

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

*Факультет соціології і права
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»*

Факультет права і адміністрації Варшавського університету

**КІБЕРБЕЗПЕКА ТА ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ:
ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ**

МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
21 квітня 2017 року

Частина I

Київ-2017

УДК 340.132:[342/951+004]+347.77/78
ISBN 978-966-622-833-1
К-38

Кібербезпека та інтелектуальна власність: проблеми правового забезпечення:
Матеріали міжнародної науково-практичної конференції. 21 квітня 2017 р., м. Київ, в 2-х частинах.. Частина перша. / Упоряд. : В. М. Фурашев, С. Ю. Петраєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. – 146 с.

Матеріали конференції присвячені проблемним питанням правового забезпечення кібербезпеки та права інтелектуальної власності у сучасних умовах розвитку інформаційного простору. У даній, основній, частині матеріалів конференції подані оцінки та пропозиції щодо вирішення питань, які окреслені тематикою конференції. Доповіді учасників конференції, що опубліковані у цій частині збірника можуть бути корисними для законодавців, вчених, фахівців та експертів інформаційної сфери та сфері інтелектуальної власності, науково-педагогічних працівників, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться сучасними суспільно-правовими проблемами інформаційної безпеки людини, суспільства та держави, забезпечення прав і свобод людини.

У другій частині цього збірника подані матеріали, які відображають студентський погляд на зазначену проблематику.

Участь у конференції взяли провідні експерти і вчені наукових установ і навчальних закладів України, Республіки Польща, представники зацікавлених державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право», «Правова інформатика» та Вісник НТУУ «КПІ» «Політологія. Соціологія. Право»

Матеріали подано у авторській редакції.

Упорядники: Фурашев В. М., Петраєв 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 № 3 від 16.05.2017 р.

Вченою радою факультету соціології і права

Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Протокол № 9 від .30.05.2017 р.

ISBN 978-966-622-833-1
К-38

© Науково-дослідний інститут інформатики і права НАПрН України, 2017
© Факультет соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», 2017
© Колектив авторів

ЗМІСТ

Новіков Б. В.	
«Інформаційне суспільство» у аксіологічному вимірі.....	5
Ожеван М. А.	
Академічна доброчесність й виховання поваги до інтелектуальної власності як пріоритетні напрями антикорупційної діяльності	10
Доронін І. М.	
Правові аспекти стратегічного планування забезпечення кібербезпеки України в сучасних умовах.....	19
Фурашев В. М.	
Проблеми забезпечення права на об'єкт інтелектуальної власності в умовах кібербезпеки.....	25
Андрощук Г. О.	
Кібербезпека: тенденції в світі та Україні.....	30
Довгань О.Д.	
Проблеми правового забезпечення кібербезпеки в Україні.....	36
Кодинець А. О.	
Правові засади реформування законодавства у сфері інтелектуальної власності.....	41
Małgorzata Dziewanowska	
Internet vigilantism - a threat or a chance for global society?	50
Гордієнко С. Г.	
Нормативне забезпечення деяких складових інформаційної сфери держави.....	52
Солончук І. В.	
Правове регулювання забезпечення кібербезпеки.....	58
Гуцалюк М. В.	
Актуальні питання правового забезпечення кібербезпеки в Україні..	63
Забара І. М.	
Кібербезпека Європейського Союзу: проблематика правового забезпечення.....	66
Каращук А.	
Забезпечення інформаційного суверенітету у кіберпросторі.....	75
Каніца Ю. М.	
Охорона авторського права у цифровій економіці в Європейському Союзі та питання адаптації законодавства України.....	78
Касперський І. П.	
Захист інформації в системах електронного урядування.....	82
Петряев С. Ю.	
Социальные риски киберсоциализации на пути к киберцивилизации.....	84
Радзієвська О. Г.	
Організаційно-правові заходи протидії негативним інформаційним впливам на дітей в Україні.....	91

<i>Петряєв О. С.</i>	
Протидія інтернет-активності радикального ісламу як проблема кібернетичної безпеки.....	95
<i>Дубняк М. В.</i>	
Правове регулювання інформаційної взаємодії в процесі прийняття рішень як фактор забезпечення кібербезпеки.....	98
<i>Іванова М. В., Голосніченко Д. І.</i>	
Інформація як продукт інтелектуальної власності в інформаційному суспільстві.....	102
<i>Цирфа Г. О.</i>	
Актуальні підходи щодо створення Вищого суду з питань інтелектуальної власності в Україні.....	106
<i>Гоголь Б. М.</i>	
Комерційна таємниця та конфіденційна інформація: окремі проблеми співвідношення.....	112
<i>Мисливий В. А.</i>	
Банківський кіберпростір як місце вчинення злочину.....	116
<i>Кириленко О. Г., Литвинова Л. А.</i>	
Відкритий доступ до знань в епоху цифрових технологій в контексті Гаазької декларації.....	119
<i>Яременко О. І.</i>	
Шкідлива інформація в змісті творів як об'єктів авторського права: проблема правової ідентифікації.....	127
<i>Троцька В. М.</i>	
Вільне використання творів для навчання.....	134
<i>Іванов Д. В.</i>	
Завдання суспільного мовника України у часи пост-правди та в умовах затяжної АТО.....	138
<i>Николаєнко Г.В.</i>	
Роль законодавства Європейського Союзу в розвитку державної статистики України.....	140

*Новіков Б. В., д.ф.н., професор
ФСП КПІ ім. Ігоря Сікорського.*

«ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО» У АКСІОЛОГІЧНОМУ ВИМІРІ

Один з найбільш жахливих, практично непоправних наслідків того, що ми ось вже понад чверть століття існуємо в «новому інформаційному просторі» є той, що країна зупинилась духовно. Не просто зупинилась – в наростаючому темпі деградує.

Люди, що вони попадають у світ (тенета) професійних «інформаційних мисливців» дуже рідко свідомі справжньої мети, справжньої участі, жеребу та долі, уготовленої їм маніпуляторами. Сприймаючи бажане за дійсне, знаходячись в перманентному стані напів-гіпнозу вони (інколи цілком щиро) вірять, що їм відкриваються всі таємниці буття, таємниці Всесвіту. Але наслідок такої гри з інформаційним вогнем завжди один і той же: знівечені долі, безповоротна втрата своєї неповторності, індивідуальності, хронічні стреси, роздвоєння особистості. Словом, проблеми вже не лише психологічного, але, скорше, психіатричного порядку.

І хто ж з них знає, що ставки – високі, що гроші – шалені, що гра – смертельна. Адже: хочеш зробити рабом – зроби невігласом.

Преса (ТБ, радіо, видавнича справа загалом, інтернет) – надто суттєвий важіль влади аби не належати нікому (це – з приводу ламентаций про «незаангажованість», «незалежність», «свободу» та «демократизм» засобів масмедіа). Будь-який з цих рупорів масової дезінформації грає по чужих нотах. Вільних імпровізацій в ділах подібних не буває. В принципі, себто, не буває. Категорично.

Гру «під хвилиний настрій» може собі нині дозволити хіба що редактор стіннівки або подібного їй друкованого органу з разовим тиражем один екземпляр.

Всі інші (без найменшого винятку) грають на замовлення, не завжди очевидне, але завжди добряче оплачене – грошима, положенням, званнями, посадами, привілеями, душевним комфортом. Страхом. Нещасними

випадками. Невмотивованими самовбивствами та загадовими дорожньо-транспортними пригодами. Для тих, хто нетямущим виявиться. Або ж – принциповим не в міру. Що поробиш: «інформаційне» суспільство...

Один зі стереотипів, притаманних індустрії масової дезінформації, індустрії неспонтанного міфотворення – виховання страхом. Раніше це були постійні (засобами теологічного, теократичного впливу) демонстрації (показові аутодафе, як земний прообраз страшного суду, невтомні нагадування про невідворотність гніву Божого і кари Божої, генерування і закріплення апокаліптичного комплексу, що він зачіпає глибинні пласти світогляду та світовідчуття), в нашому сьогоденні практикується в незрівнянно більших масштабах, та, по-своєму, «вишуканих» формах. Поставте маленький експеримент. Візьміть годинник і захронометруйте, скільки відсотків ефірного часу у випуску новин присвячено сюжетам, що вони щедро скроплені людською кров'ю: терористичним актам, вибухам, аваріям, насильницьким злочинам, катастрофам, війнам, збройним сутичкам... Зрештою, результати експерименту виявляється інваріантними, якщо його хронологічні рамки розширити до доби, тижня, місяця, року...

Історія все розставить на свої місця і розкаже істину про те, де були техногенні та природні катаклізми, а де – рукотворні диверсії. Але, поки сонце зійде – роса очі виїсть. Поки приголомшений і ошелешений таким натиском обиватель, «маленька людина» щодень накривається мокрим рядном такої «інформації» – йому не до Освіти, Науки, Гуманізму. Йому не до вивищених ідеалів і справжніх (класичних) зразків загальнолюдської Культури.

Йому б: шмат хліба, кухоль пива, день до вечора... Мені погано? А йому ж, тому, з екрана ТБ ще гірше, йому вже ніяк, його підірвали фугасом. Або ж: розчавили по асфальту грузовиком... То чому мені – погано? І яке мені діло до всіх до вас... А вам – до мене? (пам'ятає ще децицю з Кіплінга?) Все. З ним можна робити що завгодно: ліпити хоч конформіста, хоч пацифіста, хоч терориста, хоч пофігіста.

Що й треба було довести.

Адже ж – «інформаційне» суспільство.

«Ідеологічна обробка в умовах нинішнього «інформаційного» суспільства нічим не поступається, а багато в чому і перевершує «здобутки т. з. консервативних тоталітарних політичних режимів (прикладом може слугувати Іспанія часів інквізиції, або ж Німеччина, Італія, Португалія, Іспанія часів панування фашистських режимів.

Обробка свідомості (і підсвідомості) людей – конче необхідна справа, аби потому мати можливість маніпулювати поведінковими реакціями, практичними діями об'єктів подібної обробки. Саме цій меті все і підпорядковується. Особливість сучасної ситуації полягає лише в «багатоваріантності непрямого впливу на особистість як власне у вихованні, так і у вихованні засобами мистецтва. Останнє поділяється на елітарне і масове, але, переслідуючи на рівні ідеології єдину мету, відрізняється різноманіттям прийомів психологічного тиску на індивідуума, від явного до опосередкованого, малопомітного. Розвиток обох різновидів мистецтва однаково підтримується консервативним тоталітаризмом, бо обидва вони сприяють зміцненню його позицій: масове мистецтво – у вирішенні нагальних проблем, елітарне – в досягненні стратегічних цілей. Адже саме завдяки мистецтву «гола ідея» перетворюється на конкретику ілюзорного художнього простору, набуваючи помилкового статусу перевіреної досвідом істини. Відбувається приховане «бомбардування» підсвідомості реципієнта ідеологічними штампами. Прищеплені йому подібним чином стереотипи поведінки, ідеали, моральні норми органічно сприймаються згодом за власні «відкриття».

Одним з найважливіших елементів духовної культури консервативного тоталітаризму є масові видовища: від суто тотальних вистав до судових процесів, на зразок аутодафе. Подібні прояви масової культури консервативного тоталітаризму – могутній засіб впливу на емоційність натовпу, а, відтак – засіб керування ним». (Гринько О.Х. «Мистецтво в

системі культури тоталітарного суспільства». Автореферат канд. дис., Київ-2000, с.8)

Щоправда, вогнища аутодафе, що на них спалювали відьом та єретиків, масові факельні ходи, тисячні натовпи, що крокують під методичний барабанний бій – то вже в минулому. Але ж: то було в «доінформаційному суспільстві». Сьогодні в нас – «суспільство інформаційне». І немає найменшої потреби зганяти на площі населених пунктів юрби народу. В один час і в одне місце. Адже ж на вулиці – ХХІ століття. І в кожному домі, у кожній квартирі – телевізійний приймач. «Голубий вогник». «Ящики». Гаджети. І правду кажуть: сьогодні у дитини четверо батьків: тато, мама, телевізор персональний комп'ютер, «персоналка», айфон etc.

І твоєї згоди ніхто не питає, вриватися в твою оселю (а відтак – в свідомість, в душу, в психіку), а чи ні. І ти приречений «спілкуватися» (бо яке ж то спілкування, яка ж то взаємодія, який діалог?! Тут – гра в «одні ворота». Вплив, інтервенція, агресія) щодня, щовечора – зі знаючим свого справу «мисливцями» за духом, душею, тілом. Хто їх любить, кличе, жде в своїй домівці? Вони не горді: ходять «в гості» щодень засобами масової телекомунікації. «Інформаційне» суспільство, що поробиш...

Засобом тотального оглушення і отуплення є не лише зрушуваний на голови і душі читачів, слухачів, глядачів сільовий потік порнографії, насильства, апології жорстокості, вбивств, а й те, що я б назвав «кросвордизація» свідомості. Кросвордизація духу. Натомість повноцінного інтелекту, – розуму, – формується фрагментована, як агрегат здоровоглуздя та розсудковості – «кліпова свідомість».

Багатознання (поінформованість, сказали б сьогодні) розуму не навчає. Це знали ще древні. Але ж багатознання (ерудиція) досить вдало імітує розум!

От і заповнені екрани теле, радіоефір та сторінки масових видань речами на кшталт «поле чудес», «брейн-ринг», «що? де? коли?», «щасливий випадок», «о, щасливчик!» і тому подібних, без ліку. А що вже стосується

кресвордів, чайнвордів, сканвордів і тому подібного, то кожен другий пасажир метро сьогодні – увіткнутий носом у сторінку відповідного видання і напружує, напружує щиро свою пам'ять. Що він в ній, пам'яті, шукає? Залишки від «тоталітарної» освіти? Мабуть. Але ж – цілком щиро вважає, що росте. Інтелектуально. Так імітація засобами інформаційної (масової) комунікації об'єктивується. Баналізується. Утверджується повне та беззастережне домінування перетворених форм духу, почуттів, практик.

Мова не лише (хоча й про це – також) про те, що свідомо й цілеспрямовано понижується моральність народу, що пущена в розпил справжня естетична культура – надбання тисячоліть, свідомо руйнується менталітет людини: девальвуються почуття та виміри, цінності та характеристики, що вони, власне і відрізняють її від тварини, звіра, а чи то зомбі: совість, честь, вірність, солідарність, співчуття, альтруїзм і т. ін. Справа не лише в тому, що послідовно і з наростанням зусиль на місце поруйнованих людських якостей прищеплюються та насаджуються «вартості» та якості протилежні: безсовісність, безчестя, готовність зраджувати все, вся і всіх, егоцентризм та індивідуалізм, корисливість, байдужість до проблем ближнього (і дальнього), жадібність, жорстокість, агресивність, мізантропія і т. ін. Це – йде з наростанням і вже дає свої наслідки.

Ми вже не ведемо мову про баналізоване крадійство у сфері духу рафінованого, у сфері духу, котра дорогою ціною людству дається, але завжди вартує того, аби на ній, цій сфері, не економили. Ні зусиль, ні уваги, ні коштів.

Це – наука.

Хай фахівці дискутують щодо питань спеціальних, з галуззю наукознавства пов'язаних: скільки тих наук нині та як вони співвідносяться, як диференціюються та інтегруються.

В сенсі філософському ж цілком правомірно стверджувати: є одна Наука. І методологічним осереддям (серцем, мотором її розвитку) є

матеріалістична діалектика. Зупиніть це серце, зупиніть цей мотор – і неминуче зупиниться наука. Що потому? Звиття. Здичавіння.

З огляду ж на ту обставину, що матеріалістична діалектика сьогодні знаходиться в епіцентрі прискіпливої уваги та наростаючих зусиль всієї рати духовних «демократів», духовних умертвителів (це зумовлюється тією обставиною, що матеріалістична діалектика як методологія є становим хребтом бездоганної наукової теорії, наукового вчення про дійсний гуманізм), можна прогнозувати: вдасться умертвити діалектику – суспільство докінечно здеградує. Завважимо, що нині ціною подібної деградації вже не є чергова світова війна, але: гарантоване самознищення земної цивілізації. Всього живого на Землі, до вірусів, мікробів та бактерій включно...

От і виходить: немає балансу. Між інформацією та дезінформацією. Суцільний дисбаланс. На користь дезінформації...

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

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

АКАДЕМІЧНА ДОБРОЧИННІСТЬ Й ВИХОВАННЯ ПОВАГИ ДО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ЯК ПРИОРИТЕТНІ НАПРЯМИ АНТИКОРУПЦІЙНОЇ ДІЯЛЬНОСТІ

Термін *«академічна доброчесність»* впродовж останніх 2-3 років активно використовується в українській літературі з політико-правових та моральнісно-етичних питань підняття якості та конкурентоспроможності української освіти й науки. У цьому плані Україна серйозно відстала від світових та європейських трендів, оскільки відповідний англomовний термін *«academic/scientific honesty»* (антонімом є *«academic/scientific dishonesty»*) на Заході віддавна використовується у контексті політики «нульової толерантності щодо порушників кодексу честі (*«zero tolerance honor code»*) тощо.

Хоча більш вдалим, з нашої точки зору, є термін «академічна цілісність» чи «академічне зцілення» («academic integrity»). Бо, по-перше, «зцілення» в українській мові є синонімом «одужання». А, по-друге, «цілісність» освіти чи науки як суспільної інституції означає формально скріплений намір учасників великої соціальної групи (інституції) дотримуватися умов *соціального контракту*, за умов якого індивіди в обмін на користування певними правами беруть на себе певні зобов'язання щодо дотримання правил, норм, нормативів тощо.

