міжнародного права засудити будь-яких своїх опонентів у міжнародних відносинах чітко вказують на одну важливу обставину: вся система «міжнародного судочинства», яка охоплює практично всі сфери життя суспільства, була нічим іншим, як інструментом глобальної експансії суб'єкт-об'єктних зв'язків, та широко застосовується для псевдо-правового примусу, тиску, гноблення не тільки ворогів, але й безправних партнерів і союзників. А що залишається робити, якщо в царині суб'єкт–об'єктних відносин діє не «сила права», а «право сили». Всі ролі вже наперед виписані та закріплені: як суб'єктів та об'єктів впливу, тиску, примусу, гноблення…

Саме впевненість, з якою політичні діячі при першій-ліпшій нагоді моментально починають розмахувати судової дубиною, краще за будь-які формальні докази свідчить, що весь механізм цілком є перетвореною формою дійсного права та судочинства. Тобто імітацією «правової свідомості» міжнародних судів, а тому завжди гарантує зацікавленим прошаркам міжнародної еліти потрібний результат: саме тому багато «незгодних» на загибельні перспективи країн постійно знаходяться, буквально, «під судом» міжнародних квазіправових інститутів.

Чи то позови проти Китаю від США та ЄС у ВТО й у Гаагський суд відносно Південно-Китайського моря, чи то позови проти президента Білорусі Лукашенка в Гаагському суді, чи то судові позови за «окупацію країн Балтії» тощо. Те саме стосується й спільників-невдах, згадаємо Саудівську Аравію з позовами американських громадян за події «9/11» або позови в США проти Deutsche Bank.

Головне розуміти, що згадане «правосуддя» залишається чинним лише в системі суб'єкт-об'єктних відносин. Без них будь-яка гра в правосуддя перетворюється у блюзнірство та клоунаду. Багато країн вже вийшли з того віку, коли їх можна було залякати «демократичним правосуддям»: їх можна посадити на лаву підсудних, тільки єдиним способом – завдавши їм повної економічної та/або військової поразки. Однак за наявності партнерських стосунків між багатьма країнами та угод щодо захисту власної суб'єктності одна-одної результат буде однозначний – нездатність та неспроможність реалізувати давно відпрацьований сценарій.

Право, як і владу, не випрошують, а беруть-вибудовують! В політичному світі існують дуже жорсткі закономірності: сучасна капіталістична світ-система базується на протестантській етиці (а протестантизм є перетвореною формою католицтва) та має єдине ядро. Центр цього ядра – Лондон з Амстердамом, Гаагою й Вашингтон з Нью-Йорком, Брюсселем, а також Ватикан – з усіма їх переплетеними і взаємозалежними банківськими «мережами», що сходяться в Швейцарії, Люксембурзі та Ліхтенштейні. Вже навколо цього розташовані

Париж, Берлін, скандинавські й піренейські Столиці, Рим тощо. І вже далі на короткому повідку всі інші європейські столиці: Варшава, Прага, Бухарест, Загреб, Софія, Рига, Вільнюс, Таллінн тощо та інший пасивний тягар внизу харчової піраміди. Так звана периферія.

У периферії немає іншого способу стати ядром, крім як вийти з капіталістичної світ-системи та заснувати за її межами власний центр, а краще центри. Але такий крок вимагає не лозунгів про «європейський вибір», скандування «загальнолюдських цінностей» на шляху «взаємозалежності» та «інтеграції з цивілізованим світом», а – нових сутностей, змістів, ідей і вчинків зовсім іншого роду. Заперечення «влади випадку» завдяки Вчинкам-подіям з отримання та втримання власної СУБ'ЄКТНОСТІ та цілісних, всебічних, істинних МІЖСУБ'ЄКТНИХ СТОСУНКІВ загалом.

Яке ж має бути ПРАВО в царині мережевості?

ПРАВО як свідоме ПРАВО та правова СВІДОМІСТЬ (за Б.В.Новіковим)! Відома єдина належна ритміка: Людяний досвід – Об'єктивні теорії – Адекватні практики – ритміка процесу пізнання, що втілюється у поставанні людина економічна – людина суспільна – людина повністю усуспільнена (людина-творець) та сходженні в царині суспільного відтворення: Формотворення – Кеультуротворення – Свободотворення, – а також в царині Світо-перетворення: БІОСФЕРА – НООСФЕРА – КРЕАТОСФЕРА.

І в цій ритміці єдиною основою ПРАВА людини, правом як обов'язком-необхідністю та правом як повноваженням-бажанням виступає право-відповідальність ТВОРИТИ. Тобто з необхідністю вільно накопичувати та актуалізувати властивість мережевості для Свободотворення. Творити в мереживі суб'єктісно-суб'єктних взаємозв'язків та стосунків, діалектиці міжсуб'єктісного спілкування, в просторі «живого спілкування» в процесі самоорганізації.

Тільки так замість Біологізму «я хочу» або «я повинен» постає свідоме «Я МОЖУ», спрямоване на САМОзміну людини через накопичення і реалізацію потенціалу мережевості в переході від суб'єкт-об'єктних до суб'єкт – суб'єктних, а потому й суб'єктісно-суб'єктних взаємозв'язків та відносин.

Тільки так ПРАВО стає «живим» та свідомим, а свідомість – правовою, тільки так процес пізнання і перетворення-творення світу отримує дійсний критерій ОБ'ЄКТИВНОСТІ – тобто має в сутності ПРАВДУ та СПРАВЕДЛИВІСТЬ.

----------***----------

Свідло Т. М., *к.ф.н., доцент кафедри філософії ФСП КПІ ім. Ігоря Сікорського.*

ГРЕЦЬКЕ ПРАВО ЯК ОДИН З ГОЛОВНИХ ЧИННИКІВ ПРАВОВОГО ЗАКРІПЛЕННЯ ДЕМОКРАТІЇ

В українській культурі в силу тих чи тих обставин ще дуже багато «білих плям». Ще не одному поколінню українців слід буде віддавати належне заново відкритому імені, а завдяки сучасним інформаційним технологіям дійти це зможе до кожного в значно коротший термін, ніж завдяки книгодрукуванню. До таких імен належить і постать талановитого письменника, доктора права, адвоката Андрія Чайковського (1857-1935). На особливу увагу заслуговують наукові розвідки мислителя, перш за все в галузі юриспруденції: «Процес Ісуса Христа» (1893) та «Про старинний грецький процес кримінальний» (1897).

Другий із названих творів А. Чайковський починає констатацією факту, що грецьке право не стало предметом академічного навчання, його витіснило римське право, проте це не означає, що грецьке законодавство було менш значимим. Загальновизнано, що грецька культура подарувала світу багато ідей, і греки стояли вище римлян своєю культурою та освітою, отже, і законодавство греків мусило бути більш широким і нормувати всі сфери суспільних відносин. Греки мали розгалужені контакти з усім цивілізованим світом, підтримували з багатьма народами торговельні і правові, державні стосунки, тому старогрецьке законодавство заслуговує на увагу, проте навіть фаховим юристам воно мало відоме. Воно ж заслуговує на увагу, бо в ньому можна знайти деякі риси сучасного законодавства. І розібратися в цьому дослідник пропонує на прикладі кримінального процесу, звужуючи предмет дослідження до права атенського (афінського). Законодавство будь-якого народу несе в собі характерну ознаку свого народу, і афінське законодавство несе в собі специфічну ознаку – свобода громадянина, і основна задача держави – охорона свободи громадянина цієї держави. Тому афінський кримінальний процес був ліберальним від початку і до кінця: «буде тут, отже, осібно представлено про предметову і підметову приналежність суду, про особи судові, про особи процесові, про провід процесовий від жалоби аж до вироку, в кінці про виконання вироку...»[1]. Від Солона, зі зростом демократії, почалася певна спеціалізація судочинства: справи «супружні» і спадкові, про зневагу до богів і взагалі всі процеси про злочини, за які загрожувала смертна кара; окрему юрисдикцію мали справи про добро держави; про злочини військові; скоєні вбивства і замахи на вбивство. Окремо «в чотирьох судах» розбиралися справи про навмисне і ненавмисне вбивство; вбивство з метою оборони; підозрюваних у вбивстві та «вигнаних з краю»; «проти незвісних убійників».

Цікавою є процедура подання жалоби: необхідною умовою її прийняття було повідомлення «обжалованому» за 5 днів, без чого жалоба не приймалася до розгляду. Упорядкованою була і форма жалоби: «1) напис з поданням власти, до котрої вносилось жалобу, 2) імена сторін, 3) предмет»[1]. За себе можна було внести заставу або залишити закладників замість себе у в'язниці, крім особливо тяжких злочинів. Будь-яка людина могла ухилитися від процесу і кари, якщо добровільно йшла у вигнання. Щоб не виникало бажання навмисне когось занапастити,той, хто вносить жалобу, вносив певну суму, «приписану таксу». Далі починалося слідство, яке збирало докази, що поділялися на штучні і нештучні, фактичні. Свідками могли бути лише вільні і повнолітні, свідчили лише в слідстві, і якщо були «безпосереднього спостереження» (свідчення, які «чув від других», приймалися лише тоді, коли особа, від якої чув, вже померла). При недостачі доказів приймалася «присяга», яку могла запропонувати не лише «спорова сторона», а й будь-хто зацікавлений. Засідання трибуналу присяжних відбувалося щодня, крім святкових і «ферійних» днів (а таких налічувалось 100 днів у році), про що вивішували повідомлення на будинку суду. Число суддів залежало від предмету розгляду і коливалось від 200 до 500 осіб.

Цікавим фактом було те, що офіційно дозволялося ужалоблювати суддів: «прикликувались до розправ жінок, дітей, калік, родичів, котрі плачем і просьбами вимолювали увільнення» або «обжарюваний мимо того, що зблудив, цілком не є небезпечний для загалу, що противно – є дуже хосенним його членом»[1].

Отже, багато чому можна навчитися у давніх греків, які стояли не тільки у витоків демократії, а й закладали фундаментальні підвалини її у формі законодавства.

Список використаних джерел:

1. Чайковський А. Про старинний грецький процес криміналний / А. Чайковський. Спогади. Листи. Дослідження: У 3 т. / Упорядкування Б. З. Якимовича за участю З. Т. Грень, О. В. Седляра; Редкол.: Б. З. Якимович (голова) та ін. – Львів, 2002. – Т. 1 – 514 с./ Режим доступу: http://shron1.chtyvo.org.ua/Chaikovskyi/Spohady_Lysty_Doslidzhennia_Tom_1.pdf

----------***----------

Лисак Б.В., студент Радіотехнічного факультету КПІ ім. Ігоря Сікорського.
Науковий керівник: **Фурашев В.М.,**
к.т.н., с.н.с., доцент ФСП КПІ ім. Ігоря Сікорського.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ПРОЯВ ПРАВ І СВОБОДИ ЛЮДИНИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ: ПОЗИТИВНЕ І НЕГАТИВНЕ

Наслідки будь-якого науково-технічного прогресу, як правило, мають не лише позитивне значення для людства, й досить часто і дошкуляють йому. Сучасний науково-технічний прогрес в інформаційної сфері не виключенням з цього правила. Скажемо, що завдяки цьому науково-технічному прогресу, людство отримало такий засіб об`єднання людей за широким спектром спільних інтересів, як соціальні мережі. Крім того, соціальні мережі можна розглядати і як практичний засіб розширення прав і свободи людини в інформаційної сфері. Але з появою соціальних мереж виникли досить серйозні проблеми з вирішення питань забезпечення безпеки людини. Для прикладу наведемо вирішення питання забезпечення конфідціалності персональних даних користувача. Вже ні для кого не секрет, що у США відбувається неймовірно важливе розслідування - протягом декількох років компанія Cambridge Analityca за допомогою одного з додатків зібрала інформацію про більш ніж 87 млн користувачів Facebook [1]. Витоку зазнали публікації, відмітки «Мені подобається» не тільки користувачів додатка, а й їхніх друзів. Напрямів використання даної інформації безліч. Деякі з них: маніпулювання свідомістю виборців під час організації та проведення виборів віх рівнів; формування громадської думки «в потрібному напрямку» по будь-яких питань. Так, за деякими даними, завдяки саме таким маніпуляціям Дональд Трамп став президентом США [2]. Відомо, що питання збереження конфіденційності персональних даних і запобігання їх використання з метою маніпуляції на даний момент найактуальніше питання інформаційної безпеки.

Завдяки соціальним мережам, таким як Facebook, Twitter, Instagram і ін., конфедіційнп інформація про вас, про вашу сім'ю і про ваших знайомих знаходиться буквально на поверхні. Якщо ви ведете активне соціальне життя, дізнатися про що ви думаєте, де живете, хто вам подобається менше, а хто - більше можна навіть не вдаючись до дешифрування ваших особистих даних. Багато речей в Мережі з'являються тільки через те, що ви (або хтось інший) вважаєте за потрібне поділитися з усім світом своєю точкою зору або фотографією. Аналіз вашого профілю (або невеликої групи профілів) в соціальній мережі, на подив, досить неважке заняття, яке дозволяє зловмисникам діяти проти вас, впливати на вас.

Крім дрібних зловмисників, інформацію, яка лежить у вільному доступі можуть використовувати для більш серйозних цілей. Так, компанія Cambridge Analityca зібрала неймовірно великий масив даних користувачів Facebook і за допомогою певного роду інструментів змогла створити психологічні портрети американських виборців для правильного просування кандидатури Дональда Трампа під час президентських виборів [2]. Ця інформація піддалася розголосу, але напевно є не одна компанія, напрямок діяльності якої схоже напрямку Cambridge Analityca. Вашу публічну інформацію можуть використовувати і велика ймовірність, що вже використовують для складання психологічних портретів населення або будь-якої цільової аудиторії для правильного просування бажаних цілей.

Для запобігання подібного роду маніпуляцій слід ставитися до викладаємої інформації дбайливо, як і до будь-якої, яка виходить від вас в житті. Перш за все, ставте перед собою питання: «А чи варто ця інформація того, щоб бути викладеною в Інтернеті або ж її відсутність не є критичною?». Далі слід ознайомитися з політикою конфіденційності (privacy policy) сервісу, яким ви користуєтеся. У кожного сервісу, який так чи інакше володіє інформацією, повинен бути документ, який регламентує яку інформацію сервіс може обробляти, наприклад, для контекстної реклами, а яка залишається необробленої, вашої суто особистою. Якщо ви згодні з політикою конфіденційності, то далі необхідно переглянути налаштування вашого профілю в обраному сервісі, можливо, налаштувати параметри публічної доступності до публікуємих вами даних так, як ви бажаєте - залишити їх повністю публічними або ж обмежити до них доступ. Ніколи не можна ділитися паролями ваших облікових записів, оскільки це завдає шкоди вашій конфіденційності. Провівши ці дії, ви точно будете знати наскільки публічна ваша інформація і який рівень захисту пропонується певним сервісом.

Однак, інформацію збирають не тільки зловмисники, але й спецслужби різних держав. Тут мова йде не тільки про ту інформацію, яка знаходиться в соціальних мережах і умовно «не захищена», а й про інформацію про ваші переміщення, відвідуванні заходів і різного роду місць, навіть про ваших великих покупках. На сьогоднішній день відомо, що інформацію про своїх громадян збирає США, РФ, КНР.

Після подій 9 вересня 2001 р АНБ США була створена спеціальна програма з метою боротьби з тероризмом, основне завдання якої - стежити за певними громадянами тривалий час, записуючи дії останніх аж до хвилини. Влітку 2013 року ця інформація стала відомою завдяки Едварду Сноуденом і ресурсу «The Guardian» [3]. Однак, була доведена неефективність цієї програми, за весь час роботи вона зіграла ключову роль лише в одному випадку [4]. У лютому 2016 р, теж прикриваючись цілями боротьби з тероризмом, ФБР

зажадало Apple реалізувати обхід блокування пристроїв компанії [5]. Глава корпорації, Тім Кук, написав відкритого листа, в якому сповна висвітлив ситуацію, що склалася і дав відмову реалізації обходу, оскільки це сильно шкодило б безпеки всіх пристроїв. Варто зауважити, що через деякий час ФБР розблокували пристрій без допомоги Apple [6].

У РФ майже рік як прийнято «антитерористичний пакет» законопроектів, запропонований Іриною Яровий. Згідно з останнім, вся інформація, яка була опублікована вами в Інтернеті, зберігається рік, телефонні дзвінки та СМС - до трьох років, а кожен сервіс, який підтримує шифрування даних зобов'язаний допомогти ФСБ розшифрувати ці дані [7], інакше буде заблокований. Сервіс по обміну повідомлень «Telegram» відмовився забезпечувати подібну допомогу ФСБ. Пояснюється це двома причинами. По-перше, маючи універсальний алгоритм дешифрування (так званий «ключ») повідомлень ставиться під сумнів захист будь-якої листування від третіх осіб, адже будь-хто може заволодіти цими «ключами». По-друге, «Telegram» використовує такий тип шифрування, при якому «ключі» випадковим чином генеруються на пристроях самих користувачів, а не на серверах сервісу, так інформація залишається найбільш захищеною.

У Китаї теж немає як такого відкритого Інтернету та все знаходяться під наглядом. КНР по праву заслужила звання не демократично країни, але не можна стверджувати, що це найбільш незахищена країна. В середині квітня цього року китайські поліцейські затримали чоловіка-зловмисника серед численного натовпу на концерті [8]. З 2015 року в Китаї почали збирати базу національну даних використовуючи функцію розпізнавання осіб, яка називається «Гостре око». До 2020 року китайський уряд планує ввести «рейтинг громадської надійності». Згідно з ним, громадянам з більш високим рейтингом будуть надаватися соціальні допомоги, відкриватися туристичні візи або кредити з вигідними процентними ставками [9]. Це досить цікава ініціатива, яка працює за принципом карми: будь законослухняним громадянином - держава буде йти до тебе назустріч.