Особливо загострилася боротьба з порушниками правил академічної доброчесності з моменту запровадження «Болонського процесу» як структурного реформування національних систем вищої освіти країн Європи й створення на цих засадах єдиного конкурентоспроможного європейського освітнього простору (The European Higher Education Area).

Болонський процес започаткували 29 країн у 1999 році. У 2005 році до нього формально приєдналася Україна, а станом на 2017 рік число країн-підписантів досягло числа 50-ть. Якщо на першому етапі вимоги до навчального процесу в вищій школі зводилися переважно до кількісно-структурних (число кредитів, трьохступенева модель «бакалаврат - - магістратура – докторантура тощо»), то нині дедалі більша увага надається якості освіти й боротьбі з різними зловживаннями, які загрожують втратою конкурентних переваг європейській освіті в цілому та освіті у кожній з європейських країн зокрема, набуттю таких переваг в майбутньому.

Досить мляво, хоча й послідовно реагує на Болонські процесуальні вимоги Україна, яка належить до небагатьох країн Європи, які не входять до Європейської асоціації із забезпечення якості вищої освіти [1]. Тільки в 2016 році нарешті було сформовано відповідний український орган - Національне агентство із забезпечення якості вищої освіти – НАЗЯВО.

В українській школі й вищій школі зокрема зазвичай відсутній мікроклімат «нульової толерантності» щодо порушників правил і норм академічної доброчесності (списувачів, плагіаторів тощо). Зате вітчизняна

школа постійно демонструє надмірну терпимість до «піратів» - порушників прав інтелектуальної власності.

Нова редакція Закону України «Про освіту» 3491-д від 04.04.2016 (Стаття 42. Розділ V *«Забезпечення якості освіти»*, перше читання відбулося у ВРУ в жовтні 2016 року) пропонує визначення *«академічної доброчесності»* як *«сукупності етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень»* [3].

Аналогічний запис відсутній в Законі України «Про вищу освіту», прийнятому Верховною Радою України 1 липня 2014 року (на зміну аналогічному попередньому закону, що діяв з 2002 року). Розділ V цього Закону *«Забезпечення якості освіти»* фактично звівся до інструкції щодо порядку формування НАЗЯВО. Положення цього закону, спрямоване на боротьбу з дисертаційним плагіатом, звелось до скромного запобіжного заходу: наукові роботи та відгуки опонентів перед захистом мають розміщуватися на сайтах вишів та інших академічних (наукових) закладів, де відбуватиметься процедура офіційного захисту.

Закон «Про вищу освіту» 2014 року встановив також скромні каральні санкції у разі виявлення академічного плагіату у захищеній дисертації (науковій доповіді). Це є підставою для скасування рішення спеціалізованої вченої ради про присудження наукового ступеня та видачу відповідного диплома. Строком на два роки у разі виявлення академічного плагіату позбавляються права брати участь у роботі спеціалізованих вчених рад науковий керівник (консультант), офіційні опоненти, які надали позитивні висновки про наукову роботу, та голова відповідної спеціалізованої вченої ради, а відповідна установа позбавляється акредитації відповідної постійно діючої спеціалізованої вченої ради та права створювати разові спеціалізовані вчені ради строком на один рік [4].

Оскільки академічна (наукова) культура є похідною від культури соціуму, то апіорі зрозуміло, що усі соціальні групи у хворому соціумі будуть хворими й дотримання соціального контракту учасниками окремої групи неможливе, якщо на рівні всього соціуму не діятиме «великий контракт».

Основними причинами *«академічної недоброчесності»*, з нашого погляду, є наступні:

- a. *філософсько-релігійно-світоглядні;*
- b. *моральнісно-етичні;*
- c. *методико-методогічні;*
- d. *політико-правові;*
- e. *соціальні, з криміногенними включно;*
- f. *корпоративні, включно з тими, що пов'язані з кризою освіти та науки;*
- g. *техніко-технологічні, включно з тими, що пов'язані з інформаційними революціями.*

Безумовно, зростанню серед студентів та дисертантів числа плагіаторів посприяла поява великого числа сайтів як легітимних і некомерційних (включно з тими, які наповнюються джерелами піратського походження), так і нелегітимних й комерційних («фабрики дисертацій»; «paper mills college essays»). Шахраюванню на іспитах та заліках серйозно посприяло активне вживання студентами смартфонів, айфонів та інших нових медіа для пошуку інформації в різноманітних Wiki; Googles.

Разом з тим, інформаційна революція посприяла й боротьбі з порушниками правил академічної доброчесності. Зокрема. різні пошукові машини пропонують на платній або безоплатній основі програми типу «Антиплагіат». А головне, машини-пошукувачі серйозно полегшили студентам та аспірантам (докторантам) пошук джерел інформації, можливості уточнення різних фрагментів текстів. Питання боротьби з порушниками правил академічної доброчесності й плагіату зокрема набуло

принципово нових вимірів разом з бурхливим розповсюдження онлайнової (дистанційної) освіти.

Слід зазначити відсутність серйозних філософсько-методологічних розробок з проблем порушення немайнових авторських прав, незахищених чинним законодавством та неосудних або напівосудних з морально-етичної точки зору. В античній та середньовічній філософії й науці взагалі було відсутнє поняття одноосібного авторства й чимало авторів видавало свої твори, користуючись «розкрученим брендом» Платона, Аристотеля тощо. Лише з початком у XVII ст. сучасної наукової революції утвердилося поняття «автора». І так тривало до 20-х рр. XX ст.

До того ж, в різних сферах науки й культури поняття авторства та визначення дольової співучасті в колективному авторстві має свою специфіку. Наприклад чимало медичних журналів взагалі відмовилися від поняття «*автор*» на користь поняття «*співучасник*» (contributor). З'явилося малозрозуміле поняття «почесного авторства». Ще менш зрозумілим з морально-етичної точки зору є «*примарне авторство*» «ghostwriters», коли автор залишається невідомим. Натомість за наполяганням фармацевтичних компаній «авторами» публікацій часто є відомі люди, які не мають жодного відношення до даного дослідження й навіть не давали згоди на використання їх прізвищ у переліках авторів. Звичайним явищем в українській науці та науці на всьому просторі СНД є приписування до прізвища справжнього автора (авторів) роботи цілої низки прізвищ авторів, які мають до цієї роботи суто опосередковане адміністративне відношення.

Своєрідним філософсько-світоглядним виправданням академічного шахрайства є філософія постмодернізму, послідовники якої проповідують концепцію «*смерті автора*» й феномену «*оригінальності текстів*». Вважається, що автор – це просто конструктор, який використовує шматочки чужих текстів, тобто діє за методом «нижниць і клею» (в комп'ютері ці функції відповідають опціям «*виріж і встав*»).

Постмодерністи закликають до принципової неточності висловлювань та уникання визначень, проповідують схильність до двозначностей; фрагментацію текстів і відсилання до компілятивно-мережевої гіпертекстової реальності.

Статусу істинності набуває задзеркалля штучної віртуальності, коли повідомлення важливіше від події, знання стає первинним щодо об'єктів та предметів знань, а природні тіла набувають вторинного статусу. Мистецькі (а почасти й наукові) твори перетворюються на різновиди криптограм, шарад та кросвордів, - вправ для розуму, які передбачають версії «аналізів" та «рішень».

В англomовній літературі описані такі різновиди «академічної недоброчесності» як *плагіат* (*plagiarism*); *таємна змова з метою наживи* (*collusion*); *фальсифікація даних* (*data fabrication*); *шахраювання* (*cheating*) [5-7].

Український законопроект Закону «Про освіту» пропонує такі різновиди «академічної недоброчесності»: *академічний плагіат; фабрикація (фальсифікація) результатів наукових досліджень; списування; хабарництво; обман* [3]. На жаль, український законопроект не виокремлює питання вищої школи і підготовки кадрів вищої кваліфікації (докторантів), а питання про хабарництво й обман ставить у загальному контексті, тоді як у школі й вищій школі зокрема тут існує своя делікатна «специфіка». яка полягає в існуванні чисельних «фабрик дисертацій», де трудяться «ghostwriters» («літературні негри»), послугами яких часто користуються недоброчесні, але матеріально забезпечені, студенти й аспіранти (докторанти).

На особливу увагу заслуговує питання *плагіату*. Латинське «*plagiarius*» початково стосувалося викрадення дітей, рабів, тобто мало стосунок до явища, яке нині прийнято позначати як «*кіднепінг*». Згодом *плагіаторами* почали називати викрадачів (присвоювачів) чужих літературних текстів.

З методологічної точки зору доцільно розрізняти концептуальний (парадигмальний) та периферійний плагіат. Те, що зазвичай вважають плагіатом насправді часто є незумисним порушенням правил роботи з джерелами інформації: неточності в цитуванні джерел, надто тісний щодо джерела походження парафраз (переказ) чужої думки тощо [8].

Плагіат в концептуально-парадигмальному сенсі є зумисним, мотивованим бажанням обманути «лоха», викраденням чужої інтелектуальної власності або її запозиченням без наміру коли-небудь повернути позичене. Зло, пов'язане з плагіатом, полягає передусім в тому, що він плодить чималу когорту невігласів, які так по-справжньому ніколи не вчилися, позахищали «липові» дисертації, але згодом, заволодівши відповідними дипломами й званнями, імітують фаховість й можуть навіть посідати керівні посади, створюючи вертикально інтегровані імітаційні структури.

В остаточному сенсі вузівський плагіат тісно узалежнений від культурних традицій. Російській професор, який із Прибалтики приїхав працювати в Росію (м.Пензу) був неприємно вражений поблажливим ставленням до плагіату як викрадення інтелектуальної власності в РФ й констатував: «Прибалтика - частина Європи, причому не тільки в географічному сенсі. Там будь-яке крадійство включно з плагіатом непопулярне і може призвести до втрати репутації. Зовсім інша справа Росія, де крадійство, на думку багатьох європейців, мало не національний спорт, а поняття «репутація» вже давно не існує» [9].

Поширене у всьому світі явище існування ринків інтелектуальних послуг й «примарного» чи підставного авторства» («ghostwriters») не отримало поки що однозначної правової й моральної оцінки. З одного боку, з цим феноменом пов'язані конгломерати «фабрик дисертацій». За даними британської спеціалізованої агенції з якості вищої освіти (аналог українського НАЗЯВО) в Великобританії нараховується більше сотні подібних фабрик («essays mills») [11]. Усі вони пропонують «plagiarism-free

content» хоча насправді є типовими колективними плагіаторами, оскільки фактично практикують викрадення чужої інтелектуальної власності, формально не порушуючи авторського права.

Звичайно, плоди сумнівної діяльності подібних «фабрик» не давали б жодного зиску їхнім власникам та «літературним неграм» у них задіяним, якби ця діяльність не отримувала підтримки «нагорі», на рівні недоброякісних захисних рад, вузівських адміністрацій тощо та різних високопосадовців, які самі часто експлуатують «літературних негрів» з метою захисту «вір-дисертацій», написання «епохальних творів», мемуарів тощо.

Різні країни пропонують різні практики боротьби з «essays mills», У США зокрема немає федерального закону, який забороняв би подібну діяльність, хоча такі законні обмеження діють на рівні окремих штатів. Подібна заборона діє в Новій Зеландії. Проте «essays mills» завжди можуть знайти обхідні шляхи щодо подібних обмежень та заборон. Наприклад, одна з найбільших в Великобританії «фабрик паперів» Elizabeth Hall Associates спонукала для перестрахування замовників академічних праць підписувати зобов'язання (disclaimer), що вони не будуть куплений інтелектуальний продукт представляти в вузі як остаточний, видаючи його за свій власний, а використовуватимуть його виключно як «модельний об'єкт» (a guidance model only) [12].

У будь-якому разі, заради збереження й примноження належної якості освіти в Україні, оздоровлення інтелектуального клімату слід негайно запозичувати та імплементувати подібний світовий досвід і повести рішучу боротьбу з академічною (науковою) недоброчесністю у всіх її формах та різновидах, що має перетворитися на один з перспективних напрямів створення в країні антикорупційної системи.

Список використаних джерел:

1. The European Association for Quality Assurance in Higher Education (ENQA). [Електронний ресурс]. – Режим доступу: <http://www.enqa.eu/>
2. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. — Київ: Ленвіт, 2006. — 35 с.
3. Проект Закону про освіту. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=58639
4. Про вищу освіту. Закон України від 01.07.14 р. № 1556-VII // Голос України. 06.08.14 р. № 148.
5. Macdonald, R., Carroll, J. Plagiarism: A complex issue requiring a holistic Approach // Assessment and Evaluation in Higher Education, 2006. No. 31(2). P. 233–245.
6. Sutherland-Smith, W. Plagiarism, the internet and student learning: Improving academic integrity. New York: Routledge. 2008.
7. Davis, Mary. Formative feedback within plagiarism education: Is there a role for text-matching software? // International Journal for Educational Integrity. Vol. 5. No. 2. December, 2009, pp. 58–70.
8. Vander Schaaf, Anthony. Plagiarism: A philosophical analysis of aspects of property, theft, and deception. A Thesis Presented to The Faculty of Graduate Studies of The University of Guelph (Canada), 2005. ProQuest Dissertations Publishing, MR11174.
9. Левин В.И. Плагиат в российской науке // Alma Mater, № 6, Июнь 2014, С. 111-114.
10. Stevenson, Seth, Adventures in Cheating. A guide to buying term papers online // Slate. [Електронний ресурс]. – Режим доступу: http://www.slate.com/articles/life/shopping/2001/12/adventures_in_cheating.html
11. Yorke, Harry. University students could be fined or handed criminal records for plagiarised essays, new proposals suggest // The Telegraph. 21 February 2017. [Електронний ресурс]. – Режим доступу: <http://www.telegraph.co.uk/education/2017/02/21/university-students-could-fined-handedcriminal-records-plagiarised>
12. Major, Lee Elliot Web of Deceit // The Guardian. 8 January 2002. [Електронний ресурс]. – Режим доступу: <https://www.theguardian.com/education/2002/jan/08/highereducation.students>

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

ПРАВОВІ АСПЕКТИ СТРАТЕГІЧНОГО ПЛАНУВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Стратегічне планування у сфері забезпечення кібербезпеки є надзвичайно важливим завданням з огляду на існування та ескалацію відповідних загроз глобального характеру. Зокрема, за даними «Звіту глобальних ризиків 2016 року», підготовленого для Всесвітнього економічного форуму, «несприятливі наслідки технологічного прогресу», «вразливість критичної інфраструктури та критичних мереж», «широкомасштабні кібератаки та значні інциденти втрати даних» є глобальними ризиками світового масштабу [1, р.90, 93]. Реагування на такі загрози є важливим завданням із забезпечення національної безпеки для переважної більшості країн сучасного світу. Більш того складний та динамічний характер зазначених загроз вимагає вжиття швидких та адекватних заходів і посилення взаємодії на міждержавному, глобальному, регіональному та двосторонньому рівнях.

Реалізація оборонних (безпекових) функцій держави, що зумовлює вжиття заходів протидії складним сучасним загрозам, неможлива без відповідного стратегічного планування у цій сфері. В Україні таке планування відбувається шляхом ухвалення документів стратегічного планування. Стаття 2 Закону України «Про основи національної безпеки України» до числа документів стратегічного планування, на підставі яких розробляються конкретні програми за складовими державної політики національної безпеки, відносить Стратегію національної безпеки України та Воєнну доктрину України [2]. Стратегія та доктрина розглядається на засіданні Ради національної безпеки і оборони України, ухвалюються її рішенням та вводяться в дію Указом Президента України. За останні роки у нашій державі було ухвалено декілька редакцій таких документів.

Як показує побіжний аналіз змісту визначених цими документами заходів, проблеми забезпечення кібербезпеки розглядались в контексті євроатлантичної інтеграції, або ж були регламентовані шляхом імплементації міжнародно-правових актів щодо боротьби з кіберзлочинністю.

Зокрема, у п. 2.8 Стратегії національної безпеки, затвердженої Указом Президента України від 12.02.2007 № 105/2007 [3], як такий, що наближається до критичного, оцінено стан безпеки інформаційно-комп'ютерних систем в галузі державного управління фінансової і банківської сфери, енергетики транспорту, внутрішніх та міжнародних комунікацій. З метою реалізації державної політики п. 4.1 Стратегії було визнано за необхідне розробити і впровадити національні стандарти та технічні регламенти застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами.

Визначений першою редакцією Стратегії підхід з одного боку передбачав пріоритет державного впливу на рівні національних стандартів та технічних регламентів, а з іншого – зумовлював вжиття заходів правового регулювання відповідно до вимог міжнародно-правових актів, взятих на себе міжнародних зобов'язань і вимог гармонізації законодавства до європейських стандартів. Таким чином, межі та заходи прямого державного втручання було мінімізовано.

Через п'ять років Указом Президента України від 08.06.2012 № 389/2012 було затверджено нову редакцію Стратегії національної безпеки України з підназвою «Україна у світі, що змінюється» [4]. Зміна редакції Стратегії в першу чергу була зумовлена змінами у політичному курсі держави - зупиненням курсу євроатлантичної інтеграції. Характеризуючи безпекове середовище, серед чинників впливу на національну безпеку зазначений стратегічний документ визначав: «нездатність держави протистояти викликам, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації», насамперед кіберзагрозам. Водночас чинна на той час редакція ст. 8 Закону України «Про основи національної

безпеки України» серед загроз в інформаційній сфері визначала: - прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерну злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Таким чином, новітні виклики і загрози на рівні документів стратегічного планування фактично не було визначено, оскільки комп'ютерна злочинність та комп'ютерний тероризм далеко не повністю охоплюють такі загрози.