Звичайно, наведені вище приклади показують, як глобальна стеження обмежує свободу простого громадянина країни. Але, даючи доступ до своїх персональних даних, ви можете поліпшити безпеку власної держави від правопорушень різного масштабу і зробити так, щоб держава допомагала вам, в кінцевому підсумку.

Висновки. У XXI столітті приділяти увагу модеруванню вашої інформації, яка знаходиться в Інтернеті необхідно, особливо інформації персонального характеру. Соціальні мережі слід розглядати не тільки з позицій комунікаційного середовища, але і як складову сучасної зброї - інформаційного.

Незважаючи на те, що держави збирають інформацію про своїх громадян, ці дії відбуваються з метою поліпшення національної безпеки держави і положення кожного громадянина в останньому. На жаль, питання національної безпеки конфронтируют з питанням демократизації та свободи суспільства.

Список використаних джерел:

1. URL: https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM (дата звернення: 03.05.2018).
2. URL: https://meduza.io/feature/2018/03/23/kak-cambridge-analytica-vyigrala-vybory-dlya-trampa-the-guardian (дата звернення: 03.05.2018).
3. URL: https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline (дата звернення: 03.05.2018).
4. URL: https://zn.ua/WORLD/sbor-telefonnyh-metadannyh-anb-neznachitelno-pomog-v-borbe-s-terrorizmom-136569_.html (дата звернення: 03.05.2018).
5. URL: https://tjournal.ru/23244-apple-otkazalas-ispolnyat-trebovanie-fbr-predostavit-dostup-k-ayfonu-terrorista-iz-san-bernardino (дата звернення: 01.05.2018).
6. URL: https://itc.ua/news/fbr-samostoyatelno-razblokirovalo-iphone-strelka-iz-san-bernardino-i-otozvalo-sudebnyie-pretenzii-k-apple/ (дата звернення: 27.04.2018).
7. URL: https://meduza.io/feature/2016/06/24/paket-yarovoy-prinyat-i-eto-ochen-ploho (дата звернення: 02.05.2018).
8. Facial recognition at a concert leads to arrest of cyber fugitive. URL: http://www.ecns.cn/2018/04-11/298786.shtml (дата звернення: 02.05.2018).
9. URL: https://meduza.io/feature/2018/04/15/ostryy-glaz-vmesto-bolshogo-brata-kak-kitayskie-vlasti-massovo-sledyat-za-zhitelyami-strany?utm_source=telegram&utm_medium=live&utm_campaign=live (дата звернення: 03.05.2018).

----------***----------

Конах Ю. О., *студентка ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник: ***Баранов О. А.,*** *д.ю.н., професор кафедри інформаційного права та права інтелектуальної власності ФСП КПІ ім. Ігоря Сікорського.*

ПИТАННЯ ЗАКОНОДАВЧОГО ВРЕГУЛЮВАННЯ ВІДНОСИН У СФЕРІ ВИКОРИСТАННЯ КРИПТОВАЛЮТ В УКРАЇНІ

Питання легалізації та надання чіткого правового статусу криптовалюті вже давно зависає у повітрі у всьому світі, хоча в найбільш розвинених країнах здійснюються обережні кроки до вирішення питання врегулювання обігу

цифрових валют на їх території. Наприклад, законодавства Японії та КНР прирівнюють криптовалюту до віртуального товару; в Канаді біткоін та інші криптовалюти вважаються нематеріальними активами; в Ізраїлі взагалі мова не йде ні про фінансове забезпечення, ні про оподатковуваний актив.

Україна – не виключення, і в нашій державі також здійснюються активні кроки для вирішення цього питання. Створюються законопроекти, які мають на меті якнайширше врегулювати відносини у сфері криптовалют. Проте не усі спеціалісти вважають, що українське законодавство має зазнавати змін. Зокрема, заступник голови Нацбанку України Олег Чурий зазначив, що процес внесення змін до українського законодавства не має бути поспішним, оскільки до сих пір у світі ще не існує уніфікованої позиції стосовно криптовалют [5].

Але все одно спроби законодавчого врегулювання цього питання здійснюються, про що свідчить подання законопроекту «Про обіг криптовалюти в Україні», зареєстрованого під номером 7183. Метою цього документу визначено «регулювання правовідносини щодо обігу, зберігання, володіння, використання та проведення операцій за допомогою криптовалюти в Україні» [1]. У пояснювальній записці вказується, що даний законопроект «дозволить залучити міжнародні інвестиції в Україну для розвитку малого, середнього та великого бізнесу, що у свою чергу позитивно вплине на економічний клімат всередині держави, дозволить зміцнити національну валюту та збільшити ВВП» [2]. Тож які основні положення передбачаються цим законопроектом, та чого слід очікувати усім володарям біткоїнів та інших криптовалют, якщо він буде прийнятий?

Аналізуючи зміст зазначеного законопроекту, не можна не відмітити, що в ньому досить широко наведені терміни, які стосуються обігу криптовалют, а саме «криптовалюта», «криптовалютна біржа», «криптовалютний кошик», «криптовалютні транзакції», «система блокчейн», «майнер», «майнінг» і т.д. Зокрема, криптовалютою пропонується визнавати «програмний код (набір символів, цифр та букв), що є об’єктом права власності, який може виступати засобом міни, відомості про який вносяться та зберігаються у системі блокчейн в якості облікових одиниць поточної системи блокчейн у вигляді даних (програмного коду)» [1].

Після визначення дефініцій даних термінів у проекті йдеться про державне регулювання і державні гарантії у сфері використання цифрових валют. І тут починається найцікавіше. У нормативному акті зазначено, що державне управління даною сферою бере на себе Національний банк України. Стосовно ж держгарантій, тут вказується на повну непричетність держави до знецінювання криптовалюти або її втрати – ніяких зобов’язань у цих випадках вона не несе та відшкодування не здійснює. Також держава не виступає гарантом забезпечення безпечного функціонування онлайн-сервісів з обміну цифрових валют. Тобто захист та збереження власної цифрової валюти буде

лежати на плечах самого суб'єкта криптовалютних операцій, і він сам буде гарантувати їх проведення.

В той же час цей законопроект визначає криптовалюту як особисту власність майнера, з якої потрібно сплачувати відповідні податки. Таким чином, до криптовалют будуть застосовуватися загальні положення стосовно права приватної власності, які діють на території України. Кожен власник криптовалюти матиме змогу вільно розпоряджатися нею, зокрема здійснювати операції з обміну валюти будь-якого виду на інші, міняти її на електронні гроші, валютні цінності, цінні папери, послуги, товари та інше. Обмін можна буде здійснювати на криптовалютних біржах, порядок роботи яких поки що залишається невідомим. І, що важливо, все це буде здійснюватися на власний ризик.

Якщо говорити про дані, які стануть відкритими та загальновідомими у зв'язку з використанням криптовалют, то в якості таких будуть виступати дані стосовно криптовалютних операцій. Ця інформація зберігається у системі блокчейн і підпадатиме під моніторинг криптовалютної біржі. Відкритими будуть дані саме про криптовалютний кошик, де зберігається валюта власника і з якого відбувається передача. Також не можна буде приховати інформацію про одержувача, об'єм переказу та тимчасові мітки, що визначають момент передачі.

Займатися ідентифікацією та персоніфікацією суб'єктів криптовалютних операцій будуть криптовалютні біржі, порядок створення і функціонування яких визначить НБУ. Дохід таких бірж також буде обкладатися податками.

Власники криптовалюти згідно з проектом матимуть обов'язок щодо зберігання даних про здійснювані ними операції протягом 5 років. Також у законопроекті вказується, у яких випадках буде заборонено використання цифрових валют. До них відносяться випадки використання криптовалюти, якщо воно спрямоване проти основ національної безпеки України, для закликів до повалення конституційного ладу, порушення територіальної цілісності України, вчинення терористичних актів, фінансування тероризму, легалізації (відмивання) доходів одержаних злочином шляхом, обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших протиправних діянь. Якщо ж ці норми будуть порушені, покарання не змусить себе чекати – може настати цивільно-правова, адміністративна або кримінальна відповідальність згідно з законодавством України.

Наразі законопроект знаходиться на стадії доопрацювання, і, на думку Головного науково-експертного управління Апарату Верховної Ради України, в ньому слід врахувати ряд зауважень та пропозицій. Вони стосуються як термінологічного апарату, так і основних положень даного документу. Було висунуто припущення, що законодавче запровадження такого фінансового

інструменту може призвести не лише до позитивних, а й до негативних наслідків. Було згадано, що згідно з роз'ясненням НБУ щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» Bitcoin, криптовалюта була порівняна з грошовим сурогатом, не маючим вартісного забезпечення та неспроможним для використання як засіб платежу через суперечність нормам чинного українського законодавства [3].

В той же час до подання у Верховну Раду готується і інший законопроект, який отримав назву «Про застосування технології розподіленого реєстру цифрових транзакцій та правовий статус токенів і криптовалют в Україні». Зазначається, що метою цього документу є створення правил роботи з криптовалютою, токенами і смарт-контрактами для держави, юридичних і фізичних осіб, створення вільного та прозорого ринку токенів та криптовалют в Україні, вільного майнінгу, використання, зберігання і обміну цифрових цінностей із застосуванням технології розподіленого реєстру цифрових транзакцій. Окрім цього, до цілей проекту відноситься розвиток і стимулювання використання технології розподіленого реєстру цифрових транзакцій і смарт-контрактів в усіх сферах суспільних відносин, зокрема в секторі публічних відносин, медичній, освітній та інших соціально спрямованих сферах задля розвитку інформаційного суспільства, а також для недопущення ризиків використання токенів і криптовалют для відмивання коштів і фінансування тероризму, що являється перешкодою для обслуговування банківських рахунків компаній, які працюють з токенами і криптовалютою та є причиною необґрунтованих кримінальних переслідувань з боку правоохоронних органів [6].

В будь-якому разі, складно сперечатися з тим, що популярність криптовалюти зросла і продовжує зростати шаленими темпами, з чим і пов'язана необхідність правового регулювання цієї сфери у кожній країні, де криптовалюта знаходиться в обігу. Проте міжнародною спільнотою ще не визначено єдиних підходів до регулювання обігу цифрових валют. Існує думка, що саме віртуальні валюти можуть призвести до значного послаблення позицій усієї банківської системи та зумовити перехід на криптовалютні операції через незалежність від світових банків та їх валют. Однак все буде залежати від нормативних актів, спрямованих на врегулювання такої діяльності, і чи буде доопрацьований законопроект «Про обіг криптовалюти в Україні» та яка доля чекає на нього та інші законопроекти, спрямовані на врегулювання криптоіндустрії в Україні – покаже лише час.

Список використаних джерел:

1. Проект Закону України «Про обіг криптовалюти в Україні» (реєстр. № 7183 від 06.10.2017 р.)

2. Пояснювальна записка до Проекту Закону України «Про обіг криптовалюти в Україні» від 06.10.2017 р.

3. Висновок Головного науково-експертного управління Апарату Верховної Ради на проект Закону України «Про обіг криптовалюти в Україні» від 05.02.2018 р.

4. Роз'яснення НБУ щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» Bitcoin від 10.11.2014 р.

5. Глава НКЦБФР инициирует рассмотрение Советом финстабильности признания криптоединиц финансовым инструментом.URL: https://interfax. com.ua/news/economic/503953-amp.html.- (дата звернення: 16.05.2018).

6. В Україні пропонують врегулювати правовий статус токенів і криптовалют. URL: http://finpost.com.ua/news/8402.- (дата звернення: 16.05.2018).

----------***----------

Законнова Ю.Е., *студентка ФСП КПІ ім. Ігоря Сікорського*.
Науковий керівник: ***Фурашев В.М.,*** *к.т.н., с.н.с., доцент ФСП КПІ ім. Ігоря Сікорського.*

ЕЛЕКТРОННЕ УРЯДУВАННЯ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ЛЮДИНИ

Розвиток інформаційних технологій зумовив становлення нового роду суспільних відносин, пов'язаних із здійсненням державної влади. На сьогоді впровадження інформаційних технологій надає можливість швидко та ефективно вирішити існуючі проблеми, забезпечити комунікацію між владою та суспільством, обійти бюрократичні процедури та прискорити реалізацію прав та законних інтересів осіб.

Так, однією з концепцій сучасності є концепція електронного урядування. Електронний уряд – це сукупність інформаційних ресурсів та мереж, за допомогою яких здійснюється частина державних функцій. За допомогою е-уряду є можливість надати громадянам адміністративні та соціальні послуги, зокрема, забезпечити видання довідок, реєстрацію підприємства, шлюбу, народження дитини. Фактично електронне урядування є засобом комунікації між владою, суспільством та бізнесом [3].

Е-уряд містить такі складові як е-демократія (проведення електронних виборів, інститут електронних петицій, участь громадськості в обговоренні НПА), е-адміністрування (можливість отримання довідок, вчинення реєстраційних дій завдяки електронним мережам), е-бізнес (здійснення бізнесу та спрощення процедур шляхом переведення їх в електронний формат), е-суд (здійснення судового процесу на дистанційному рівня, через Інтернет) тощо [2].

Найбільш ефективна модель е-уряду притаманна Естонії, де громадянин може укласти правочин чи шлюб, отримати необхідну довідку, зареєструвати бізнес, не залишаючи домівки [1].

Однак в Україні поки що стан побудови е-уряду залишається на низькому рівні. Причина того – в незахищеності інформаційних систем та низькій інформаційній культурі суспільства.

По-перше, інформаційна інфраструктура України є недостатньо розвиненою. Так, на сьогодні до мережі Інтернет має доступ більше половини населення, однак вагома частка – близько 30-40% відрізані від цієї мережі. Це зумовлено різними чинниками: нерозвиненою інфраструктурою (зокрема, у сільській місцевості), економічною складовою, віком та стереотипними уявленнями окремих громадян. За таких умов частина громадян відрізана від інформаційних послуг від держави [4].

По-друге, недостатньо реалізованими є інформаційні ресурси держави. На жаль, сучасні інформаційні ресурси часто піддаються хакерським атакам (наприклад, нещодавне блокування сайту Міністерства енергетики або тогорічний вірус Petya). Така нестабільність інформаційних мереж зумовлює недовіру громадян до інформаційних послуг держави.

По-третє, не завжди відбувається комунікація з державними установами. Досить часто з боку органів місцевого самоврядування, територіальних підрозділів спостерігається байдуже ставлення до підвищення якості інформаційних послуг.

Зрештою, інформаційна безграмотність населення постає однією з найбільших проблем, яка гальмує становлення е-уряду в Україні [4].

На наше переконання, електронне урядування необхідно в Україні, оскільки воно сприятиме реалізації прав громадян. Для впровадження дієвого електронного урядування в Україні слід здійснити ряд кроків:

По-перше, забезпечити всіх громадян на безоплатній основі ID-картками та надати електронний кабінет в єдиній державній інформаційній системі. Має бути створена національна інформаційна мережа, в якій кожен зможе прийняти участь у громадських обговореннях, голосуваннях (у т.ч. виборах та референдумі), подати заявку для реєстрації до відвідування посадових осіб.

По-друге, мають бути створені умови для реєстрації без явки до органів державної влади шляхом підтвердження документальних даних в мережі Пенсійного фонду, Фонду соціального страхування. Громадяни повинні мати можливість отримати адміністративні, пенсійні та соціальні послуги дистанційно, шляхом замовлення через Інтернет. Окрім того, черга до дитячих садків, шкіл, поліклінік має мати електронний характер, що спростить життя громадянам.

По-третє, мають бути створені мобільні додатки, в яких особа зможе здійснити всі функції.

Електронне урядування має забезпечити кожну людину доступом до мережі Інтернет та державних послуг, що забезпечить право особи на інформацію та принцип доступності. Держава має створити відповідну інфраструктуру, завдяки якій громадяни зможуть отримати доступ до Інтернету та державних послуг в будь-який час.

Окрім того необхідним вбачається покращення грамотності населення шляхом інформаційної кампанії та спецкурсів у закладах освіти, поширення універсальних карт безкоштовно. Кожен має отримати персональну карту безкоштовно, аби зрозуміти всі позитивні властивості цього інструменту у повсякденній діяльності. Але головним критерієм має бути саме розвиток громадянської відповідальності та правової грамотності населення.

Список використаних джерел:

1. Бершидський Л. Естонський електронний уряд, як приклад для наслідування. URL: http://hvylya.net/analytics/tech/estonskiy-elektronniy-uryad-yak-priklad-dlya-nasliduvannya.html
2. Електронний уряд. URL: https://uk.wikipedia.org/wiki/Електронний_уряд
3. Електронний уряд: держава без чиновника. URL: https://www.radiosvoboda.org/a/25003573.html
4. Що таке електронний уряд? Трохи теорії та статистики. URL: https://24tv.ua/special/egovenrment/

----------***----------

Стребкова Ю. В., *к.ф.н., доцент КПІ ім. Ігоря Сікорського*.