Серед завдань забезпечення інформаційної безпеки, окрім визначених у першій редакції Стратегії, додатково було зазначено: - стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів; - забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури; - створення національної системи кібербезпеки.

І нарешті, у чинній редакції Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.2015 № 287/2015 [5], серед загроз інформаційній безпеці визначено: - ведення інформаційної війни проти України; - відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Загрозами кібербезпеці і безпеці інформаційних ресурсів є: - уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; - фізична і

моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Отже, у чинній Стратегії національної безпеки України характеристику сучасних загроз кібербезпеці обмежено, а фактично зведено до кібератак та застарілості системи охорони інформації з обмеженим доступом. З іншого боку, визначення як окремої загрози ведення інформаційної війни проти України розширило поле, яке характеризує загрози у кіберпросторі.

Формулюючи основні напрями державної політики щодо забезпечення кібербезпеки та інформаційної безпеки, внаслідок розділення цих сфер безпеки не вдалося уникнути певного дуалізму і у формулюванні напрямів політики. Зокрема, створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них і моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації є багато у чому пов'язаними заходами. До того ж розвиток інформаційної інфраструктури держави стосується не тільки забезпечення кібербезпеки, а й інформаційної безпеки також.

Слід зазначити, що у березні минулого року було ухвалено новий вид документу стратегічного планування – Стратегію кібербезпеки України [6]. Хоча його прийняття не викликано прямими вимогами чинного законодавства, оскільки Закон України «Про основи національної безпеки України» визначає необхідність ухвалення тільки Стратегії національної безпеки і Воєнної доктрини. Оскільки існування Стратегії кібербезпеки було новим для нашої держави, її розробка та ухвалення не зумовлювалося прямими вимогами чинного законодавства, можливо стверджувати, що при цьому керівництво держави не в останню чергу виходило з наявних трендів у світовій політиці забезпечення безпеки. Протягом останніх п'яти років такі стратегії, як документи стратегічного планування, ухвалено практично в усіх державах світу. Незважаючи на різні правові та політичні системи, в їх переважній більшості демонструвались спільні підходи. Зокрема, спочатку характеризувалось безпекове середовище, кіберпростір, наявні та потенційні

загрози, а потім – відповідні заходи реагування в залежності від характеру загроз. Слід зазначити, що заходи з протидії загрозам, як правило, не були деталізовані, а лише визначали відповідні напрями політики.

Подібний підхід застосовано і у Стратегії кібербезпеки України. На рівні виступу неможливо дати повний аналіз змісту зазначеного документу. Водночас слід звернути увагу на певні аспекти правового характеру. Насамперед, роль зазначених документів стратегічного характеру в сучасній Україні не передбачає прямого впливу на державне управління, визначення організаційних заходів, також вони не є правовими нормами прямої дії. У той же час, характер організаційних заходів, який пропонується, вимагає змін у чинному законодавстві. Якщо проаналізувати імплементацію положень Стратегії кібербезпеки України, то вона відбувається шляхом затвердження розпорядженнями Кабінету Міністрів України Планів заходів на рік [7,8]. За останні півтора роки ухвалено вже два плани. На нашу думку мова може йти про певну надмірність планування. Існуюча світова практика дещо інша. Наприклад, Стратегія кібербезпеки Чорногорії, що містить як додаток План дій, визначає період планування у 4 роки, а не в один рік [9]. Аналогічний підхід застосовано у Великій Британії, Чехії, Словаччині, Естонії, Литві, Ірландії, Туреччині, Канаді та інших країнах. Щорічне планування призводить до систематичного невиконання заходів, зміни відповідальності державних органів, бюрократизації процесу виконання та інших негативних моментів організаційного характеру. Що і має місце якщо проаналізувати зміст Планів заходів з виконання Стратегії кібербезпеки за два останні роки.

Іншим проблемним питанням, є стан реалізації правотворчих заходів, які передбачені зазначеними документами. Якщо у Плані заходів на 2016 рік передбачено формулювання переліку першочергових нормативно-правових актів, які потребують розроблення та внесення змін, як перший захід, то у Плані заходів на 2017 рік передбачено вже 6 законотворчих пропозицій з термінами підготовки у першому півріччі, і ще принаймні 7 заходів явно містять нормотворчу компоненту на рівні підзаконних актів. При цьому такі

заходи знову очолюють розроблений Кабінетом Міністрів України план. На нашу думку такий стан речей є черговою ілюстрацією надмірної захопленості нормотворчою складовою реформ, коли розробка законопроектів та нормативно-правових актів є основним (а іноді єдиним) заходом реагування державних органів на сучасні виклики та загрози.

Зазначене у виступі дозволяє прийти до наступних висновків:

1. З огляду на сучасний стан загроз в інформаційній сфері формулювання основних напрямів державної політики на рівні документів стратегічного планування, у тому числі затвердження в Україні Стратегії кібербезпеки, є виправданим.

2. Необхідно змінити підходи до обмеження визначення документів стратегічного планування, що міститься у чинному Законі України «Про основи національної безпеки України», з метою більш швидкого і адекватного реагування на поточні та перспективні загрози.

3. При плануванні конкретних заходів забезпечення кібербезпеки на рівні держави необхідно відійти від практики щорічного планування, збільшити період, який планується до 4-5 років.

4. Існуючий механізм реалізації заходів стратегічного планування шляхом правотворчості виглядає не зовсім обґрунтованим, оскільки зміни у законодавстві мають бути не метою, а засобом забезпечення державної політики, у т.ч. з забезпечення кібербезпеки.

Список використаних джерел:

1. The Global Risks Report 2016. 11 Edition.— [Електронний ресурс]// World Economic Forum - Електрон.дані. — 2016. — Режим доступу:<http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf>. — Назва з екрана. — Дата звернення: 13.04.2017р.

2. Закон України «Про основи національної безпеки України»//Відомості Верховної Ради України. — 2003. - № 39. — Ст. 351.

3. Стратегія національної безпеки, затверджена Указом Президента України від 12.02.2007 № 105// Офіційний вісник України. — 2007. - № 11. — С. 7, Ст. 389.

4. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України»//Офіційний вісник Президента України. – 2012. - № 20. – С.9, Ст. 470.

5. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»//Офіційний вісник Президента України. – 2015. - № 13. – С.50, Ст. 874.

6. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96//Офіційний вісник Президента України. – 2016. - № 10. – С.39, Ст. 198.

7. Розпорядження Кабінету Міністрів України від 24.06.2016 № 440-р «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України»//Урядовий кур'єр від 05.07.2016. - № 123.

8. Розпорядження Кабінету Міністрів України від 10.03.2017 № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України»//Урядовий кур'єр від 22.03.2017. - № 54.

9. National Cyber Security Strategy for Montenegro 2013-2017.– [Електронний ресурс]// Електрон.дані. – 2013. – Режим доступу: <http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=165416&rType=2&file=Cyber+Security+Strategy+for+Montenegro.pdf>. – Назва з екрана. – Дата звернення: 13.04.2017р.

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

*Фурашев В. М., доцент кафедри
інформаційного права та права
інтелектуальної власності к.т.н., с.н.с.,
доцент ФСП КПІ ім. Ігоря Сікорського*

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ПРАВА НА ОБ'ЄКТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УМОВАХ КІБЕРБЕЗПЕКИ

*Спочатку тезисно розглянемо **сутність** деяких загальноприйнятих та загальновживаних термінів.*

Власність це – все те, що належить фізичній або юридичній особі, суспільству, державі відповідно до визначених норм і правил поведінки та взаємостосунків (суспільних відносин), які встановлені у даному суспільстві, даній державі та, за необхідністю, визнані іншими суспільствами, державами.

Право на власність – офіційно визнаний показник відповідності визначеним нормам і правилам поведінки та взаємостосунків (суспільних відносин), які встановлені у даному суспільстві, даній державі та, за необхідністю, іншими суспільствами, державами.

Об'єкт інтелектуальної власності – результат (продукт) творчого (розумового) труда, незалежно від стадії його завершеності, якій не має офіційно встановлених аналогів.

Право власності на об'єкт інтелектуальної власності - офіційно визнаний показник відповідності визначеним нормам і правилам поведінки, в т.ч. й морально-етичним, та взаємостосунків (суспільних відносин), які встановлені у даному суспільстві, даній державі та, за необхідністю, іншими суспільствами, державами. Право на інтелектуальну власність може належати окремим фізичним та юридичним особам, групам фізичних осіб та державі.

Інформаційний простір це – сфера обороту інформації та сукупності суб'єктів і об'єктів забезпечення функціонування цього обороту.

Умовно інформаційний простір можна розподілити на наступні види: індивідуальний (персональний, особистий); колективний (груповий); національний; глобальний.

Природно що всі перелічені види інформаційного простору, тій чи іншою мірою, є складовими глобального інформаційного простору та базуються, більшою мірою, використанні об'єктів забезпечення функціонування обороту інформації, які притаманні саме глобальному інформаційному простору.

Глобальний інформаційний простір це - сфера обороту інформації, яка не має національних, державних, особистністних та інших кордонів та сукупності функціонально пов'язаних національних та міждержавних суб'єктів і об'єктів забезпечення функціонування цього обороту на визначених умовах та правилах.

Глобальний інформаційний простір, у більшості, є наслідком фінансово-економічної глобалізації. Саме цілі та завдання фінансово-економічної глобалізації надали поштовх на прискорення еволюційного розвитку процесу науково-технічного прогресу

Далі розглянемо, також тезисно, **наслідки** вказаних вище процесів та процедур.

Процес глобалізації інформаційного простору «породив» не лише «позитив», а й «негатив», дуже велику кількість проблемних питань, в тому числі й у сфері визначення права на об'єкт інтелектуальної власності, які людство лише починає усвідомлювати.

Глобалізація інформаційного простору, а точніше, об'єкти забезпечення функціонування обороту інформації в цьому просторі, стала «матір'ю» таких процесів і явищ як «кіберзлочинність», «кібертероризм» та ін., що можна об'єднати під одним терміном – «кібернебезпека». В першу чергу, це відноситься до програмно-інструментальних та телекомунікаційних об'єктів забезпечення функціонування обороту інформації в сучасному інформаційному просторі. Також необхідно не забувати про принципи максимально вільної доступності до інформації, причому суттєво розширеного масиву інформації – майже безмежного, свободи слова та розповсюдження інформації та інші демократичні принципи.

Вільний доступ до різноманітної інформації, розвинуті сервіси пошуку, накопичення та обробки інформації, полегшили та спростували процес привласнення «чужого» - *плагіату*.

Сучасний стан програмно-інструментальних та телекомунікаційних засобів та тенденції їх розвитку і вдосконалення забезпечення обороту інформації в глобальному інформаційному просторі забезпечили можливість несанкціонованого віддаленого доступу до конкретного робочого місця, з метою зняття, знищення або спотворення інформації, незалежно від форми її представлення.

Наведене та багато іншого не могли не відобразитися на процесах визначення (ідентифікації) суб'єктів права на інтелектуальну власність, причому у далеко на кращому ракурсі.

Щодо оцінки сучасного стану охорони та захисту прав інтелектуальної власності.

Навіть поверховий аналіз чинного законодавства України показує, що питання нормативно-правової охорони прав інтелектуальної власності вирішується досить задовільно. Нажаль, подібної оцінки неможливо надати вирішенню питань забезпечення безпеки прав інтелектуальної власності.

Майже всі зловживання крім, плагіату, у сфері створення (формування) об'єкту права інтелектуальної власності з використанням сучасних програмно-інструментальних та телекомунікаційних засобів зводяться до кіберзлочинності, а точніше – до несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, або до несанкціонованого збуту, або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, або до несанкціонованих дій 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.

Щодо захисту від плагіату – однозначної оцінки дати неможливо.

Плагіат, як дія щодо привласнення результату (продукту) творчого (розумового) труда, незалежно від стадії його завершеності є, скоріш за все, об'єктом не лише правового регулювання, а й, що ближче до природи цієї дії, об'єктом морально-етичного виховання, морально-етичної поведінки.

Плагіат може бути як відвертим, явним, так й прихованим.

З явним плагіатом ще можна боротися шляхом встановлення факту привласнення або спроби привласнення за допомогою інформаційних та програмно-інструментальних засобів.

Зовсім інша ситуація з встановленням прихованого плагіату. Об'єкт інтелектуальної власності має дві нерозривні складові – внутрішню, сутнісну, нематеріальну (задум, думки, бачення, уявлення та ін.) та зовнішню, матеріальну (креслення, документація, ноти, рукописи, дослідні зразки та ін.). Проблема полягає у тому, що, з визначеною мірою достовірності, за допомогою сучасних інформаційних та програмно-інструментальних засобів можна встановити факт наявності плагіату, навіть у випадку часткової зміни зовнішньої складової об'єкту інтелектуальної власності.

Але як бути з визначенням факту плагіату внутрішньої складової об'єкту інтелектуальної власності? Корегування зовнішньої складової не завжди відображається адекватним корегування внутрішньої, самій головний, складовій об'єкту інтелектуальної власності.

Ситуація ускладнюється і у зв'язку зі стрімкими темпами “роботизації” з елементами штучного інтелекту, які так само стрімко перетворюються на повноцінний штучний інтелект. Тоді вже постане питання визначення не лише встановлення наявності або відсутності плагіату, а питання визначення суб'єктності на право власності щодо об'єкту інтелектуальної власності.

Підведемо деякі підсумки:

1. Глобальний інформаційний простір досить суттєво ускладнює процес створення об'єкту інтелектуальної власності та визначення права власності на нього.

2. Вже сьогодні, а не завтра, процеси створення об'єкту інтелектуальної власності та їх впровадження повинні супроводжуватися юристами – спеціалістами з інформаційного права та права інтелектуальної власності. Мало знати загальні структури та положення нормативно-правових актів в інформаційної сфері та сфері права інтелектуальної власності. Потрібно, у визначеній сфері діяльності, досконально знати ці

положення – “диявол ховається в деталях”. На жаль, розуміння цього поки що не спостерігається, що нагадує відношення роботодавців та суспільства в цілому до спеціалістів у сфері ІТ-технологій наприкінці ХХ-го – початку ХХІ сторіччя.

3. Сутність поняття “інтелектуальна власність”, суспільні відносини у цій сфері з розвитком науково-технічного прогресу неминуче будуть піддаватися визначеній, не виключно – кардинальній трансформації.

4. Сам хід науково-технічного прогресу, його темпи і масштаби об’єктивно висувають правову науку, як регулятора суспільних відносин, в перші ряди. Правова наука, особливо у галузях інформаційного права і права інтелектуальної власності, із спостерігача за формуванням суспільних відносин та визначенням моменту їх правового регулювання повинна, разом з “двигунами” науково-технічного прогресу, перетворитися в активного творця цих суспільних відносин, стати одним з цих рівноправних “двигунів”.

На завершення: природно, що наведене не є аксіомою Навпаки, коли дані міркування стануть предметом дискусій, автор буде тільки радий.

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

*Андрощук Г. О., головний науковий
співробітник НДІ інтелектуальної
власності НАПрН України, к.е.н.,
доцент.*

КІБЕРБЕЗПЕКА: ТЕНДЕНЦІЇ В СВІТІ ТА УКРАЇНІ

Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз міжнародній та національній та безпеці. Поряд із інцидентами ненавмисного походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет.

Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Згідно даних Центру стратегічних і міжнародних досліджень (CSIS) США світова економіка втрачає до 445 млн доларів на рік через злочини в мережі. Останні роки кіберзлочинність переживає бурхливе зростання, страждають торгівля, конкурентоспроможність та інновації. За найскромнішими підрахунками, збитки оцінюється в 375 млн. доларів, а за найсміливішими - в 575 млн. Найбільші втрати несуть найбільші економіки світу - США, Китай, Японія і Німеччина. Експерти оцінюють їх збитки в 200 млн доларів щорічно. Втрати, пов'язані з витоками персональних даних, як, наприклад, крадіжки даних кредитних карт, складають 150 млн доларів [1].

Кібервтручання здійснюються не лише з меркантильною метою, але й з метою викрадення державної таємниці іншої країни. Так, за даними ФБР, КНР на сьогодні має армію у 180 тис. хакерів, які займаються щоденними атаками на кібермережі США. Тільки в 2009 році ними здійснено 90 тис. атак проти комп'ютерів Міністерства оборони США. З 180 тис. хакерів 30 тис. є військовими, а 150 тис. – комп'ютерними експертами з приватного сектору, місією яких є отримання доступу до військових та комерційних секретів США та внесення розладу до урядових та фінансових служб [2].