ПІДГОТОВКА СОЦІАЛЬНИХ ПРАЦІВНИКІВ У КОНТЕКСТІ НАЦІОНАЛЬНОГО ПЛАНУ ДІЙ З ВИКОНАННЯ РЕЗОЛЮЦІЇ РАДИ БЕЗПЕКИ ООН 1325 “ЖІНКИ, МИР, БЕЗПЕКА”

Резолюція Ради безпеки ООН 1325 «Жінки, мир, безпека» була прийнята у 2000 році і має ряд суміжних – «сестринських» резолюцій, що були прийняті пізніше та заторкали тему ґендерної взаємодії у сфері безпеки: 1674 (2006), 1820 (2008), 1882 (2009), 1888 (2009), 1889 (2009), 1894 (2009), 1960 (2010), 1998 (2011), 2106 (2013), 2122 (2013), 2242 (2015), 2250 (2015) та ін. Резолюції 1265, 1999 року та 1296 (2000), що були прийняті раніше, також містять положення про особливий вплив збройних конфліктів на жінок, дітей та інші вразливі групи. Заяви Голови Ради S/PRST/2012/29 та S/PRST/2015/2 стосуються постконфліктного миротворчого процесу, а резолюція 2068 (2012) засуджує порушення норм міжнародного права, пов’язані із каліцтвами, зґвалтуваннями

та іншими формами сексуального насильства щодо дітей у збройних конфліктах.

Значна кількість міжнародних резолюцій Ради безпеки ООН і відповідних Заяв Голови Ради підтверджує, що дотримання ґендерної рівності та розширення прав і можливостей жінок має надзвичайно важливе значення для безпеки. Резолюціями передбачається ряд заходів міжнародного, регіонального, національного та місцевого масштабу з впровадження положень, викладених у цих резолюціях, оцінки та координування їх виконання, моніторингу дотримання передбачених норм ґендерної рівності та недискримінації. Національний план дій з виконання резолюції Ради Безпеки ООН 1325 "Жінки, мир, безпека" на період до 2020 року було затверджено 24 лютого 2016 р. розпорядженням Кабінету Міністрів України № 113-р, проте наразі розглядається внесення суттєвих змін до цього плану. Для чого 20 квітня 2018 р. у Мінсоцполітики засідала експертна міжвідомча група. У Міністерстві оборони, також, створено робочу групу, а план заходів МВС України щодо виконання національного плану включає систему моніторингу та оцінки, затверджену наказом Міністерства внутрішніх справ України від 12.12.2017 № 1019.

Українські жіночі громадські організації, зокрема Ла Страда та Урядова уповноважена з Питань ґендерної політики (Катерина Левченко) зосереджуються на боротьбі з насильством щодо жінок у тому числі під час збройних конфліктів. Забезпечення ґендерних пріоритетів (у т.ч. запобігання і протидія ґендерно обумовленому насильству, торгівлі людьми тощо) є невід'ємною складовою діяльності МВС [3, с. 4].

Резолюція 1888 (2009) спонукає місцевих жительок вступати до лав національних збройних сил та сил безпеки, проте, VIII періодична альтернативна доповідь з виконання Україною Конвенції про ліквідацію всіх форм дискримінації щодо жінок та заключні зауваження по CEDAW містять інформацію про наявність в Україні дискримінаційних положень у доступі жінок до освіти за військовими та «силовими» спеціальностями [2]. Нещодавно прийнятий закон про розширення тимчасового переліку штатних посад рядового, сержантського і старшинського складу, які можуть обіймати жінки, не вирішує цю проблему. Отже, більшість українських жінок у зоні конфлікту будуть мати цивільний фах.

Зміни щодо залучення жінок з метою удосконалення структури та управління територіальною обороною наразі не передбачені: відповідно до Указу Президента України від 23 вересня 2016 року № 406/2016 «Про затвердження Положення про територіальну оборону України», Законів України «Про оборону України», "Про правовий режим воєнного стану", постанови КМУ від 22.07.2015 року №544 – жінки не розглядаються як потенціал для

організації, підготовки та ведення територіальної оборони України. На нашу думку, ефективна взаємодія між органами місцевого самоврядування та військами (силами), які дислокуються на території України неможлива без урахування ґендерної складової.

Міжнародні організації накопичили багатий досвід цивільно-військової співпраці у зоні військових та збройних конфліктів, зокрема з урахуванням ґендерної політики. Ґендерна проблематика була включена у якості однієї з цілей до щорічних командно-штабних віртуальних навчань НАТО з управління кризовими ситуаціями «CMX-2015» (04-10.03.2015 р., штаб-квартира НАТО, м. Брюссель). Річна національна програма Україна-НАТО на 2018 містить розділ «Ґендерна рівність». Ґендерні перспективи в цілях партнерства НАТО – Україна включають створення умов, що дадуть змогу ґендерним консультантам приймати участь у взаємодії місцевого населенням та сил оборони під час національних, багатонаціональних та інших операцій, у тому числі на чолі з НАТО.

Військово-цивільна співпраця та антикризове управління на всіх рівнях потребують залучення як військового, так і висококваліфікованого цивільного персоналу, рівноправної та повноцінної участі жінок з відповідною фаховою підготовкою. Розроблені у КПІ ім. Ігоря Сікорського, на основі системного підходу, програми підготовки фахівців дозволяють залучати знання з різних галузей для цивільно-військової співпраці. Наприклад, у рамках підготовки фахівців-геоматиків нами було успішно впроваджено застосування технологій картографування для візуалізації ґендерно дизагрегованих даних та маркування небезпек ґендерного характеру.

Зазначимо, що загрозу безпеці, становить «криза системи охорони здоров'я і соціального захисту населення і, як наслідок, небезпечне погіршення стану здоров'я населення; поширення наркоманії, алкоголізму, соціальних хвороб» [4]. Засуджується ООН відсутність жінок серед головних чи провідних посередників у мирних перемовинах, що проводяться під егідою цієї організації. Жінки становили лише 2% медіаторів і посередників та 9% переговірників у військових конфліктах світу протягом 1992-2011 рр. [0].

На нашу думку, саме фахівці з соціальної роботи якнайбільше підходять для організації військово-цивільної співпраці. Враховуючи сучасне геополітичне становище України та можливі сценарії розвитку збройного конфлікту, можна стверджувати, що буде збільшуватись потреба у висококваліфікованих фахівцях із соціальної роботи, здатних організовувати та надавати послуги новим вразливим групам, що виникли внаслідок збройного конфлікту на Сході: військовим, ВПО, вдовам, ветеранкам, волонтеркам, жінкам, які працюють на фронті, дружинам і рідним ветеранів, загиблих, зниклих без вісти, та ін.

Отже, враховуючи потребу у фахівцях, які зможуть надавати соціальні послуги в умовах конфлікту, до плану підготовки бакалаврів за напрямком «Соціальна робота» мають входити такі дисципліни: «Ґендерні дослідження», «Медико-соціальні основи здоров'я», «Медіація та організація переговорного процесу», «Практика волонтерської діяльності», «Соціальна робота з мігрантами та внутрішньо переміщеними особами», «Соціальна робота з військовослужбовцями, демобілізованими та звільненими в запас».

Список використаних джерел:

1. Preventing Conflict. Transforming Justice. Securing the Peace. A Global Study on the Implementation of the UN Security Council Resolution 1325. – p.14.
2. Альтернативна доповідь по виконанню Україною Конвенції про ліквідацію всіх форм дискримінації щодо жінок: VIII періодична доповідь / За ред. М.М. Скорик. – Київ: БО БТ Київський інститут ґендерних досліджень», 2017- 60 с.
3. Методичні рекомендації до Плану заходів Міністерства внутрішніх справ України щодо виконання Національного плану дій з виконання резолюції Ради Безпеки ООН 1325 «Жінки, мир, безпека» на період до 2020 року. [Електронний ресурс] : – Режим доступу: http://nakaz-no1019-vid-12122017-pro-zahody-z-vykonannya-rozporyadzhennya-kabinetu-ministriv-ukrayiny-vid
4. Про основи національної безпеки України [Електронний ресурс] : Закон України від 19.06.2003 № 964-IV. – режим доступу. – http://zakon0.rada.gov.ua/laws/show/964-15.

----------***----------

Кравченко І. А*., ст. викладач кафедри фіолсофії КПІ ім. Ігоря Сикорського*

ІНФОРМАЦІЙНО-КОММУНІКАТИВНІ ТЕХНОЛОГІЇ В СОЦІАЛЬНОЇ РОБОТІ

За останні роки в Україні було багато прийнято рішень, концепцій та законодавчих актів для розвитку інформаційного суспільства як одного з пріоритетів України. Одним з інструментів цього розвитку, підвищення конкурентоспроможності та стимулювання соціально-економічного розвитку країни, а також «формування нового типу держави, орієнтованої на задоволення потреб громадян» у «Концепції розвитку електронного урядування» було позначено електронне урядування як першочерговий пріоритет реформування системи державного управління та «розбудови в Україні ефективних цифрової економіки і цифрового ринку та його подальшої інтеграції до єдиного цифрового ринку ЄС (EU Digital Single Market Strategy)».