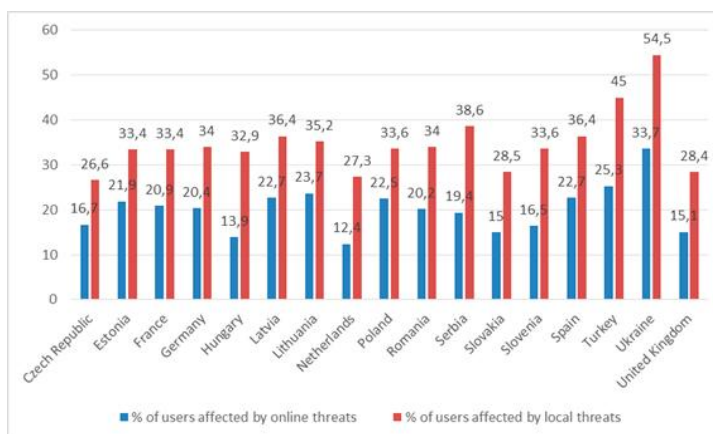
У глобальних протистояннях у кіберпросторі, й передусім у відстеженні та подальшому аналізі кібератак, величезну роль відіграють різноманітні приватні безпекові організації, які часто поєднують свою основну діяльність з виробництвом антивірусних продуктів. Серед таких компаній відзначимо McAfee, Avast, Kaspersky Lab, ESET, F-Secure та ін. Саме вони завдяки більшій свободі у своїй діяльності все частіше стають викривальниками масштабних кібероперацій, у т.ч. таких, як Stuxnet, Flame, Red Octobr. В Україні організацій подібного масштабу немає, а чи не єдиний антивірус національного виробництва (Zillya!) лише намагається увійти на цей ринок.

Нещодавно в Будапешті (Угорщина) відбувся форум з кібербезпеки, організований Kaspersky Lab. Європейські експерти обговорили тенденції галузі, дали поради щодо захисту свого бізнесу і особистого життя, а також охарактеризували ситуацію по країнах. Україна стала лідером за внутрішніми та зовнішніми кіберзагрозами в Європі. За останні роки наша країна неодноразово ставала мішенню не тільки для дрібних шахраїв, але й для масштабних кібероперацій. Майбутнє готує ще більше викликів. Експерти прогнозують, що повністю зміниться структура кібероперацій і методи їх проведення. Вони стануть більш непомітними для систем виявлення і фаєрволів. Мотивом атак буде не стільки демонстрація хакерської потуги, скільки повернення інвестицій для держав-замовників. У перспективі сфера кібершпигунства поповниться новими учасниками. Чим більший попит, тим більше пропозиція. Експерти очікують, що такі послуги будуть доступні всім, хто здатний їх оплатити. У мережі зацікавленим особам продаватимуть доступ до конфіденційної інформації високопоставлених жертв. Так з'явиться AaaS - або Access-as-a-Service. Під загрозою будуть також приватні особи. Очікується, що значно зросте кількість троянських програм, які атакують банківські акаунти користувачів. Їх поширення прогнозують на раніше не схильних до загроз платформах, зокрема на пристроях з OS X або IoT-платформах. Кіберзлочинці шукають нові способи викрадення коштів. Слід очікувати, що сучасні платіжні системи на кшталт Apple Pay і Android Pay також стануть мішенями фінансових кібератак. Поточна ситуація в Україні не вселяє оптимізму. Експерти Kaspersky Lab сформулювали перелік загроз, які роблять нашу країну однією з головних «гарячих точок» на кіберкарті світу. Вісім тез про кібербезпеку в Україні.

1. Українські користувачі значною мірою схильні до заражень через неоновлення програмного забезпечення і піратські копії програм. Показово також, що 17% всіх заражень припадає на користувачів, що працюють із застарілою операційною системою Windows XP.

2. Нерідко спамери для розсилки «нігерійських листів» спекулюють на темі політичної ситуації в Україні або ж розсилають листи від імені «російських наречених»: дівчат з Росії і України, які скаржаться на свою нелегку долю і просять перевести на їх рахунки деяку суму.

3. Україна, зокрема, посіла п'яте місце в світі (і перше в Європі) за ризиками зіткнення з веб-загрозами в 2015 році. За даними, Kaspersky Security Network третину (33,7%) українських користувачів мережі зіткнулися із загрозами, що розповсюджуються через інтернет.



4. Україна займає третю сходинку рейтингу країн з найбільшим ризиком зараження через інтернет: 35,7% користувачів зіткнулися з веб-загрозами за звітний період.

5. Україна опинилася на 9 сходинці рейтингу країн з найбільшим ризиком зараження мобільними зловредами (8,39%). Досить високий і ризик зіткнення з локальними загрозами (54,5%). Сюди потрапляють об'єкти, які проникли на комп'ютери шляхом зараження файлів або знімних носіїв або спочатку потрапили на комп'ютер не у відкритому вигляді (наприклад, програми в складі складних інсталяторів, зашифровані файли і т.п.). За цим показником країна займає передостанню сходинку в топ-20 у світі, але перше в Європі.

6. В Україні відзначено велику кількість спрацьовувань антивірусу на програми-вимагачі і шифрувальники - шкідливі програми, мета яких - заблокувати пристрій або браузер, чи зашифрувати файли користувача,

зробивши їх недоступними без спеціального ключа, за який потрібно заплатити викуп.

7. Серед жертв Turla - однієї з найскладніших кібершпигунських кампаній, яка діє вже більше 8 років, виявлені комп'ютери українських чиновників. Угруповання, що стоїть за Turla, заразила сотні комп'ютерів більш ніж в 45 країнах світу, які належать, зокрема, державним установам, посольствам, військовим, дослідницьким центрам і фармацевтичним компаніям. Метою кіберзлочинців є збір необхідних або конфіденційних даних з комп'ютера жертви.

8. Українці також були серед жертв таких кампаній, як CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy,

В Україні нині відсутня цілісна термінологічна система, що сформувала би єдиний термінологічний апарат у сфері кібербезпеки: „кібербезпека”, „кібератака”, „кіберпростір” тощо [3]. Необхідно змінити ситуацію у цій сфері, адже в Стратегії національної безпеки України, затвердженої Указом Президента 26 травня 2015 року, роз'яснюються загрози кібербезпеці і безпеці інформаційних ресурсів України, даються рекомендації стосовно заходів забезпечення кібербезпеки і безпеки інформаційних ресурсів.

Указом Президента України введено в дію Рішення Ради національної безпеки і оборони "Про Стратегію кібербезпеки України" від 27 січня 2016 року. Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України.

Забезпечення кібербезпеки України, як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах: верховенства права і поваги до прав та свобод людини і громадянина; забезпечення національних інтересів України; відкритості, доступності, стабільності та захищеності кіберпростору; державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам; пріоритетності запобіжних заходів; невідворотності покарання за вчинення кіберзлочинів; пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях; забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [4].

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Список використаних джерел:

1. Хакеры ежегодно выкачивают из мировой экономики полмиллиарда долларов [Електронний ресурс]. – Режим доступу: <http://kr.ua/life/457249-khakery-ezhehodno-vykachyvauit-yz-myrovoi-ekonomyky-polmyllyarda-dollarov>

2. Андрощук Г.О. Інформаційно-комунікаційні технології (ІКТ) в Україні: стан та перспективи розвитку // Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України : матеріали парлам. слухань у Верховній Раді України 3 лютого 2016 р. / Верховна Рада України, Комітет з питань інформатизації та зв'язку. - К. : Парлам. вид-во, 2016, - С. 202-250.

3. Дубов Д. "Сучасні тренди кібербезпекової політики: висновки для України". Аналітична записка. [Електронний ресурс] – Режим доступу: <http://www.niss.gov.ua/articles/294/>

4. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/96/2016>

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

УДК 351.746.1+004.9: 340.13(043.2)

Довгань О. Д., д.ю.н., с.н.с., Науково-дослідний інститут інформатики і права Національної академії правових наук України.

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Питання необхідності створення цілісної та узгодженої системи забезпечення інформаційного суверенітету, управління ризиками і можливостями новітніх викликів у інформаційній сфері, розбудови власних спроможностей надійних та достовірних державних комунікацій та створення тісної взаємодії між органами влади, формування інфраструктури національного інформаційного простору з метою створення умов для його інтегрування у світовий інформаційний простір, налагодження комунікаційного процесу між органами влади та споживачами інформації та інше в сучасних умовах залишаються актуальними, а питання кібербезпеки, у

т.ч. її правового забезпечення, у нашій державі має надзвичайно велике значення.

Розпочнемо дещо з незвичного. Останнім часом тематика заходу є привабливою. Звернемо увагу на проблематику ряду публікацій: *Кібербезпека в Україні: У 2015 році наша країна - «найгарячіша» точка Європи; Киберфронт в Украине: иллюзия спокойствия; Гібридна війна – хто наступний?; 52 млрд. втратили світові компанії у результаті кібератак; Росія в 2016 році здійснила тисячі кібератак на Україну (Полторак); Для ефективного забезпечення кібербезпеки важливі як знання, так і обладнання»; Укроборонпром розпочав підготовку до створення єдиного центру кібербезпеки та ін.*

І таких публікацій не те, що десятки, а більше сотні. Про що це говорить. Звичайно про актуальність питань, які є предметом сьогодишнього нашого форуму.

Тому, питання забезпечення кібербезпеки нині є надзвичайно важливим для України. Оскільки, застосування країною-агресором по відношенню до України технологій гібридної війни, в першу чергу в інформаційній сфері, сформувало нові виклики та загрози інформаційній безпеці держави. Кібернетичні атаки на інформаційні ресурси держави стали невід'ємним компонентом такої гібридної війни. В таких умовах актуальними на сьогодні залишаються питання необхідності створення цілісної та узгодженої загальнодержавної системи кібербезпеки.

За нашими оцінками, така система перебуває на етапі формування, а заходи з протидії викликам і загрозам у цій сфері знаходяться на початковому етапі та не мають комплексного характеру. *Що ми маємо в правовому полі.*

Візьмемо період з 2014 року, після «Революції гідності», анексії Криму, окупації окремих районів Донецької та Луганської областей. За цей період на державному рівні прийнято ряд нормативно-правових актів: Указ Президента України № 449/2014 від 1 червня 2014 р., яким уведено в дію рішення Ради

національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Вказаним документом, серед іншого, передбачено (передбачалося) приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України тощо.

Прийнята Стратегія національної безпеки України (травень 2015р.) визначила загрози кібербезпеці і безпеці інформаційних ресурсів та безпеці критичної інфраструктури. При цьому до пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів Стратегією віднесено: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трестового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Якщо детально розглянути ці пріоритети, то видно, що фактично був визначений реальний дороговказ, що потрібно робити.

З набуттям чинності Стратегії кібербезпеки України (*січень 2016 року*) наша країна підтвердила наміри у напрямі розбудови національної системи кібербезпеки. На державному рівні задекларовано, що пріоритетами й напрямками забезпечення кібербезпеки в сучасних умовах є: розвиток безпечного, стабільного та надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів і критичної інформаційної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; боротьба з кіберзлочинністю тощо.

Далі було ухвалено низку доктринальних документів і підзаконних нормативно-правових актів, серед яких *Концепція розвитку сектору безпеки і оборони України*, затверджена Указом Президента України від 14.03.16 р. № 92/2016 (визначає, що одним із основних завдань сектору безпеки і оборони є забезпечення інформаційної та кібербезпеки, створення національної системи кібербезпеки з використанням можливостей суб'єктів сектору безпеки і оборони для ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, розвитку мережі реагування на комп'ютерні надзвичайні події (CERT)), *Стратегічний оборонний бюлетень*, уведений в дію Указом Президента України від 06.06.16 р. № 240, *Положення про Національний координаційний центр кібербезпеки*, затверджене Указом Президента України від 07.06.16 р. № 242/2016, *Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави*, затверджений постановою Кабінету Міністрів України від 23.08.16 р. № 563. Указами Президента України від 16 січня №8/2017 уведено в дію рішення РНБО України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» та від 13 лютого 2017 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

На виконання Стратегії кібербезпеки України розпорядженням Кабінету Міністрів України від 24.06.16 р. № 440-р було затверджено план заходів на 2016 рік з реалізації зазначеної Стратегії. Крім цього, цілий розділ

4.4. Річної національної програми «Україна - НАТО» присвячено кібербезпеці.

Все це є підтвердженням важливості питань, що стосуються кібербезпеки. А зазначені акти по суті вказують на поштовх (мабуть черговий) до розгортання національної системи забезпечення кібербезпеки.

Окремо потрібно говорити про проект Закону України *«Про основні засади забезпечення кібербезпеки України»*, який було прийнято Верховною Радою України за основу у вересні 2016 р. Проте, зазначений проект далекий від досконалого, на що справедливо було звернуто увагу науковцями. Нещодавно стало відомо, що вже існує доопрацьований проект для другого читання та прийняття в цілому. Нажаль замало залучають науковий світ до обговорення та проведення наукової експертної оцінки законопроектів.

На наше переконання, прийняття цілого ряду нормативних-правових актів, у т.ч. стратегії кібербезпеки і подальше схвалення закону про кібербезпеку має не просто убезпечити країну та захистити її від ряду нових загроз, але і переформатувати роботу спецслужб і інших державних органів. Звичайно, це стане можливим за наявності політичної волі та комплексного бачення майбутнього розвитку країни. Простого виходу із такої ситуації не має. Рішення повинно бути комплексним і комбінованим. Питання кібербезпеки – це питання виживання країни і можливості її розвитку. Час стискається, світ змінюється і, якщо не вжити потрібні заходи сьогодні, через декілька років ми не в змозі наздогнати ці процеси.

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

*Кодинець А. О., д.ю.н., доцент кафедри
інформаційного права та права
інтелектуальної власності ФСП КПП
ім. Ігоря Сікорського.*

ПРАВОВІ ЗАСАДИ РЕФОРМУВАННЯ ЗАКОНОДАВСТВА У СФЕРІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Реалізація інноваційної моделі розвитку України не можлива створення сучасної системи нормативного регулювання відносин у сфері охорони результатів інтелектуальної, яка б забезпечувала надійний захист прав суб'єктів творчої діяльності (авторів, виконавців, винахідників), гарантувала їх додержання їх прав, охорону від можливих правопорушень.

Перші кроки в удосконаленні правоохоронного механізму у галузі використання результатів інтелектуальної, творчої діяльності були закладені прийнятим у 2003 р. Цивільним кодексом України (надалі – ЦК України), який не лише значно розширив сферу права інтелектуальної власності, але і суттєво збагатив його змістовне наповнення. У ЦК України [1] відносини у сфері інтелектуальної власності вперше були зафіксовані в окремій структурній частині (книзі 4 «Право інтелектуальної власності»), що свідчить про їх важливість для приватного права.

Подальше удосконалення нормативного регулювання відносин у галузі охорони результатів творчої діяльності передбачає деталізацію положень Цивільного кодексу на рівні законів, підзаконних правових актів, створення надійних механізмів реалізації і захисту прав їх суб'єктів. Необхідним є також приведення існуючого нормативного матеріалу у відповідність до концепції і загальних підходів, визначених ЦК України з врахуванням положень Угоди про асоціацію [2], укладеною між Україною та Європейським Союзом, глава 9 якої (ст.ст. 157-252) містить вимоги та стандарти щодо охорони що стосуються прав інтелектуальної власності

Розпорядженням Кабінету Міністрів України від 1 червня 2016 р. № 402-р була схвалена Концепція реформування державної системи правової

охорони інтелектуальної власності в Україні, згідно якої основними напрямками реалізації Концепції є:

запровадження прозорої дворівневої структури державної системи правової охорони інтелектуальної власності, за якої Мінекономрозвитку забезпечує формування та реалізацію державної політики у сфері інтелектуальної власності, а національний орган інтелектуальної власності виконує окремі публічні функції (владні повноваження) з реалізації державної політики у зазначеній сфері;

реорганізація системи колективного управління майновими авторськими та суміжними правами;

удосконалення національного законодавства та його гармонізація до законодавства ЄС.

Постановою КМ України від 23 серпня 2016 р. № 585 було ліквідовано Державну службу інтелектуальної власності, завдання і функції з реалізації державної політики у сфері інтелектуальної власності було покладено на поклавши на Міністерство економічного розвитку і торгівлі

Удосконалення національного законодавства та його гармонізація із законодавством ЄС здійснюватиметься шляхом:

виконання плану імплементації Угоди про асоціацію;

внесення змін до законодавства щодо:

- правової охорони об'єктів авторського права та суміжних прав, винаходів, корисних моделей, промислових зразків, комерційних позначень (торговельних марок, географічних зазначень, фірмових найменувань) з урахуванням досвіду держав ЄС;

- порядку розподілу прав на об'єкти інтелектуальної власності, створені у зв'язку з виконанням трудового договору, договору за замовленням, за рахунок коштів державного бюджету;

- захисту прав інтелектуальної власності, в тому числі щодо захисту авторського права та суміжних прав в Інтернеті;

- відповідальності за порушення прав інтелектуальної власності (зміни до Кримінального кодексу України та Кодексу України про адміністративні правопорушення).

Так, повертаючись до першого з основних напрямів реформи, дворівнева структура передбачає, насамперед, ліквідацію ДСІВ та створення на базі ДП «Український інститут інтелектуальної власності» нового національного органу інтелектуальної власності. Найцікавіше те, що до повноважень цього органу пропонується віднести ті повноваження, які сьогодні здійснює ДСІВ, а також ті, які здійснює ДП «Український інститут інтелектуальної власності».

Чи не найбільше вражають визначені міністерством та Кабміном строки реалізації концепції реформування: 2016 – I квартал 2017 року. Враховуючи, що вона передбачає вдосконалення національного законодавства, а також беручи до уваги те, як проблематично в Україні проходять процедури ліквідації та створення державних органів такі строки видаються досить оптимістичними.