Дослідження ООН (United Nations E-government Survey) щодо розвитку електронного урядування визначає індекс електронної участі (EPI), за яким відображаються використання інтерактивних послуг для сприяння наданню

інформації урядами громадянам (e-information), взаємодія та консультації з громадянами (e-consultation) та участь громадян в процесах прийняття державних рішень.

В сучасних умовах будь в якої галузі досягнення необхідного рівня ефективності та результативності неможливе без широкого використання сучасних інформаційні, комунікативні та комунікаційні технології.

В більшості країн значна частка населення зайнята в процесах підготовки, зберігання, обробки і передавання інформації. Інформаційні процеси є важливими елементами виробничих і соціальних процесів.

Інформаційні технології мають значущу роль в забезпеченні взаємодії між людьми. За допомогою передавання, розподілу та розповсюдженню інформації (комунікативні технології) створюється інформаційне середовище.

Інформаційно-комунікативні технології в соціальної сфері, в тому числі й в соціальної роботі, в розвинутих країнах достатньо активно використовуються в досі широкому діапазоні, починаючи з використання в самому навчальному процесі при підготовці спеціалістів в галузі соціальної роботи до надання послуг в різних напрямках соціальної роботи: дистанційне навчання; отримання доступу до соціальної інформації, консультаційних послуг; запити щодо довідок; можливість інтерактивного спілкування, обміну інформацією між соціальним працівником та клієнтом як в реальному часі (режим on-line) так й в режимі off-line; можливість проходження анкетування, наприклад з питань певних медичних, психологічних проблем; вирішення питань працевлаштування; моніторинг та охорона навколишнього середовища; моніторинг суспільної думки; збір, облік, обробка даних по клієнтах певних соціальних груп тощо. В України, також, поступово поширюється впровадження інформаційно-комунікативних технологій в соціальної сфері, що з одного боку, надає нові можливості підвищення ефективності роботи в соціальної сфері, а з іншого, породжує низку проблем пов’язаних як з безпекою самих створюваних інформаційних ресурсів, так и з безпекою людини в цьому інформаційному середовище, що в свою чергу потребує вдосконалення нормативно-правової бази, яка регулює сферу розвитку інформаційно-комунікативних технологій в соціальної сфері, регулювання форм взаємодії між органами влади, фізичними і юридичними особами, питання їх ідентифікації, підвищення рівня інформаційної безпеки та захисту інформації в інформаційно-комунікаційних системах соціальної сфери та подолання цифрової нерівності на різних рівнях.

----------***----------

Борисов О. Ю., *магістрант ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник: **Фурашев В. М.,**
к.т.н., с.н.с., доцент ФСП КПІ ім. Ігоря Сікорського.

МІНСЬКІ ДОМОВЛЕНОСТІ У СВІТЛІ КОНСТИТУЦІЇ УКРАЇНИ

З давніх давен політика відігравала значну роль в житті народів і держав. Але не завжди рішення політиків відповідають очікуванням людей та реальним потребам держави, більше того, політичні рішення не завжди відповідають навіть нормам закону і моралі. Дана проблема зберігає свою актуальність і в сучасному світі.

Минає 4-й рік з початку перших боїв на сході України. Лічильник втрат серед українських воїнів та мирного населення давно перевалив за позначку у 10 000 осіб, а наступальну війну 2014 року змінила позиційна, яку красномовно називають «режимом припинення вогню». Переваги нинішньої ситуації на фронті активно висвітлюються міжнародними та українськими політичними діячами. Ми ж маємо дещо інші переконання щодо ситуації в Україні та (не)ефективності домовленостей із загарбниками.

Позиційною війна в Україні стала через встановлений так званими Мінськими домовленостями режим припинення вогню. Згідно цих домовленостей захисники України отримали наказ із забороною першими відкривати вогонь по супротивнику та вести будь-які наступальні дії. Артилерію та важке озброєння було відведено від лінії фронту. Тих самих умов мала б дотримуватись й інша сторона конфлікту.

Проте, факти свідчать про відсутність тиші на фронті та щоденні втрати з нашого боку. Таким чином, війна продовжується, але через угоди з терористами Збройні сили України не можуть вести її з використанням всіх наявних засобів, на відміну від супротивника, який не цурається порушувати будь які домовленості щодо припинення вогню та використання важкого озброєння.

Цікавий факт, провідні держави світу, як правило, не ведуть перемовин з терористами. Єдиною їх реакцією на збройну агресію з боку незаконних збройних формувань є адекватна збройна відповідь.

❖ Так, лідер міжнародної терористичної організації «Аль-Каїда» – Осама бен Ладен був ліквідований Американськими силами спеціальних операцій. Причому відповідна спецоперація проводилася спецпризначенцями США на території суверенної держави – Пакистану без жодного погодження з її державними органами. Таким чином Сполучені Штати Америки в черговий раз продемонстрували світові готовність захищати власні інтереси та безпеку в будь-якому регіоні планети навіть не надто правомірними шляхами.

❖ Керівник чеченського визвольного руху – Шаміль Басаєв був свого часу знищений російськими спецслужбами. ЗМІ, представники силових структур та високопосадовці тоді активно використали дану подію для покращення власної репутації та переконання населення у правильності та переможності боротьби з повстанцями.

❖ Ісламська Держава – сучасний оплот глобального тероризму, сьогодні знаходиться на межі знищення об'єднаними силами Коаліції. Державні службовці та політики країн-учасниць міжнародної антитерористичної операції протягом всього часу її проведення активно заявляють про необхідність подальшої міжнародної взаємодії з питань боротьби з організованим тероризмом.

В той же час, лідери розвинутих держав світу, які успішно знищують будь-які загрози їх незалежності та суверенітету, а нині ще й опікуються ситуацією в Україні, переконують світове співтовариство, що єдиним шляхом до припинення війни в Україні є подальше дотримання Мінських домовленостей.

Чи варто пояснювати, що домовляння із загарбниками на міжнародному рівні жодним чином не узгоджуються з принципами міжнародного права, серед яких є принципи непорушності державних кордонів і територіальної недоторканості держав. Не відповідають Мінські домовленості і положенням Конституції України, стаття 2 якої визначає територію України як цілісну і недоторкану. Адже ідучи на перемовини з терористами, Україна фактично поставила під удар власний суверенітет та недоторканість, визнала, що перегляд кордонів незалежної держави можливий попри будь-які міжнародні заборони.

На наше тверде переконання, наслідком Мінських угод є лише консервування конфлікту, подальше обмеження конституційних прав та свобод певної частини українських громадян, а не його реальне вирішення. Одностороннє виконання домовленостей позбавляє нашу державу можливості перемогти у війні та відновити свою територіальну цілісність.

Варто зазначити деякі негативні наслідки консервування збройного конфлікту:

- деморалізація війська та суспільства;

- поступове формування у цивільного населення ілюзії мирного життя, ціною якого є щоденні втрати в зоні конфлікту;

- матеріальне виснаження держави.

У довгостроковій перспективі такі процеси зможуть призвести до чого завгодно, але не до перемоги у війні і не до відновлення соборної та незалежної України.

Таким чином, на нашу думку, Мінські домовленості не відповідають національним інтересам України, суперечать принципам міжнародного права,

Конституції України і сприяють лише затягуванню конфлікту, а не його реальному вирішенню.

Не слід забувати давню істину: той, хто поміж війною і безчестям обирає безчестя, у підсумку все одно отримує війну.

----------***----------

Касперський І. П., *доцент спеціальної кафедри Національної академії СБ України к.ю.н., с.н.с., доцент.*

ПРОБЛЕМИ АВТОМАТИЗАЦІЇ НАДАННЯ ЮРИДИЧНИХ ПОСЛУГ В УКРАЇНІ

Технічний прогрес намагається увійти майже у всі сфери суспільного буття, спрямовуючи та об'єднуючи зусилля людства довкола найактуальніших завдань та викликів сьогодення. У зв'язку із цими процесами перед нами все частіше постає питання про те, до якої межі ми можемо дозволити сучасним технологіям замінити нас у нашій звичайній діяльності. Використання штучного інтелекту дійсно дозволяє прискорити, знеособити, зменшити вартість окремих звичних процедур, проте одночасно породжує і страх залежності від прийняття рішень машиною, яка може помилитись та діяти всупереч нашим інтересам не усвідомлюючи хибності власних дій.

Особливо критичної уваги потребує автоматизація тих процесів, в ході яких відбувається обмін інформацією з обмеженим доступом, що викликає потребу взаємної довіри між суб'єктами таких стосунків. Саме до такого виду відносин і належить надання юридичних послуг, автоматизація яких на сьогодні сягнула помітного рівня як за кордоном, так і в Україні.

Для розуміння суті процесів потрібно проаналізувати можливості такої автоматизації, які на сьогодні вже створено. За повнотою вирішення завдання ці послуги можливо поділити на декілька рівнів.