У будь-якому випадку, ДСІВ продовжуватиме здійснювати повноваження та функції з реалізації державної політики у сфері інтелектуальної власності до набрання чинності актом Кабінету Міністрів України щодо можливості забезпечення здійснення зазначених повноважень та функцій Міністерством економічного розвитку і торгівлі.

Аналізуючи зміни, що відбулися у галузі цивільного законодавства, що регулює відносини інтелектуальної власності, можна зробити висновок, що фактично починаючи з 2003 р. - дати прийняття Цивільного кодексу України -, вітчизняне законодавство про інтелектуальну власність не було змінено. ЦК України так і не став тим поштовхом, який би забезпечив оновлення відповідної законодавчої бази, а багато його норм (деякі з яких носять справді новаторський характер) так і не отримали своєї конкретизації на рівні спеціальних законів та підзаконних правових актів.

Наведемо декілька прикладів. Стаття 429 ЦК України регламентує відносини щодо розподілу майнових прав інтелектуальної власності на об'єкти створені на підставі трудового договору – майнові права на такі об'єкти належать спільно роботодавцеві та працівникові, що створив такі об'єкти, якщо інше не встановлено трудовим договором.

Спеціальні закони про інтелектуальну власність (ст. 16 Закону України «Про авторське право і суміжні права», ст. 9 Закону України «Про охорону прав на винаходи і корисні моделі») містять норми, що виключне майнове право на службовий твір чи службовий винахід належить роботодавцю, якщо інше не передбачено трудовим договором (контрактом) та (або) цивільно-правовим договором між автором і роботодавцем. Подібна правова норма міститься також ст. 8 Закону України «Про охорону прав на промислові зразки».

У зв'язку з наведеним, виникає питання який правовий документ слід застосовувати: пізніше прийнятий ЦК України, що містить загальну норму, яка вказує про спільність прав роботодавця і працівника на службовий об'єкт інтелектуальної власності чи раніше прийняті спеціальні закони, які свідчать про належність даних прав роботодавцю? Відповідь на нього міститься у самому ЦК України, ст. 4, якого зазначає, що ЦК України є основним актом цивільного законодавства України, а інші закони України мають прийматися відповідно до Конституції України та Кодексу, тобто, до відносин, пов'язаних з розподілом прав на службові твори застосовується положення ст. 429 ЦК України. Але безумовно, законодавець мав би усунути зазначену колізію.

Залишився також нерозв'язаним комплекс питань, пов'язаних з створенням таких службових результатів творчої діяльності. А саме, яка природа такого договору; чи має право працівник у зв'язку з створенням цих об'єктів на одержання додаткової винагороди, крім своєї заробітної плати; в якій формі має бути оформлене доручення роботодавця щодо створення таких службових об'єктів (у вигляді умови трудового договору, наказу,

посадової інструкції, службового завдання тощо); яким чином має бути ідентифікований такий об'єкт інтелектуальної власності в таких наказах чи умовах договору. Законодавство про інтелектуальну власність має більш детально врегулювати зазначені суспільні відносини, пов'язані із створенням службових результатів інтелектуальної діяльності та надати відповіді на поставлені питання.

Подібна ситуація має місце і стосовно регламентації відносин щодо реєстрації договорів у сфері інтелектуальної власності. Друга частина статті 1114 ЦК України містить положення, що факт передання виключних майнових прав інтелектуальної власності, які відповідно до ЦК України або іншого закону є чинними після їх державної реєстрації, підлягає державній реєстрації. Враховуючи, що права на об'єкти патентного права, komponування інтегральної мікросхеми та торговельні марки набувають чинності з моменту їх реєстрації, то договір про передання майнових прав на такі об'єкти є чинним з моменту його державної реєстрації.

Однак, спеціальне законодавство містить інші вимоги до державної реєстрації договорів про передачу прав на об'єкти промислової власності, встановлюючи факультативність подібної реєстрації. Беручи до уваги, що ЦК України є основним актом цивільного законодавства (ч.2 ст. 4), то його норми мають пріоритет над положеннями спеціальних законодавчих актів, а тому застосовується підхід, визначений у ЦК України.

Залишилися також чинними положення Закону України «Про охорону прав на винаходи і корисні моделі», що стосуються деклараційного патенту на винахід та деклараційного патенту на корисні моделі, хоча зазначені патенти вже протягом тривалого часу не видаються в Україні. Наразі патент на винахід видається за результатами кваліфікаційної експертизи, а тому він не може бути деклараційним, а патент на корисну модель, який видається в результаті проведення формальної експертизи, який хоча він і не має назву деклараційний, але по суті таким являється, оскільки кваліфікаційна експертиза корисних моделей під час їх патентування не проводиться.

Норми ЦК України подекуди також далекі від досконалості, а законодавче викладення окремих положень норм кодексу не сприяє однозначному їх застосуванню. Найбільш курйозною у цьому аспекті є норма ст. 488 ЦК України, яка стосується правовому регулюванню строків чинності майнових прав інтелектуальної власності на сорти рослин та породи тварин, частина четверта цієї статті повністю, дослівно, співпадає з частиною шостою.

Прикладом іншої невдалої норми у ЦК України, що стосується інтелектуальної власності є положення ч. 3 ст. 1122 ЦК України, яка містить наступне формулювання: «умова договору, відповідно до якої користувач має право продавати товари (виконувати роботи, надавати послуги) виключно певній категорії покупців (замовників) або виключно покупцям (замовникам), які мають місцезнаходження (місце проживання) на території, визначеній у договорі». При фіксації цієї норми законодавець, мабуть забув записати основну кінцеву фразу – «є нікчесною». Лише за такого розуміння положення ч. 3 ст. 1122 набуває юридичного сенсу. Проте незважаючи на десятиліття, що сплинуло після набрання чинності Цивільного кодексу України законодавець так і не спромігся усунути ці недоліки та технічні помилки із його тексту.

Якщо закріплення цих положень кодексу ще можна пояснити технічними описками, то окремі норми ЦК України фактично суперечать одна одній чи взагалі не можуть застосовуватися на практиці. Так, стаття 478 ЦК України передбачає можливість відновлення достроково припинених майнових прав інтелектуальної власності на компонування інтегральної мікросхеми. З цією метою особа, якій належать дані права подає заяву у встановленому законом порядку. Проте чинний Закон України “Про охорону прав на топографії інтегральних мікросхем” не містить правових положень, що стосуються підстав та процедури відновлення чинності прав інтелектуальної власності на топографію інтегральної мікросхеми (далі - ІМС). Відсутність законодавчо встановленого порядку відновлення чинності

майнових прав інтелектуальної власності на компонування ІМС унеможливорює застосування цієї норми.

Існує також колізія між положенням ст. 430 ЦК України та ст. 1112 ЦК України. Згідно ст. 430 ЦК України майнові права інтелектуальної власності на об'єкт, створений за замовленням належать спільно творцеві цього об'єкта та замовникові, якщо інше не встановлено договором. Із формулювання зазначеної норми чітко не зрозуміло про який договір замовлення йде мова в цій статті. Про договір підряду, що передбачає передачу результату замовникові, але за договором підряду права інтелектуальної власності замовникові не передаються. Можливо, йде мова про договір про створення за замовленням і використання об'єкта інтелектуальної власності (ст. 1112 ЦК України), але такий договір має містити положення щодо способів та умов використання об'єкта інтелектуальної власності замовником. На жаль чинне законодавство не містить конкретизації цієї правової норми, а отже актуальною залишається колізія між формулюванням ч. 2 ст. 430 ЦК України та ч. 2 та 3 ст. 1112 ЦК України, тому єдине, що можна рекомендувати сторонами договору про створення об'єкта інтелектуальної власності на замовлення – це чітко фіксувати положення про розподіл майнових прав інтелектуальної власності на створений об'єкт.

Недоліки чинного законодавства щодо регулювання відносини у сфері розпорядження майновими правами інтелектуальної власності відобразилися на практиці. Наведемо декілька найбільш конфліктних ситуацій.

По-перше, Глава 75 ЦК України поряд з ліцензійним договором в якості самостійної договірної моделі виділяє ліцензію на використання об'єкта інтелектуальної власності. В юридичній літературі як приклад таких ліцензій наводяться правочини щодо комп'ютерних програм. Як правило, йде мова про погодження користувача з умовами ліцензії під час установки (інсталяції) програми на своєму комп'ютері. Хоча, якщо проаналізувати зміст таких договорів, слід відзначити, що вони спрямовані не на надання прав інтелектуальної власності – ці права залишаються за виробником

комп'ютерної програми - власнику носія надається можливість використовувати програми шляхом її встановленні на власному комп'ютері. Але це право і так йому надане у силу договору купівлі-продажу матеріального носія комп'ютерної програми та положень чинного законодавства. Тобто, по суті, права інтелектуальної власності не надаються особі, яка придбала носій програми. Вони залишаються у виробника – розробника комп'ютерної програми.

Згідно положень ст. 1107 ЦК України ліцензія як інші договори щодо розпорядження майновими правами інтелектуальної власності мають бути укладені письмово. Згідно ст. 207 ЦК правочин вважається таким, що вчиненим у письмовій формі, якщо його зміст зафіксований в одному чи кількох документах, якими обмінялися сторони. Правочин вважається таким, що вчинений у письмовій формі, якщо він підписаний його стороною (сторонами). Ліцензію на використання комп'ютерної програми при її інсталяції, зміст якої відображений в електронній формі не підписує ні виробник, ні користувач програмного забезпечення. Користувач шляхом вчинення конклюдентних дій (як правило, у вигляді натискання відповідних кнопок) погоджується з умовами ліцензії і ініціює процес установки програмного забезпечення. Тому така ліцензія не має з позиції ЦК України юридичного значення та є нікчемною.

По-друге, Закон України “Про авторське право і суміжні права” виділяє такі види авторського договору як авторський договір про передачу виключного права на використання твору та авторський договір про передачу невиключного права на використання твору. Однак, Закон дає визначення виключного права лише як майнового права особи щодо твору, виконання, фоно та відеограми та іншого об'єкту суміжних прав. З положень Закону можна зробити попередній висновок, що оскільки виключне право – це майнове право, то невиключне – це особисте немайнове право інтелектуальної власності. Однак, загальновідомо, що особисті немайнові права – не можуть бути відчужені на підставі договору, це суперечить

конструкції такого права як немайнового блага, що є невід’ємним від особи та позбавлене економічного змісту.

Лише на підставі системного тлумачення Закону у його порівнянні з ЦК України можна визначити, що авторський договір про передачу невиключного права – це договір про надання невиключного дозволу на використання творів чи об’єктів суміжних прав, оскільки договірною формою відчуження (передачі прав) інтелектуальної власності твір є авторський договір про відчуження авторських прав. Тобто, за авторським договором про передачу невиключного права здійснюється надання майнових авторських прав на умовах невиключного дозволу (ліцензії), іншими словами, права не передаються (не відчужується) правонабувач лише отримує дозвіл на їх використання у межах встановлених умовами цього договору. Однак, існування такої термінології у Законі може вводити в оману осіб, які не є фахівцями в сфері інтелектуальної власності.

По-третє, ч. 3 ст. 436 ЦК України містить положення щодо договору про співавторство. А саме, “відносини між співавторами можуть бути визначені договором. У разі відсутності такого договору авторське право на твір здійснюється всіма співавторами спільно”. Подібне положення закріплюється ст. 13 Закону “Про авторське право і суміжні право”. Проте законодавство не визначає природу цього договору, його співвідношення з договорами щодо розпоряджання правами інтелектуальної власності, регламентовані Главою 75 ЦК України, форму укладання, істотні умови тощо, хоча на практиці твори досить часто створюються у співавторстві. Вбачається, що такий договір має ознаки як договорів про спільну діяльність у сфері інтелектуальної власності. За цим договором співавтори зобов’язуються здійснювати спільну творчу діяльність по написанню твору, визначають строки виконання своїх зобов’язань по створенню твору в цілому та його окремих частин, характер та обсяг їх діяльності, регламентують умови про розподіл винагороди та можуть визначити свого представника для представництва перед третіми особами (видавництвом, редакцією тощо).

Проте у законодавстві необхідне більш детальне правове регулювання договірних відносин у сфері співавторства.

Підводячи підсумок розгляду окремих колізій законодавства, що регулює сферу інтелектуальної діяльності, можна констатувати, що зазначені недоліки регламентації суспільних відносин є наслідком суперечності положень спеціальних законів про інтелектуальну власність та норм ЦК України, а також незбалансованості окремих положень самого ЦК України, зокрема, книги 4 кодексу і глав 75 та 76 кодексу, які присвячені договірним зобов'язанням у сфері інтелектуальної, творчої діяльності.

Недоліки чинного законодавства щодо регулювання відносин у сфері інтелектуальної власності негативно впливають на практику та зумовлюються відсутністю стійких наукових підходів до правової охорони результатів творчої діяльності. Хоча науковці та юристи-практики неодноразово звертали уваги на потребу оновлення законодавства у сфері інтелектуальної власності. Вирішення зазначених проблем законодавчого регулювання сфери інтелектуальної власності є перспективним завданням вітчизняної правової системи, яке, однак, потребує свого нагального розв'язання.

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

Dr. Małgorzata Dziewanowska
Zakład Kryminologii
Instytut Prawa Karnego
Wydział Prawa i Administracji
Uniwersytet Warszawski.

INTERNETOWY WIGILANTYZM – ZAGROŻENIE CZY SZANSA DLA SPOŁECZEŃSTWA GLOBALNEGO?

Celem wystąpienia jest zaprezentowanie fenomenu internetowego jakim stał się w ostatnich latach „human flesh search engine”, nazywany również internetowym wigilantyzmem (Internet vigilantism). To zjawisko, wywodzące się z Chin, polega na wykorzystywaniu stron internetowych do piętnowania zachowań ludzkich, zdobywania drogą nieformalną personalnych informacji, czy wreszcie

wymierzania swoistej sprawiedliwości w sytuacji gdy instytucje państwowe nie podejmują żadnych, wymaganych przez społeczność internetową, działań. Jest to wyjątkowa forma jednoczenia się ludzi niekiedy z całego świata przeciwko jednostkom, których zachowanie w ocenie społecznej (lub ocenie danej społeczności internetowej) jest naganne, ale jednocześnie naruszające prawo tych jednostek do ochrony danych osobowych, do prywatności, niekiedy prowadzące do ostracyzmu, w sytuacjach skrajnych skutkujące samobójstwem ofiar tych działań.

Jednocześnie niektóre działania stanowią pewne uzupełnienie niekiedy niewydolnych systemów ścigania sprawców przestępstw, mobilizując tysiące ludzi w celu ujawnienia danych osobowych przestępców, czy zidentyfikowania miejsca przestępstwa. Na podstawie tak zebranych informacji dochodzi niekiedy do skazania sprawcy. W ramach tego zagadnienia mieszczą się również działania grupy hakerów (anonymous) mające na celu likwidowanie stron z pornografią dziecięcą oraz demaskowanie konkretnych osób z nich korzystających.

W dobie monitoringu wizyjnego, dostępu do Internetu przy pomocy tabletów i innych urządzeń, a także rosnących możliwości nagrywania obrazu i dźwięku przy pomocy aparatów telefonicznych i udostępniania ich na stronach internetowych, należy mieć świadomość, iż nasze zachowanie może podlegać stałej obserwacji. Przykłady internetowego wigilantyzmu jasno ukazują, jak silna jest korelacja między opinią na forum a faktycznym działaniem.

W przypadku takich zjawisk należy zastanowić się czy stanowią one zagrożenie dla prywatności jednostki, czy może są szansą na wymierzanie sprawiedliwości większej liczbie sprawców oraz na włączenie społeczeństwa w działania na rzecz zachowania porządku i ochrony „moralności”. A może jest to powrót do klasycznych samosądów, lub realizacja założeń kryminologicznej teorii abolicjonistycznej Nielsa Christie, który postuluje oddanie konfliktu w ręce stron? Czy stanowią one zagrożenie dla państwa, czy będą jego podporą?

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

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

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ДЕЯКИХ СКЛАДОВИХ ІНФОРМАЦІЙНОЇ СФЕРИ ДЕРЖАВИ

В той час, коли наука розглядає інформаційну сферу різносторонньо і достатньо активно, то практика вкрай специфічно - лише під певним політичним кутом.

Цьому є просте пояснення - надто популярними у політиків є заклики до розвитку інформаційної складової держави, інноваційної діяльності та її складової інтелектуальної власності. Адже якісно нове знання виступає потужним, і майже невичерпним нематеріальним активом на відміну від застарілого виробництва епохи індустріалізації.

Тобто практика і наука йдуть своїми шляхами.

Беззаперечним є те, що розвиток інформаційної сфери — це важливий напрям державної політики, безсумнівний пріоритет стратегічного курсу розвитку України. Від здатності держави розробити та реалізувати ефективну інформаційну доктрину, політику, концепцію та стратегію значною мірою залежить її майбутнє існування.

Інформаційна сфера, зокрема інформаційні ресурси, за сучасних умов стають системоутворювальним фактором життя і діяльності суспільства й держави. Розвиток інформаційної сфери все більше впливає на політичну, економічну, соціокультурну, оборонну, інші складові розвитку суспільства й держави, забезпечення національної безпеки в сучасних умовах.