Перший рівень являє собою надання довідкової інформації, щодо суб'єктів, які пропонують юридичні послуги, зокрема при потребі термінового виклику адвокатів для супроводу слідчих дій. Це системи «Oblava bot» [1] та «Legal Alarm» [2].

На другому рівні пропонують аналітичні послуги такі як прогноз судової перспективи конкретної справи системою «Дом юриста Analytics» [3].

На третьому рівні системи готові формувати юридичні документи: контракти для ІТ-компаній («Bot and partners») [4] та заяви про розірвання шлюбу («Sudobot») [5].

На четвертому рівні починається супровід тендерних процедур («Easy Tender») [6] та рекламацій до авіакомпаній («Air Advisor») [7] або інтернет-магазинів («Pinky Solutions») [8].

Усі вказані групи послуг не пропонують кінцевих рішень, вони лише частково доповнюють функції юристів, проте з'явилась і система Patent Bot [9], яка забезпечує кінцеве рішення – реєстрацію торгової марки.

За кордоном цю сферу іменують Legal Tech і пропонує вона програмні продукти та ресурси як для користування самими юристами наприклад для перевірки дійсності отриманих документів, так і для кінцевого споживача – перевірка обґрунтованості штрафних санкцій за порушення правил паркування [10].

Безсумнівно, використання таких систем надає споживачам низку переваг. У першу чергу інтернет-боти спрощують доступ до юридичних послуг: скорочується час між виникненням потреби у допомозі юриста і початком консультації, зменшується собівартість послуг, нівелюється можливий суб'єктивізм у особистому несприйнятті клієнтом конкретного юриста.

Але ризиків щодо якості та результативності такої допомоги у порівнянні із класичним юридичним супроводом значно більше. Першою і найсуттєвішою проблемою стає забезпечення конфіденційності обміну інформацією між клієнтом і віртуальним юристом, бо за законодавством в інтересах клієнта необхідно забезпечити захист адвокатської таємниці [11]. Сам факт застосування мережевих ресурсів значно ускладнює захист інформації, бо простим шифруванням даних, який застосовується у сучасних системах обміну повідомленнями, на яких базуються деякі боти, тут не обійтись. Другий і ще суттєвіший ризик породжує шаблонність роботи наперед запрограмованих алгоритмів. На якість виконання простих завдань, таких як укладення стандартних документів це не впливає, проте за умови участі ботів у підготовці до спорів шаблонно прийняті рішення породжують спокусу формування таких же шаблонів протидії штучно та прогнозовано сформованій лінії захисту, якій до того ж буде складно врахувати індивідуальні особливості кожного клієнта.

Виходом із цієї ситуації вбачається запровадження обов'язкової сертифікації програмних та програмно-апаратних засобів, які використовуються з метою надання юридичних послуг, за двома напрямами: рівень технічного та криптографічного захисту інформації (Держспецзв'язку) та відповідність чинному законодавству (Мін'юст). Такі заходи дозволять юридичним фірмам забезпечити додаткові гарантії захисту прав своїх клієнтів у процедурах автоматизації надання юридичних послуг.

Список використаних джерел:

1. Поліція на порозі? OBLAVAbot в допомогу.- [Електронний ресурс]. – Режим доступу: http://loyer.com.ua/uk/politsiya-na-porozi-oblavabot-v-dopomogu/

2. LEGAL ALARM: ваша безопасность в один клик.- [Електронний ресурс]. – Режим доступу: http://www.legalalarm.com
3. Як побудовано Дом юриста Analytics.- [Електронний ресурс]. – Режим доступу: http://analytics.domjurista.ua/#/analytics/about-system
4. Скрипин В. Украинские юристы Axon Partners запустили нового бота, который помогает IT–компаниям составлять договоры.– [Електронний ресурс]. – Режим доступу: https://itc.ua/news/ukrainskie-yuristyi-axon-partners-zapustili-novogo-bota-kotoryiy-pomogaet-it-kompaniyam-sostavlyat-dogovoryi/
5. Публічна оферта на використання програмного забезпечення SudoBot. – [Електронний ресурс]. – Режим доступу: http://sudo.bot.lawyer /terms
6. EasyTender — Государственные закупки: как участвовать в тендере Прозоро. – [Електронний ресурс]. – Режим доступу: https://easytender. com. ua /about-us/
7. Отримайте компенсацію, якщо ваш рейс затримали, скасували або вам відмовили в посадці за останні 3 роки.– [Електронний ресурс]. – Режим доступу: https://airadvisor.com/ua
8. Pinky solutions – платформа по онлайн разрешению споров.– [Електронний ресурс]. – Режим доступу: http://pinky.solutions
9. Just TM it !.– [Електронний ресурс]. – Режим доступу: https://patent. bot.lawyer/home?PGID=1&CMD=SET_LANG&LANG=2
10. Новак Н. Legal Tech: коли боти замінять юристів. – [Електронний ресурс].Режимдоступу:https://www.epravda.com.ua/publications/2018/02/14/634059/
11. Закон України «Про адвокатуру і адвокатську діяльність» від 5.07.12 р. // Офіційний вісник України від 23.08.2012 — 2012 р., № 62, стор. 17, стаття 2509, код акту 62964/2012

----------***----------

Камоцкий А. Б., *к.ю.н., доцент кафедры информационного права и права интеллектуальной собственности ФСП КПИ им. Игоря Сикорского*

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ: ПРАВОВЫЕ, ПСИХОЛОГИЧЕСКИЕ И ТЕХНИКО - КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ

Проблемы защиты информации в автоматизированных системах обработки данных интенсивно обсуждаются в зарубежной печати вот уж более 20 лет. При этом необходимо отметить, что с течением времени интерес к проблеме практически не снимается. Достаточно сказати, что, например, только в США ежегодно публикуются сотни работ (в том числе и монографий) по различным аспектам защиты информации, регулярно проводятся специальные совещания, симпозиумы и конференции. Все это красноречиво говорит о научно

– практическом интересе, проявленом зарубежными специалистами к рассматриваемой проблеме.

Информатизация общества, развитие средств вычислительной техники (СВТ) породили новые способы хищения. Наряду с ростом традиционных видов преступлений увеличиваются правонарушения, преступления, совершаемые с помощью компьютера.

Действия электронных преступников оказались в центре внимания средств массовой информации и специалистов различных отраслей знаний. Значительное распространение получило хищение кредитных карточек, с помощью которых осуществляются безналичные расчеты при покупке товаров в розничной торговле. Особо отмечают зарубежные специалисты опасноcть электронных преступлений в области финансов. Американские специалисты утверждают, что за несколько последних лет убытки по этой статье составили десятки миллионов долларов.

До недавних пор пользователи автоматизированных систем обращали внимание главным образом на организацию надежной охраны СВТ от поломок и краж. Однако практика показала, что связанные с этим издержки ничто по сравнению с убытками, наносимыми в результате утечки хранимых в ЭВМ сведений, пропаже или фальсификаций машинных программ.

Специалисты утверждают, что последствия от несанкционированного получения информации сегодня могут иметь самый различный масштаб: от безобидной проказы до воровства такого размера, по сравнению с которым меркнут знаменитые ограбления банковских бронированных автомобилей.

Как отмечается в исследованиях, проводимых западными учеными, проведение деловых операций с использованием персональных компьютеров обострили проблему промышленного шантажа, других преступлений в области предпринимательства.

Как утверждают американские специалисты, в последнее время резко участились случаи хищения программ для ЭВМ. По заявлению специалистов, эти хищения приняли характер эпидемии: на каждую законную копию программы имеющей сколько-нибудь широкое распространение, существует минимум четыре (а по некоторым оценкам, даже 10 и более) копии, полученные незаконным путем. С ростом успеха программы растет и количество незаконных копий. Объясняется это относительно дороговизной программ и большой важностью их для эффективной работы вычислительных систем.

Большинство крупных фирм в целях повышения оперативности расчетов стремятся запрограммировать и ввести в память ЭВМ все данные о сотрудниках, клиентуре, рынках сбыта, торговых партнерах и их технико-экономическом потенциале. Чем выше концентрация введенных в ЭВМ сведений, тем большими неприятностями чреват доступ к ним посторонних лиц.

Содержащая сведения магнитная лента или другие носители информации представляют непосредственный интерес для конкурентов и они, подчас, готовы платить за них миллионы.

В новых условиях объектами преступных посягательств, наряду с банками и ювелирными магазинами, все чаще становятся вычислительные центры с хранилищами социально-экономической информации. Но наибольшую опасность, по результатам анализов, представляют сами работники вычислительных центров.

Лицам, обладающими специальными познаниями, подчас достаточно лишь нажатие кнопки на электронно-вычислительной машине для совершения деяний связанных с нанесением материального ущерба.