Інформаційні ресурси є важливим не тільки стратегічним, але й тактичним об'єктом (особливо це стосується державних структур), який неможливо не враховувати при прийнятті рішень у всіх сферах державного управління. Рівень розвитку інформаційного середовища є одними з найвагоміших факторів у всіх сферах національної безпеки.

Тобто, обов'язковою складовою успішних реформ в Україні є розвиток її інтелектуального потенціалу.

Можна констатувати, що інформаційна сфера поступово стає вирішальним чинником розвитку окремо взятої сучасної країни та людського суспільства в цілому.

Аналітики визначають ряд основних положень які дозволяють використовувати інформаційний продукт у військових цілях: інформаційні ресурси повинні охоронятися з тим же ступенем обережності, що і ядерна зброя; спрямовані інформаційні операції не несуть екологічного збитку, тому можуть бути використані раніше ядерної зброї; інформаційні операції можуть бути спрямовані на руйнування політико-економічної системи; інформаційні операції можуть вести до деградації національної свідомості; інформаційні операції можуть приводити нації до невиправданих висновків і рішень; інформаційні операції і технології істотно підсилюють військову ефективність звичайних систем зброї тощо.

Ефект цільового інформаційного впливу на противника порівнюється з застосуванням засобів масового ураження і загроза піддатися такому впливу може стати важливим фактором стримування потенційного агресора.

Небезпека для країн з невисоким рівнем розвитку полягає в тому, що, відставши від економічно сильних держав, ліквідувати розрив, що утворився, стає практично неможливо. Тому вплив на економіку і політичний лад такої країни досягатиметься відключенням її від інформаційного обміну, що дешевше і простіше, ніж воєнні дії.

А як же розвивається у даному напрямку Україна? Частково, відповідь на це питання ми надамо далі.

Наведемо для демонстрації вказаного лише фрагментарно наступне.

18 жовтня 2014 р. на порталі ВР України опубліковано проект рекомендацій слухань у Комітеті Верховної Ради України з питань науки і освіти «Інтелектуальна власність в Україні. Стан та концептуальні засади розвитку».

Учасники слухань звертають увагу на у цілому незадовільний стан розвитку сфери інтелектуальної власності та черговий раз надають рекомендації Верховній Раді України, Кабінету Міністрів, Верховному Суду України, вищим спеціалізованим судам України та Комітету Верховної Ради України з питань науки і освіти з питань покращення стану правовідносин у сфері інтелектуальної власності. Безперечно, що останні так і залишаються рекомендаціями без відповідного контролю за їх виконанням¹.

Додатково до невиконаних раніше стратегічно важливих державних завдань, розпорядженням КМ України від 4 червня 2015 р. № 575-р затверджено «План заходів з реалізації Концепції реформування державної політики в інноваційній сфері на 2015—2019 роки»², яким знову, черговий раз відпрацьований план заходів без механізму їх контролю і відповідальності за невиконання.

Зазначені проблеми обговорюються в Україні вже не перший раз³.

Реалізуючи прийняті Верховною Радою України засади зовнішньої і внутрішньої політики та стан виконання законів України та постанов Верховної Ради України щодо наукової та науково-технічної політики України, **учасники парламентських слухань на тему: «Про стан та законодавче забезпечення розвитку науки та науково-технічної сфери держави», що відбулися 2 липня 2014 року,** знову виказали низку рекомендацій Президенту України, Верховній Раді України, Комітету Верховної Ради України з питань науки і освіти, Кабінету Міністрів України, безпосередньо Міністерству фінансів України, Міністерству освіти і науки

¹ <http://sips.gov.ua/ua/news.html? m=publications& t=rec&id=2797>

² Розпорядження КМ України від 4 червня 2015 р. № 575-р. «План заходів з реалізації Концепції реформування державної політики в інноваційній сфері на 2015—2019 роки.

³ Постанова Верховної Ради України від 20 червня 2007 року «Про Рекомендації парламентських слухань на тему: «Національна інноваційна система України: проблеми формування та реалізації» (Відомості Верховної Ради України (ВВР), 2007, N 46, ст. 525); Постанова Верховної Ради України від 21 жовтня 2010 року «Про Рекомендації парламентських слухань на тему: "Стратегія інноваційного розвитку України на 2010-2020 роки в умовах глобалізаційних викликів" (Відомості Верховної Ради України (ВВР), 2011, N 11, ст. 72).

України, Міністерству освіти і науки України та Міністерству фінансів України, Міністерству освіти і науки України та Національній академії педагогічних наук України, Міністерству аграрної політики та продовольства України та Національній академії аграрних наук України, Міністерству охорони здоров'я України та Національній академії медичних наук України, Міністерству соціальної політики України⁴.

Тому, вважається, що зазначена сфера державної діяльності вимагає негайного реформування шляхом систематизації норм права з чіткого визначення компетенції державних органів та організацій з питань інноваційної, науково-технічної діяльності та трансферу технологій.

Відповідно до викладеного вище, держава почала у 2016 році здійснювати певні організаційні та управлінські заходи з метою удосконалення охорони та захисту об'єктів інтелектуальної власності, про що свідчить зміст **Розпорядження Кабінету Міністрів України «Про затвердження плану пріоритетних дій Уряду на 2016 рік» та Розпорядження Кабінету Міністрів України № 418-р «Про затвердження плану пріоритетних дій Уряду на 2016 рік»**недоліками яких є їх «заземленість» на вкрай вузьких, суто прикладних питаннях сьогодення, вирішення яких не дає можливості ефективно, саме за змістом, а не формою реформувати систему охорони та захисту інтелектуальної власності України⁵.

На виконання **Розпорядження Кабінету Міністрів України від 1 червня 2016 р. № 402-р «Про схвалення Концепції реформування державної системи правової охорони інтелектуальної власності в Україні»** Міністерству економічного розвитку і торгівлі разом із зацікавленими центральними органами виконавчої влади необхідно

⁴ Постанова Верховної Ради України від 11 лютого 2015 року «Про стан та законодавче забезпечення розвитку науки та науково-технічної сфери держави» (Відомості Верховної Ради (ВВР), 2015, № 16, ст. 117).

⁵ Розпорядження Кабінету Міністрів України від 27 травня 2016 р. № 418-р «Про затвердження плану пріоритетних дій Уряду на 2016 рік».

розробити та подати у місячний строк Кабінетові Міністрів України план заходів з реалізації Концепції⁶, яка розроблена відповідно до Програми діяльності Кабінету Міністрів України, схваленої **постановою Верховної Ради України від 14 квітня 2016 р. № 1099-VIII**, та на виконання пункту 174 плану дій Кабінету Міністрів України на 2016 рік, затвердженого розпорядженням Кабінету Міністрів України від 16 березня 2016 р. № 184 (Офіційний вісник України, 2016 р., № 24, ст. 961).

Надалі, **Розпорядження Кабінету Міністрів України від 27 травня 2016 р. № 418-р «Про затвердження плану пріоритетних дій Уряду на 2016 рік»** визначає напрями розвитку інновацій, реформування державної системи охорони інтелектуальної власності та аудит і реформування науково-інформаційної системи України.

Але навіть і таке реформування до цього часу не відбулося. Останнє видно із відповіді керівництва Мінекономрозвитку України автору⁷.

Постанова Верховної Ради України «Про Рекомендації парламентських слухань на тему: "Обороздатність України у XXI столітті: виклики, загрози та шляхи їх подолання"»⁸ з урахуванням викликів і загроз національній безпеці держави, її обороноздатності у нинішньому столітті у найкоротший строк вимагає забезпечити вирішення широкого ряду стратегічних питань, які перераховувати наразі недоцільно, тим більше коментувати результати її реалізації.

⁶ Розпорядження Кабінету Міністрів України від 1 червня 2016 р. № 402-р «Про схвалення Концепції реформування державної системи правової охорони інтелектуальної власності в Україні».

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

⁸ Постанова Верховної Ради України від 12 серпня 2014 року № 1639-VII «Про Рекомендації парламентських слухань на тему: "Обороздатність України у XXI столітті: виклики, загрози та шляхи їх подолання"»

Указ Президента України № 92/2016 «Про рішення Ради національної безпеки і оборони України "Про Концепцію розвитку сектору безпеки і оборони України"» метою Концепції визначає одним з основних завдань сектору безпеки і оборони захист інформації з обмеженим доступом та забезпечення інформаційної та кібербезпеки⁹.

Указ Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"»її метою визначає створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави¹⁰.

Указ Президента України № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"»її метою визначає уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни¹¹. Здається, що цього для Доктрини замало.

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"»констатує, що комплекс проблем у сфері забезпечення кібербезпеки (без її визначення) та її кризовий стан загрожує національній безпеці (остання також має ознаки примарності і розпливчастості)¹².

⁹Указ Президента України № 92/2016 «Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України"».

¹⁰ Указ Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"».

¹¹ Указ Президента України № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"».

¹² 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"».

Розпорядженням Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» визначені основні заходи з її реалізації¹³.

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» також передбачає ряд стратегічно важливих завдань з реформування державної політики в інноваційній сфері на 2015—2019 роки¹⁴. Аналізувати їх виконання адекватним буде через два роки, хоча...

Після аналізу викладеного матеріалу є можливість зробити ряд висновків:

1. інформаційна сфера діяльності держави, складається у першу чергу не з пропагандистської діяльності, а включає до своєї структури ще велику кількість складових, які мають бути визначені законодавчо;
2. удосконалення інформаційної галузі має бути науково-обґрунтованим не окремими вченими, а колективами фахівців під проводом Верховної Ради;
3. удосконалення інформаційної сфери має завершитися кодифікацією норм права, які її регулюють;
4. з метою забезпечення та надійного захисту об'єктів інформаційної сфери достатньо належним чином і своєчасно розробити політику інформаційної безпеки й запровадити процес моніторингу її дотримання.
5. Останнє, неможливе без політичної волі керівництва України, яке має забезпечити відповідне завданню організаційне (в першу чергу),

¹³ Розпорядження Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України».

¹⁴ 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».

контрольне (по друге) та матеріально-технічне забезпечення вказаної діяльності.

6. Однак, самим першим кроком має стати перевірка якості виконання вже прийнятих державними органами рішень, а не прийняття нових нормативно-правових актів, яких уже й так достатня кількість.

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

*Солончук І. В., старший викладач
кафедри інформаційного права та
права інтелектуальної власності ФСП
КПІ ім. Ігоря Сікорського.*

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Кіберпростір є невід’ємним атрибутом життєдіяльності сучасного суспільства – інформаційного суспільства. В кіберпросторі сучасні люди знайомляться, спілкуються, обмінюються інформацією, знаходять однодумців, висловлюють власні позиції з конкретних проблем, купують та відчужують речі матеріального світу, подають електронні заяви та здійснюють багато інших функцій, знайомих фактично кожному. Сьогодні нікого вже не дивують поняття «електронна черга», «електронна пошта», «електронний уряд», і навіть відбуваються обговорення запровадження «електронного суду». Але, поряд із вагомими перевагами, кіберпростір містить велику кількість загроз як для окремої особи, так і для загального інформаційного суспільства та держави, про що зазначають такі провідні науковці як Фурашев В. М., Баранов О. А. та ін. Тому завданням держави на сучасному етапі розвитку інформаційних відносин є впровадження дієвого правового регулювання забезпечення кібербезпеки як мінімум на трьох рівнях: кібербезпеки держави, кібербезпеки суспільства, кібербезпеки особи. Для України вирішення зазначеної проблеми має власні аспекти, зумовлені агресією Російської Федерації.

Метою даного дослідження є огляд та аналіз положень основних нормативно-правових актів, які регулюють забезпечення кібербезпеки, щодо повноти визначення поняття кібербезпеки та переліку загроз для неї..

Стратегія кібербезпеки України (далі – Стратегія) затверджена рішенням Ради національної безпеки і оборони України від 27 січня 2016 року [1]. Даний нормативний документ базується на положеннях Конвенції про кіберзлочинність [2] та Стратегії національної безпеки України [3]. Стратегія містить розуміння кібербезпеки як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [1]. Серед сучасних загроз кібербезпеці України називаються:

- кібератаки, вмотивовані інтересами окремих держав, груп та осіб;
- незаконне збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжки та шахрайства у мережі Інтернет (кіберзлочинність).

Для порівняння, Національна програма кібербезпеки Республіки Молдова на 2016-2020 роки визначає кібербезпеку як нормальний стан, що виник внаслідок застосування комплексу проактивних и реактивних заходів, якими забезпечується конфіденційність, цілісність, доступність, достовірність та неможливість відмови в доступі до інформації в електронному форматі, інформаційних систем і ресурсів, державних та приватних послуг в кіберпросторі. Проактивні та реактивні заходи охоплюють політики, концепції, стандарти та інструкції з безпеки, управління ризиками, діяльність з підготовки та інформування, запровадження технічних рішень щодо захисту кібернетичної інфраструктури та ін. [6].

Доктрина інформаційної безпеки України, затверджена рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року, містить

поняття «національні інтереси України в інформаційній сфері», до яких відносить:

— життєво важливі інтереси особи, зокрема: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, на захист приватного життя, а також захищеність від руйнівних інформаційно-психологічних впливів;

— життєво важливі інтереси суспільства і держави, зокрема: захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації; забезпечення вільного обігу інформації, крім випадків, передбачених законом; збереження і примноження духовних, культурних і моральних цінностей Українського народу; розвиток медіа-культури суспільства та соціально відповідального медіа-середовища; створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди; розвиток інформаційного суспільства та інші, визначені розділом 3 Доктрини [4].

Проаналізувавши нормативно-правові акти України, які регулюють забезпечення кібербезпеки, можемо зробити висновок, що сьогодні в нашій державі немає чинного закону як акту вищої юридичної сили, який би регулював забезпечення кібербезпеки та, принаймні, визначив єдину концепцію державної політики в цій сфері. Принагідно слід зазначити, що Верховною Радою України прийнято в першому читанні 20 вересня 2016 року Проект Закону «Про основні засади забезпечення кібербезпеки України», в якому запропоноване визначення кібербезпеки як захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [5]. Визначається достатньо широкий спектр об'єктів кібербезпеки, зокрема: людина та громадянин; конституційні права і

свободи людини та громадянина; суспільство; сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава; конституційний лад держави; державний суверенітет; територіальна цілісність і недоторканість держави; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави.

На нашу думку, зважаючи на неоднозначне нормативне трактування поняття, об'єктів та загроз кібербезпеки, враховуючи відсутність в Україні закону щодо засад забезпечення кібербезпеки, дане питання потребує додаткового наукового обговорення.

Список використаних джерел:

1. Указ Президент України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"; Стратегія від 15.03.2016 № 96/2016: [Електронний ресурс] – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/96/2016>.

2. Конвенція про кіберзлочинність: Рада Європи; Конвенція, Міжнародний документ від 23.11.2001: [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575.

3. Указ Президент України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України", Стратегія від 26.05.2015 № 287/2015: [Електронний ресурс] – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/287/2015/paran14#n14>.

4. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Доктрина від 25.02.2017 № 47/2017: [Електронний ресурс] – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/47/2017>.

5. Проект Закону про основні засади забезпечення кібербезпеки України: [Електронний ресурс] – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2126%D0%B0&skl=9

6. Постановление Правительства Республики Молдова «О Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы»: Постановление Nr. 811 от 29.10.2015: - [Электронный ресурс] – Режим доступа: <http://lex.justice.md/index.php?action=view&view=doc>

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

Гуцалюк М. В., с.н.с. Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України, к.ю.н., доцент.

АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

В Україні, яка активно інтегрується в європейське інформаційне суспільство, значна увага приділяється питанням кібербезпеки, без забезпечення якої неможливе функціонування інформаційних систем як державних установ, так і приватних структур. Важливість забезпечення належного рівня кібербезпеки та протидії кіберзлочинності, у тому числі організованих, зумовлена зокрема тисячами кібератак [1], які в останні роки спрямовані на інформаційні ресурси України, включаючи об'єкти критичної інфраструктури.

З урахуванням нових викликів та загроз в умовах гібридної війни Указом Президента України від 26 травня 2015 року № 287/2015 затверджено Стратегію національної безпеки України, в якій визначені такі пріоритети забезпечення кібербезпеки в державі, як: розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, захист державних інформаційних ресурсів з урахуванням практики держав-членів НАТО та ЄС [2].

Активного реформування зазнає сектор кібербезпеки після затвердження Указом Президента України від 15 березня 2016 року № 96/2016 Стратегії кібербезпеки України, в якій зокрема визначено: чинники, через дію яких актуалізуються загрози кібербезпеці України; суб'єкти забезпечення кібербезпеки в Україні та сфери їх відповідальності; пріоритетні напрями забезпечення кібербезпеки, серед яких зокрема створення вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізація нормативних документів, організація кібербезпеки відповідно до

міжнародних стандартів, а також наголошено на необхідності боротьби з кіберзлочинністю.

Європейські країни активно підтримують Україну в реформуванні її безпекового сектору. Це передусім стосується Республіки Польща, яка проводить заходи з підготовки кадрів, а також розробці практичних рекомендацій, зокрема щодо створення системи кіберзахисту об'єктів критичної інфраструктури. Налагоджуються відносини з такими організаціями як Європол та Євроюст.

Разом з тим, на сьогодні на законодавчому рівні ще не визначені такі терміни, як: кіберпростір, кіберзлочин, кібератака, електронний доказ, об'єкт критичної інфраструктури та ін., що зумовлює певні проблеми в практичній діяльності правоохоронних органів, органів прокуратури та судів.