По данным Федерального бюро расследований (ФБР), лица работающие на электронно-вычислительных машинах присваивают в среднем за одно преступление 500 тыс. долларов, т.е. в 20 раз больше, чем при использовании других методов хищения. Общая сумма ущерба от "электронного грабежа" ежегодно составляет более 600 млн. долларов.

Однако, по мнению специалистов, это далеко не полные данные, так как большинство "электронных воров" остаются неразоблаченными. Так исследователь А.Паркер из Стенфордского университета (штат Калифорния) в монографии "Преступление с помощью компьютера" констатирует, что не менее 85% подобных преступлений латентны, скрыты и поэтому безнаказанны. Специалисты единодушно считают, что число таких преступлений будет непрерывно расти, а похищаемые суммы увеличиваться, поскольку методы преступников совершенствуются, а средства и приемы их распознавания требуют серьезного, вдумчивого, научного анализа и разработки.

В зарубежной печати приводятся примеры "электронного рекета" - наиболее изощренного шантажа, и крупного вымогательства. В 1977 году были украдены магнитные ленты ЭВМ из правления концерна "ИСИ" в Амстердаме. Магнитные записи содержали информацию о планах концерна в Западной Европе, воссоздать которую было трудно и потребовалось бы много времени и средств. За возвращение магнитной записи воры потребовали у "ИСИ" 200 тыс. фунтов стерлингов. В другом случае трое служащих американского издательства "Британской энциклопедии" скопировали ленты, содержащие весьма важные справочные материалы и продали их конкуренту. Убыток издательства оценивался в суде примерно в 3 млн. долларов.

В исследовании, проведенным главным счетным управлением США, сообщается о многочисленных преступлениях "наиболее интеллигентных преступников XX века" в сфере банковских и кредитных операций.

Сержант военно-воздушных сил США, обслуживал компьютер, следящий за распределением горючего на военно-воздушной базе Кенеди (штат Техас) и

запрограммировал ЭВМ на покупку несуществующего топлива у мифических поставщиков. Компьютер без "колебаний" выдавал чеки фиктивным компаниям, "учреждениям" запрограммированных сержантом и его сообщниками. К моменту разоблачения злоумышленники успели прикарманить 100 тыс. долларов.

В одном из крупнейших гамбургских банков программист приказал компьютеру не округлять, как обычно, десятые доли, а отчислять их на его банковский счет. В итоге он получил 498 тыс. евро за 2 года.

Наиболее распространенный способ присвоения денег с помощью ЭВМ - программирование фиктивных счетов на вымышленных сотрудников при оплате работ. Так один из служащих фирмы "Залинген" (ФРГ) за короткий срок присвоил около 280 тыс. марок. Руководство предприятия обратило внимание на неожиданно возросшие расходы по зароботной плате, что и послужило основанием для проверки.

Дж. Макнайт (штат Нью-Йорк) в книге "компьютер - орудие преступлений" приводит курьезные данные об использовании "мертвых душ" сотрудниками вычислительных центров в целях личного обогащения. В ФРГ один из служащих химического концерна "продлил жизнь" умершему пенсионеру и получал на него причитающуюся тому пенсию, он несколько изменил программу и деньги стали поступать на его банковский счет. Аналогичный случай зарегистрирован в частной страховой компании Канады, где преступник в течении нескольких месяцев получал деньги на умерших клиентов. Только допущенная им путаница в банковских счетах позволила раскрыть преступление.

В США распространено присвоение денег при удержании завышенных налогов. Обычно при этом налогоплательщики не замечают недостачу в несколько центов при уплате налогов. Так, в федеральном налоговом управлении оператор ЭВМ переводил незначительные части средств, поступающих в виде налогов, на текущий счет родственников. Махинацию случайно вскрыл один из налогоплательщиков, по иронии судьбы оказавшийся однофамильцем получателя. В руководстве по расследованию таких преступлений приводят примеры, когда из подобных центов отчислений вырастали банковские счета в миллионы долларов.

Сейчас в США и других странах широко рекламируют совместное использование ЭВМ несколькими фирмами, для которых не под силу приобрести собственную вычислительную технику. В таких случаях связи клиентуры с ЭВМ осуществляется с помощью специального шифра, чтобы обеспечить неприкосновенность информации и программ пользователей. Однако и здесь выявилась тщетность предохранительных мер.

Группа банковских служащих выдавала коды своим сообщникам, которые использовали их для снятия денег со счетов вкладчиков. В одном из Нью-Йорских банков электронный мозг "эксплуатировали" сразу несколько человек, в том числе вице-президент и директор банка. В результате в карманы респектабельных жуликов перекочевало более 6,8 млн. долларов.

Многие руководители банков всерьез заинтересовались исследованиями» указывающими путь к решению возникших проблем. Введена более строгая процедура обращения с информацией. Цифровые носители с компьютерной информацией перевозят с теми же предосторожностями, что и валютные ценности. В крупных вычислительных центрах введен строжайший полицейский контроль за деятельностью обслуживающего персонала. Особенно контролируется доступ к информации, используемой при ведении крупных финансовых операций.

Однако положение усугубляется тем, что несведущие лица не в состоянии контролировать действия программистов и операторов. Шантажируя своих хозяев, предприимчивые жулики зачастую программируют и акт воздействия, возлагая его исполнения на саму ЭВМ. Так, недовольный служащий одного из центров в США составил программу таким образом, что через 8 месяцев после его ухода с работы в запоминающем устройстве ЭВМ были автоматически стерты все сведения о счетах. Отчаявшаяся администрация коммерческой компании тщетно взывала к совести клиентов, поместив многочисленные объявления в газетах с просьбой оплатить счета. Откликнулись лишь единицы и компания обанкротилась.

Фирмы, выпускающие ЭВМ, не любят сообщать ни о негативных последствиях использования СВТ, ни о мерах по защите информации. Оснащение ЭВМ дополнительной защитной информацией, аппаратурой и контрольными средствами приводит к значительному удорожанию системы, чего никто не хочет делать, да и не может себе позволить в условиях ожесточенной конкуренции. Не последнюю роль здесь играют и соображения делового престижа: клиент не захочет иметь дело с фирмой, не способной обеспечить сохранность капитала.

Проблема преступлений, совершаемых с помощью компьютера, сегодня настолько серьезна, что стала предметом специальных обсуждений в конгрессе США. Так, например, ещё в феврале 1980г. сенатор А. Рибиков выступил с предложениями по совершенствованию уголовного законодательства, касающегося этих преступлений. Приведя многие примеры злоупотреблений, сенатор обратился к президенту США с просьбой ускорить рассмотрение вопроса об усовершенствовании правил пользования СВТ и их защиты от несанкционированного доступа.

Здравомыслящие политические и общественные деятели отмечают, что корни преступности в современном обществе слишком глубоки, чтобы можно было всерьез рассчитывать выкорчевать их правовыми средствами. По мнению американских криминологов, "электронная преступность" лишь "надводная часть суперайсберга социально-экономических злоупотреб- лений". И это подтверждают цифры уголовной статистики. Ежегодно в США прямые убытки от хищений, совершаемых служащими, составляют около 10 млрд. долларов, взятки, вымогательства и хищения ценных бумаг – на 5 млрд. долларов.

В Америке, по мнению юристов, судебно правовая система терпит крах. Она просто не действует. Слишком часто преступники-рецидивисты, закоренелые нарушители законов, профессиональные преступники – называйте их, как вам угодно, грабят, насилуют и избивают абсолютно безнаказанно, и, как уже говорилось, в буквальном смысле слова, им сходят с рук даже убийства".

Таким образом, на повестку дня сегодня ставятся проблемные вопросы новых способов хищений, правонарушений совершаемых с помощью компьютера, промышленный шпионаж, "электронный рэкет".

Следовательно, практика ставит сегодня перед учеными юристами, кибернетиками и психологами вопросы, которые требуют научного исследования. Среди них:

– методы защиты информации в автоматизированных системах и персональных компьютерах и их технико-криминалистическое обеспечение;

– причины, способствующие преступным посягательствам на банки информации и разработки мер защиты от несанкционированного доступа;

– распознавание категории лиц (криминалистические, криминологические и психологические аспекты) способных совершать преступления с использованием современных средств вычислительной техники;

– разработки методов определения размеров убытка при совершении компьютерных преступлений;

– способов и методов хищения информации;

– методов борьбы с преступлениями связанных с использованием средств вычислительной техники.

ДЛЯ НОТАТОК

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Перемоги, 37
Київ, 03056

Підп. до друку 16.06.2018. Формат $60\times84^{1}/_{16}$. Папір офс. Гарнітура Times.
Спосіб друку – ризографічний. Ум. друк. арк.10,23. Обл.-вид. арк. 17,02. Наклад 75 пр. Зам. № 18-076.
Видавництво «Політехніка» КПІ ім. Ігоря Сікорського
вул. Політехнічна, 14, корп. 15
Київ, 3056
тел. (044) 204-81-78