Надзвичайно актуальним є питання вдосконалення системи збору, аналізу та оцінки електронних (цифрових) доказів у правозастосовній діяльності. Адже відсутність чіткого законодавчого закріплення цього поняття, видів та джерел таких доказів призводить до зниження рівня розкриття окремих злочинів та невизнання їх у суді.

На відміну від традиційних видів доказів, електронні набагато легше змінити чи підробити, що створює для правоохоронних органів додаткові труднощі, адже потрібно дотримуватися таких правил поведінки з ними, які дають змогу забезпечити допустимість доказів. Крім того, однією з особливостей кіберзлочинів є відсутність державних кордонів при їх вчиненні, а тому для їх розслідування необхідною умовою є міжнародне співробітництво у цій сфері.

Як відомо, Україна є учасником Конвенції про кіберзлочинність (Convention on Cybercrime – далі Конвенція), яка підписана 23 листопада 2001 року в м. Будапешті і ратифікована із застереженнями і заявами Законом України від 07 вересня 2005 року № 2824-IV.

Відповідно до положень частини 2 Конвенції, кожна сторона повинна вжити законодавчих та інших заходів, які необхідні для

впровадження процедур збору доказів в електронній формі по кримінальних правопорушеннях та імплементації таких статей Конвенції:

- стаття 16 – Термінове збереження комп'ютерних даних, які зберігаються;
- стаття 17 – Термінове збереження і часткове розкриття даних про рух інформації;
- стаття 19 – Обшук і арешт комп'ютерних даних, які зберігаються;
- стаття 20 – Збирання даних про рух інформації у реальному масштабі часу;
- стаття 21 – Перехоплення даних змісту інформації.

У чинному Кримінальному процесуальному кодексі України лише в ст. 99 вказано про те, що до документів, за умови наявності в них відомостей, передбачених частиною першою цієї статті, можуть належати у тому числі електронні носії інформації.

Європейські експерти рекомендують прямо вказати, що джерела доказів в електронному вигляді можуть міститися в таких пристроях, як комп'ютери та їх периферійне обладнання, комп'ютерні мережі, мобільні телефони, цифрові камери, а також отримані з глобальної мережі Інтернет.

Також особливої уваги потребують процедури, необхідні для забезпечення цілісності даних, для того щоб у сторін судового розгляду не виникало сумнівів щодо їх модифікації.

Не в повному обсязі вирішені на законодавчому рівні питання щодо збереження електронних доказів Інтернет-провайдерами, адже для забезпечення запитів правоохоронних органів, кількість яких, як показує практика європейських країн, буде постійно збільшуватися, необхідне не тільки спеціалізоване обладнання, але й додаткове кадрове забезпечення відповідних структур.

Вирішення зазначених питань надасть змогу більш продуктивно використати всі переваги інформаційного суспільства та зміцнити довіру до правоохоронних органів та судів як громадян, так і приватного сектора.

Список використаних джерел:

1. Полторак: Росія здійснила сім тисяч кібератак [Електронний ресурс]. Режим доступу: <http://ua.korrespondent.net/ukraine/3835687-poltorak-rosiia-zdiisnyla-sim-tysiach-kiberatak>
2. DR Mykhaylo Gutsalyuk Ukraine's Cybersecurity strategy and ways to implement it // European Cybersecurity journal. – Volume 2 (2016). The Kosciuszko Institute. Poland. – P. 65-69.
3. Закон України від 07 вересня 2005 року «Про ратифікацію Конвенції про кіберзлочинність» № 2824-IV (2824-15) [Електронний ресурс]. Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2824-15>

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

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

**КІБЕРБЕЗПЕКА ЄВРОПЕЙСЬКОГО СОЮЗУ:
ПРОБЛЕМАТИКА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ**

Розвиток інформаційно-комунікаційних технологій і, як наслідок, поступовий рух до глобального інформаційного суспільства відкривають колосальні можливості для розвитку і добробуту. Проте, цей процес має й зворотний бік, що супроводжується новими і серйозними загрозами та наслідками.

Не залишилась поза увагою ця проблема і в Європейському Союзі. Характерні для початкового періоду розвитку спорадичність та епізодичність, з часом були змінені на стійкі та тривалі відносини, які виокремили питання інформаційної безпеки, боротьби із кіберзлочинністю в самостійну область соціальних і регіональних відносин. Наслідком стало формування спеціальних норм, покликаних регулювати відносини з інформаційної безпеки в ЄС. У зв'язку з цим вартими розгляду є питання розвитку правового регулювання протягом чотирьох періодів, зокрема 1980–1998 рр., 1999–2004 рр., 2005–2008 рр. і сучасного періоду 2009–2017-х років.

Розвиток правового регулювання інформаційної безпеки ЄС протягом першого періоду 1980–1998 років пов’язаний із кількома факторами, що безпосередньо на нього вплинули. Вони полягають у такому:

по-перше, загальне бачення майбутнього міжнародно-правового регулювання інформаційних відносин, пов’язаних із впровадженням нових цифрових технологій, було сформовано низкою міжнародних організацій протягом другої половини 70-х років - кінця 90-х років ХХ ст. і позитивно сприймалося ЄС у контексті загального розвитку міжнародних відносин;

по-друге, впровадження автоматизованих баз даних, розвиток інформаційних та телекомунікаційних мереж, вільне переміщення осіб, транскордонна передача та обмін даними викликали потребу у захисті приватного життя індивідуальних свобод людини;

по-третьє, правові питання, пов’язані у цей період з інформаційною безпекою, переважно розглядалися з позицій захисту загальновизнаних прав людини і базувалися на основних міжнародно-правових актах. Проте поширення і різноманітність злочинів, пов’язаних із використанням нових цифрових технологій у 80–90-і роки ХХ ст., а також необхідність попередження злочинності та створення кримінального правосуддя у боротьбі із високотехнологічною та комп’ютерною злочинністю, викликали потребу розробці нових нормативних актів;

по-четверте, переважна більшість норм щодо питань інформаційної безпеки містилася у резолюціях міжнародних органів та організацій, у спільних заявах, деклараціях, комюніке (нормах soft law «м’якого права»);

по-п’яте, складність та чисельність питань інформаційної безпеки, призвела до концептуального бачення майбутнього міжнародно-правового регулювання виключно на рівні, який спрямований на вирішення кримінальних аспектів, пов’язаних із використанням інформаційно-комунікаційних технологій.

Все це поступово сформувало загальне бачення розвитку інформаційної безпеки з урахуванням європейських потреб.

Розвиток співробітництва в політичній, соціально-економічній, науково-технічній, правоохоронній сферах передбачав, крім іншого, ще й вільний рух інформації. Тому один із найважливіших напрямів інформаційного співробітництва країн ЄС ґрунтувався на використанні комп'ютерних технологій з метою збору, зберігання і обміну між державами-членами необхідної інформації, результатом чого стало створення як єдиних інформаційних систем та комп'ютеризованих баз даних, призначених для спільного користування органами різних держав Європейського Союзу, так і баз даних і мереж, що належали приватним фінансовим, комерційним та іншим установам.

Як приклад єдиних інформаційних систем і баз даних, які були створені у той час для спільного користування держав — членів ЄС, *стали інформаційні системи універсального призначення* (Шенгенська інформаційна система, Інформаційна система Європолу) та *інформаційні системи спеціального призначення* (Інформаційна система митних органів, Європейська система зберігання зображень дійсних та справжніх документів).

Крім того, в цей період, у рамках ЄС було створено кілька спеціальних інформаційних мереж, зокрема *Європейська інформаційна мережа з питань расизму та ксенофобії* (*Réseau européen d'Information sur la racisme et la xénophobie* — *Raxen*), *Європейська інформаційна мережа в області правосуддя* (*Réseau judiciaire européen*), *Європейська інформаційна мережа із попередження злочинності* (*Réseau européen de prevention de la criminalité*). Варто зазначити, що були створені й інші інформаційні системи і мережі - у банківській, страховій, фінансовій, транспортній, пенсійній та іншій сферах.

Директиви ЄС сприйняли напрацьований ОЕСР і Радою Європи позитивний досвід у питанні захисту персональних даних і деталізували його.

Варто зазначити, що прийняття Директиви 95/46/ЄС від 24 жовтня 1995 р. «*Про захист осіб у зв'язку з обробкою персональних даних та вільним*

обігом цих даних» було необхідним і важливим кроком у напрямку гармонізації законодавства.

Директива 97/66/ЄС Європейського парламенту та Ради від 15 грудня 1997 р. *«Про обробку персональних даних і захист права на невтручання в особисте життя осіб у телекомунікаційному секторі»* була прийнята в умовах, коли в ЄС широко почали використовуватися передові цифрові технології та надаватися нові телекомунікаційні послуги.

Разом з тим варто наголосити, що проблеми інформаційної безпеки на той період вже не обмежувалися виключно захистом персональних даних і потребували комплексного підходу. Нагальною потребою поставала боротьба із комп'ютерними злочинами, про міжнародний характер яких було зазначено ще у 1976 (!) р. Коло правових питань, пов'язаних із використанням Інтернету, потребувало від ЄС окремого комплексного підходу, що і було розпочато на наступному етапі.

Початок другого періоду, 1999–2004 роки, пов'язують з прийняттям Європейським парламентом і Радою від 25 січня 1999 р. № 276/1999/ЄС *Рішення про багаторічний план дій Співтовариства зі сприяння безпечному використанню Інтернету шляхом боротьби із незаконним і шкідливим змістом у глобальних мережах*. Програма Плану дій «Безпечний Інтернет», розрахована на період 1999–2004 років, мала на меті сприяти безпечному користуванню Інтернетом і формувати сприятливе середовище для розвитку європейської Інтернет-індустрії.

У той період головна увага законодавця була зосереджена на кількох важливих питаннях, а саме: пошук правових заходів створення безпечного європейського інформаційного суспільства; розробка єдиної правової термінології в галузі інформаційних відносин; визначення основних груп комп'ютерних злочинів і боротьба з ними.

Набули пріоритетного значення питання щодо розробки загальних правових засад формування безпечного інформаційного середовища, саморегулювання і прийняття кодексу поведінки у глобальних мережах;

обмеження поширення інформації певного змісту (інформації, що містить дитячу порнографію, заклики до проявів расизму і ксенофобії); питання міжнародного співробітництва з питань інформаційної безпеки ЄС.

З'явилося і спільне бачення проблем правової термінології. Термінологічна система з питань інформаційної безпеки почала відповідати загальному рівню розвитку інформаційних відносин і враховувала пропозиції низки міжнародних організацій.

Досить вагомий внесок у розуміння проблем інформаційної безпеки вносила Європейська Комісія. Її зусилля спрямовувалися на аналіз і вивчення проблеми кіберзлочинності і визначення ефективних заходів для боротьби із загрозою забезпечення цілісності, доступності і надійності інформаційних систем і мереж. Низка законодавчих ініціатив була викладена в опублікованих у 2001 р. повідомленнях «Створення безпечного інформаційного суспільства, підвищення безпеки інформаційних інфраструктур і боротьба з комп'ютерною злочинністю» і «Мережа та інформаційна безпека».

У результаті реалізації Плану дій «Безпечний Інтернет» та інших програм, прийнятих у цей період («Електронна Європа», «План дій по Інтернету», «Технології інформаційного суспільства») постали й інші правові питання, які вимагали свого рішення. Організаційно-правові заходи потребували створення інфраструктури проти високотехнологічної комп'ютерної злочинності, захисту проти атак на інформаційні системи, захисту дітей та неповнолітніх від небажаної інформації, захисту від некорисних комерційних повідомлень («спам»), захисту критичної інфраструктури у боротьбі проти тероризму.

Необхідність вирішення цих питань потребувала створення договірного та інституційного механізмів у боротьбі із кібернетичними злочинами, що власне і почало відбуватися у цей період. Крім того, значний вплив на розвиток законодавства ЄС здійснили кілька конвенцій з питань інформаційної безпеки, розроблених Радою Європи, і ратифікованих

переважною більшістю держав ЄС. Однією з перших, 24 січня 2001 р., була прийнята *Європейська Конвенція про правовий захист послуг, що надаються на основі обумовленого доступу, або які полягають у наданні обумовленого доступу*. Конвенція має на меті заборонити на території держав-учасниць певні види діяльності, що дозволяють здійснювати несанкціонований доступ до захищених послуг. При цьому положеннями Конвенції передбачається прийняття сторонами заходів щодо покладення на винних осіб кримінальної, адміністративної та іншої відповідальності.

Більш широкий спектр правопорушень було визначено Радою Європи у прийнятій 23 листопада 2001 р. *Конвенції «Про кіберзлочинність»*. На сьогодні Конвенція визнана важливим міжнародним інструментом у боротьбі із кіберзлочинністю і підтримана різними міжнародними організаціями. До цього варто додати те, що відповідно до положень Лісабонського договору, у ЄС з'явилася можливість стати членом Ради Європи і тому не виникло потреби у розробці дублюючих нормативних актів.

Прийняття Конвенцій стало поштовхом для розробки низки директив ЄС, спрямованих на формування нормативно-правової бази у сфері інформаційної безпеки. Перелік завдань, що були покладені на національні органи, згідно з *Директивою 2002/21/ЄС від 7 березня 2002 р. «Про загальну нормативно-правову базу для електронних комунікаційних мереж і послуг (Рамочна Директива)»*, містив: забезпечення високого рівня захисту персональних даних і конфіденційної інформації, цілісності і безпеки комунікаційних систем.

Директиви 2002/20/ЄС, 2002/22/ЄС, 2002/19/ЄС, 2002/58/ЄС від 7 березня 2002 р., а також Резолюція Ради від 18 лютого 2003 р. «Про реалізацію Плану дій “Електронна Європа 2005”» були спрямовані на досягнення цієї загальної мети.

Варто звернути увагу, що на цей період припадає проведення Женевського (першого) етапу Всесвітнього саміту на вищому рівні з проблем інформаційного суспільства 2003 р. У *Женевському плані дій*, прийнятому за

результатами саміту, наголошується на важливості проведення заходів у боротьбі з кіберзлочинністю. У подальшому це сприяло розробці спільної політики, цілей та принципів *Глобальної програми кібербезпеки Міжнародного Союзу Електрозв'язку*, які були позитивно сприйняті ЄС.

Як свій внесок у питання боротьби із кіберзлочинністю та з метою забезпечення високого й ефективного рівня інформаційної безпеки на регіональному рівні, 10 березня 2004 р. було створено *Європейське агентство з мережевої та інформаційної безпеки*. Головною метою утворення Агентства стало забезпечення належного, відповідного сучасним викликам рівня мережевої та інформаційної безпеки, підвищення потенціалу держав-учасниць і бізнес-співтовариства з профілактики і регулювання загроз безпеки інформаційним мережам, формування культури безпеки в інтересах громадян, споживачів, підприємств і організацій публічного сектора, допомагаючи планомірному функціонуванню внутрішнього ринку, а також сприяння підвищенню рівня поінформованості і доступності інформації з проблем інформаційної безпеки і бачення загального глобального підходу до проблем мережевої та інформаційної безпеки (ст. 2 Регламенту).

Третій період, 2005–2008 роки, розпочався з прийняття Європейським парламентом і Радою від 11 травня 2005 року № 854/2005/ЄС Рішення про запровадження багаторічної програми *Співтовариства зі сприяння безпечному використанню Інтернету і нових онлайн-технологій*.

Програма «Безпечний Інтернет Плюс» була розрахована на 2005–2008 роки. Ґрунтуючись на попередній, нова програма мала розширені завдання, спрямовані переважно на боротьбу із поширенням небажаної інформації та розробку спільної політики у боротьбі з кіберзлочинністю.

Питання щодо боротьби із поширенням небажаної інформації передбачало здійснення комплексу заходів спрямованих проти спаму, шпигунського та шкідливого програмного забезпечення. Було визнано, що спам є транскордонною проблемою і для боротьби з ним було прийнято цілу

низку ініціатив у галузі транскордонного співробітництва правоохоронних органів, зокрема створення Контактної мережі правоохоронних органів у боротьбі зі спамом, прийняття Лондонського плану дій (діяльністю правоохоронних органів у цьому напрямі було охоплено 20 країн і визначено процедури транскордонного співробітництва), і розширення співробітництва ЄС із США, КНР, Канадою і Японією. Фактично на цьому етапі продовжувалося забезпечення реалізації прийнятих ще у 2002 р. Директив «Про недоторканість приватного життя і електронних комунікацій» (вводила заборону на відправку спаму) та «Про недобросовісну комерційну діяльність» (захищала споживачів від агресивної комерційної практики).

Питання щодо розробки спільної політики у боротьбі з кіберзлочинністю передбачали налагодження оперативного співробітництва між правоохоронними органами та проведення спільних акцій з попередження і боротьби із великомасштабними атаками проти національних інформаційних структур; удосконалення методів протидії шахрайству і незаконній торгівлі в Інтернеті, у секторах, пов'язаних із безготівковими платіжними засобами в електронних мережах; боротьбою з незаконним змістом матеріалів у мережах, що спонукають до тероризму, сексуального насилля над дітьми, здатного спровокувати агресивну поведінку у неповнолітніх. Майбутніми напрямками співробітництва були визнані співпраця з третіми країнами з технічних методів боротьби з протизаконним змістом і процедурами ліквідації нелегальних сайтів та укладення угоди щодо блокування і закриття нелегальних сайтів.

Четвертий період 2009–2017 роки, передбачає реалізацію програми ЄС «Безпечний Інтернет 2009–2013 роки», — яку було розпочато відповідно до Рішення Європейського парламенту і Ради від 16 грудня 2008 р. № 1351/2008/ЕС *«Про встановлення багаторічної програми Співтовариства по захисту дітей, що користуються Інтернетом і іншими комунікаційними технологіями»*.

Метою програми є підвищення навичок і знань дітей при користуванні новими технологіями, а також ідентифікація ризиків використання нових технологій і посилення боротьби з ними. Програма спрямована на протидію незаконному і шкідливому змісту Інтернету, і реалізується шляхом підвищення інформованості дітей, батьків і вчителів; боротьбу з незаконною інформацією і згубною поведінкою; сприяння співробітництву на національному, європейському та міжнародному рівнях; створенню безпечного інформаційного середовища.

Підсумовуючи розгляд питань становлення і розвитку правового регулювання інформаційної безпеки в Європейському Союзі можна зазначити:

Законодавство ЄС у сфері інформаційної безпеки розвивалося у руслі міжнародних ініціатив Ради Європи, Організації економічного співробітництва і розвитку, Міжнародного Союзу Електрозв'язку, Організації Об'єднаних Націй.

Законодавчі заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програм Європейського Союзу — «Безпечний Інтернет» (1999–2004 рр.), «Безпечний Інтернет Плюс» (2005–2008 рр.), «Безпечний Інтернет 2009–2013 рр.», прийнятих рішеннями Європейського Парламенту і Ради, і переважно були спрямовані на захист персональних даних, сприяння безпечному користуванню Інтернетом, формуванню сприятливого середовища для розвитку європейської Інтернет-індустрії, захист дітей, що користуються Інтернетом і новими інформаційними технологіями.

Найважливіші заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програми Європейського Союзу «Попередження і боротьба із злочинністю» і передбачали співробітництво в протидії кіберзлочинності.

Складність та чисельність питань кібернетичної і інформаційної безпеки сформувала в законодавчих органах Європейського Союзу концептуальне бачення майбутнього міжнародно-правового регулювання виключно на рівні, спрямованому на вирішення кримінальних аспектів,

пов'язаних із використанням інформаційно-комунікаційних технологій. В Європейському Союзі не було сприйнято концепцію міжнародної інформаційної безпеки, яка передбачала б комплексне вирішення проблеми на трьох рівнях міжнародно-правового регулювання – військово-політичному, терористичному і кримінальному.

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

Каращук А., доцент кафедри іноземних мов, Інститут міжнародних відносин кийського національного університету імені Тараса Шевченка.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ У КІБЕРПРОСТОРІ

Тезисне викладення теми вимагає чіткого визначення розуміння автором основних понять, що містяться у назві теми.

Перше поняття – це інформація, або чи все, що ми бачимо на телебаченні, в Інтернеті та чуємо по радіо можливо вважати інформацією? Звісно ні, оскільки все що ми чуємо, бачимо складається з конотаційних інваріантів, які додаються до невеличкої частки інформації, шляхом дискурсивних технологій на різних рівнях. Тобто відображення в реальності частки дійсності і є інформацією, а інформаційна політика медіа, держави, офіційного дискурсу, якого дотримуються господарі медіа, переконання журналістів і таке інше, створюють конотативні, додані інваріанти, що формують **інформаційні продукти**, які ми бачимо в різних медіа. Важливо чітко зазначити, що у тому, що зазвичай називають інформацією інформації не більше одного відсотка, все інше – це те, що можливо порівняти зі спеціями та консервантами, продуктами, що мають тільки смакові (конотативні) властивості, що замінюють натуральний продукт (інформацію). Ці інформаційні продукти не мають на меті маніпулювати значеннями, вони маніпулюють на рівні чуттєвого сприйняття масами у чітко зазначених напрямках. Ці напрямки встановлюються на рівні побудови конотаційних

інваріантів інтерпретації невеличкої частини інформації, яка прихована нашаруваннями інформаційного продукту. Відповідно, коли автор говорить про інформаційну безпеку, або суверенітет він має на увазі саме забезпечення суверенітету тільки інформаційної складової усіх інформаційних продуктів, що містяться у різних медіа. Цей підхід водночас радикально зменшує потік інформаційних продуктів на контролі, та спрощує програмування медійної протидії.

Друге важливе поняття це конотаційні інваріанти. Інваріант—це те, у чого є варіант. Тобто, різноманітна варіація інформації з конотативною константою. Розробка варіантів та інваріантів і є медійним втіленням інформації з заданою конотацією. Навпаки, пошук конотаційних інваріантів є головним елементом деконструкції інформаційного продукту, головним інструментом пошуку інформації під нашаруваннями інформаційних продуктів. Відповідно, забезпечення інформаційного суверенітету може бути представлене у формі забезпечення просування інваріантів з заданою конотацією («своїх»), та збереження конотації власних інваріантів під час впливу на них з метою деконструкції, та навпаки деконструкції «ворожих» інваріантів та перепрограмування (зміни) конотацій «ворожих» інформаційних продуктів.

Як тільки ми говоримо про забезпечення суверенітету в медійному просторі необхідно визначити наступне поняття: «дискурс». Дискурс розуміється автором як тимчасове збереження конотації вузлової точки. Тобто, дискурс складається з вузлових точок, які як вузлики формують мережі (сітки) на різних рівнях дискурсивної безпеки. Сітки складаються з вузликів (вузлових точок), та з'єднань, які являють собою «елементи» та «моменти». Моменти— це фіксація значень шляхом поєднань вузлових точок одного шару, «елементи» це можливі фіксації значень вузлових точок на рівні конотації. Кількість вузлових точок визначається необхідністю та можливостями забезпечення контролю конотації вузлових точок мережі (сітки). Мережа має проекції на рівні реальних медіа за допомогою

інваріантів та варіантів, які формуються під конкретне завдання. Ця побудова дає змогу гнучкого нападу та всеохоплюючої відповіді на дискурсивну агресію. Іншими словами, вузлові точки – це опорні пункти, які дозволяють перекривати вогнем простір між собою, а також готувати багаторівневу оборону на критичних, та досягати стратегічної переваги на проривних напрямках.

Все те, що називається «інформаційними війнами» - такими бути не може, оскільки снарядами цих війн є інформаційні продукти, опорними пунктами є вузлові точки дискурсу. Тому це є дискурсивні війни, які ведуться за збереження конотації своїх точок та деконструкції конотації «ворожих» точок.

Чому конотація, а не значення? Оскільки дискурсивні війни ведуться на територіях міфологічної свідомості, то просувати інформацію немає сенсу.

Традиційно зміну артикуляції вузлової точки, що веде до зміни конотації, подають як основний метод ведення дискурсивних війн, однак за останні роки з'явилися і інші методи, як підтримки різноманітних елементів міфологічної свідомості, так і виведення з цього стану людей.

Побудова мереж дискурсивної безпеки є завданням відповідальним та витратним. Перший шар мережі будується на відповідності вузлових точок першого рівня реперним точкам формування особистості, інші будуються та контролюються під конкретні завдання, ресурси та можливості.

Мережі дискурсивної безпеки можуть забезпечити потрібну конотацію вузлових точок знаходячись під постійним впливом на деконструкцію без правових обмежень Інтернету, та у такий спосіб забезпечити «інформаційний» суверенітет. Також ця схема дає змогу деконструкції гіперреальності та контролю реальності.

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

ОХОРОНА АВТОРСЬКОГО ПРАВА У ЦИФРОВІЙ ЕКОНОМІЦІ В ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА ПИТАННЯ АДАПТАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ.

1. Характерним для ЄС є в рамках стратегічної програми утворення єдиного цифрового ринку виділення пріоритетів у охороні прав інтелектуальної власності у сучасному цифровому середовищі.

У 2010 році Європейська комісія виступає з Повідомленням «Цифровий порядок денний для Європи». Мета: пошук економічних та соціальних вигід від єдиного цифрового ринку, що базується на швидкому та ультрашвидкому Інтернеті і міжоперабельності.

Щодо сфери авторського права і суміжних прав, першочергові заходи були пов'язані з спрощенням управління правами інтелектуальної власності та транскордонним ліцензуванням через:

- підготовку пропозиції рамкової директиви щодо колективного управління правами;
- створення правового середовища для прискорення оцифрування та розповсюдження культурних надбань у Європі;
- проведення подальшого діалогу з суб'єктами ринку стосовно використання творів, які не публікуються на цей час.

Інші ініціативи включали:

- підготовку до 2012 року звіту про додаткові заходи стосовно колективного управління правами, який має включати заходи із застосування транскордонних і загальноєвропейських ліцензій;
- завершення підготовки Зеленої книги щодо розповсюдження аудіо-візуальних творів онлайн (до 2010 року: відповідне повідомлення прийнято 13 липня 2011 року);

— на підставі аналізу реалізації директиви 2004/48/ЄС до 2012 року підготовку звіту щодо додаткових заходів із захисту прав інтелектуальної власності в онлайн-середовищі, що відповідало б фундаментальним правам захисту персональних даних та особистої інформації.

Основні питання та виклики, що стосуються особливостей охорони прав інтелектуальної власності були узагальнені Комісією у Повідомленні «Єдиний ринок для прав інтелектуальної власності. Підтримка творчості та інновацій для забезпечення економічного зростання, високоякісних робочих місць та першого класу виробів та послуг у Європі» (24.05.2011)¹⁵.

У повідомленні зазначалося, що в ЄС відсутній єдиний онлайн-ринок творів, захищених авторським правом. Існують фрагментовані національні ринки. Завданням є формування середовища, яке б створювало можливості для гарантованого отримання авторами винагороди при продажу їх творів онлайн, а також для розповсюдження творів у єдиному цифровому ринку. Вказане стосується:

- системи колективного управління правами;
- управління технологіями та базами даних;
- змісту, що створений користувачами;
- зборів за приватне копіювання;
- доступу до культурного надбання Європи;
- прав виконавців;
- аудіовізуальних творів;
- прав слідування.

Зокрема, реалізуючи наведені завдання, ЄС було прийнято директиви 2012/28/ЄС про деякі дозволені використання сирітських творів та 2014/26/ЄС про колективне управління авторським правом і суміжними

¹⁵ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «A Single Market for Intellectual Property Rights. Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe». COM (2011) 287 final.

правами та мультитериторіальне ліцензування прав на музичні твори для використання онлайн на внутрішньому ринку.

2. У 2015 р. Європейська комісія здійснює наступний крок у галузі авторського права і суміжних прав. Приймається Повідомлення «Стратегія єдиного цифрового ринку для Європи», 6.05.2015 р., а також повідомлення «До сучасних більш європейських умов охорони авторського права», 9 грудня 2015 р. та «Підтримка справедливої, ефективної та конкурентоздатної європейської економіки, заснованої на авторському праві, у Єдиному цифровому ринку», 14.9.2016.

Також було представлено проекти нормативних актів у зазначеній сфері, включаючи: Пропозицію до директиви щодо авторського права у єдиному цифровому ринку, 2016 р. тощо.

Повідомлення 2015 р. включає завдання з:

- зняття перепон з міжкордонного доступу до контенту та циркуляції творів та аудіовізуальних послуг;
- забезпечення можливостей з оцифрування творів, продаж або надання доступу до яких не здійснюється;
- запровадження стандартизованої ідентифікації творів, створення Інтернет площадок для ліцензування творів; підтримки розробки агрегатору пошукових систем он-лайн, спрямованих на кінцевих користувачів;
- проведення досліджень текстів та даних (text and data mining) у наукових цілях;
- уточнення виключення стосовно «ілюстрацій у навчальних цілях» для застосування для цифрових користувачів та навчання он-лайн;
- забезпечення зберігання ресурсів у цифровій формі установами культури;
- здійснення відділеного доступу до творів у закритих електронних мережах, які використовуються у академічних науково-дослідних бібліотеках для дослідницьких цілей та навчання тощо.

3. Стосовно паралелей заходів, що відбуваються в ЄС та Україні, слід відзначити, що наведені вище ініціативи, а також прийняття директив з колективного управління та сирітських творів – не знайшли відображення в Угоді про асоціацію між Україною та ЄС. Також, слід зазначити, що як на рівні підготовки засад розвитку охорони права інтелектуальної власності в Україні, так і наукового обговорення на цей час більшість з зазначених вище питань (крім колективного управління) не підіймається в Україні.

В той же час, практика використання творів та об'єктів суміжних прав в Україні та накопичення значного обсягу проблем свідчать про необхідність:

- нагального вирішення питань з запровадження ефективно діючої системи колективного управління, збору та розподілу коштів та виплати винагороди. Вказане має здійснюватися з використанням принципів директиви ЄС про колективне управління 2014 р.;

- визначення на державному рівні бачення (у вигляді стратегії, концепції, програми) оцифрування культурної спадщини з врахуванням досвіду ЄС щодо сирітських творів, а також вирішенням проблеми використання творів, що не є у продажу або вільному доступі;

- визначення політики та механізмів відкритого доступу для наукових публікацій державних установ з врахуванням документів та практики ЄС стосовно Рамкової програми досліджень та інновацій «Горизонт 2020» та інших;

- запровадження комплексу заходів з спрощення та полегшення доступу до легітимного контенту на території України;

- визначення з врахуванням різних підходів держав-членів ЄС найбільш ефективної для України моделі захисту від он-лайн піратства.

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

*Касперський І. П., доцент спеціальної
кафедри Національної академії СБ
України, к.ю.н., с.н.с., доцент.*

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Запровадження системи електронного урядування в Україні є безумовно прогресивним кроком, який сприятиме розвитку громадянського суспільства, проте шляхи розвитку цієї системи створюють низку загроз захисту прав громадян на недоторканість їх приватного життя.

Суть проблеми полягає у тому, що в ході створення системи відбувається фактичне об'єднання інформаційних ресурсів органів державної влади у тому числі загальнодержавних реєстрів, які містять персональні дані.

Ядром такого об'єднання стає Єдиний державний демографічний реєстр (далі – Реєстр), в якому планується акумулювати дані які будуть використовувати для видачі 17 видів документів, зокрема паспорта громадянина України, паспорта громадянина України для виїзду за кордон та посвідчення водія. При цьому до Реєстру зокрема вносяться відцифровані зразок підпису особи, образ обличчя особи, інформація про податковий номер та відцифровані відбитки пальців рук особи. Також до реєстру будуть включати досить докладну інформацію щодо особистого життя - місце проживання, про народження дітей, про шлюб і розірвання шлюбу [1].

Більше того, до системи електронного урядування за твердженням заступника голови Державного агентства з питань електронного урядування Олексія Вискуба збираються включити електронну систему охорони здоров'я eHealth, до якої буде включено інформацію про лікарів та запроваджено сервіс електронних медичних карт і електронних рецептів. При цьому зазначене агентство «всіляко сприятиме інтеграції майбутньої системи eHealth з існуючими електронними реєстрами країни» [2].

У цих тенденціях вбачаються суттєві порушення принципів обробки персональних даних, закріплених у Законі України «Про захист

персональних даних» [3] та 108-ї конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [4], які полягають у ненадмірності обсягу персональних даних, які включаються до певного реєстру, стосовно мети їх обробки та незаконного розширення мети використання індивідуального податкового номера фізичних осіб, створення якого передбачало виключно потребу ідентифікації платника податків і аж ніяк не туриста, що подорожує за межі держави.

Такі ж дивні для демократичного суспільства прагнення вже були у 2004 році зупинені нашим парламентом. Тоді на підставі висновку Комітету Верховної Ради України з питань Європейської інтеграції Верховна Рада України відхилила законопроект про реєстрацію фізичних осіб в Україні, як такий, що не відповідає нормам Європейського Союзу, зобов'язанням України перед Радою Європи та суперечить Конституції України.

Ці ж причини призвели до того, що Президент України Віктор Ющенко своїм Указом від 10 березня 2005 року за № 457/2005 року анулював попередні рішення Президента Кучми щодо створення «Єдиного державного реєстру фізичних осіб» [5].

Позитивна світова практика свідчить про те, що у Великобританії ще в 1953 році Верховний Суд скасував право поліції вимагати від громадян пред'явлення ідентифікаційної картки як незаконне. Потім це призвело до скасування британського Закону про державну реєстрацію і всієї системи ідентифікаційних карток. В 1986 році уряд Австралії намагався запровадити загальнодержавну ідентифікаційну картку, що викликало масові протести і призвело до відмови від такого рішення [6]. У 1998 році Верховний Суд Філіппін ухвалив рішення про те, що національна система ідентифікації є порушенням конституційного права на приватність. У 1991 році Конституційний суд Угорщини дійшов висновку, що закон про введення багатоцільових особистих ідентифікаційних номерів порушує конституційне право на приватність [7].

З огляду на вітчизняну та світову практику суспільство та уряд повинні визнати, що наявність внутрішнього паспорта в Україні чи то у вигляді «книжечки», чи пластикової ID картки— це рудимент радянського паспортного режиму, який за умови сучасного розвитку інформаційних технологій створює суттєву загрозу приватності, будує підґрунтя для зловживань владою та численних видів злочинних посягань і від якого слід показово відмовитись, запровадивши відповідні заборонні норми у законодавство. Також слід переглянути практику зосередження державних реєстрів довкола окремих державних органів та єдиних адміністраторів, розділивши компетенції Мін'юсту, органів внутрішніх справ та міграційної служби. Органи державної влади повинні надавати адміністративні послуги у тому числі із використанням ресурсів електронного урядування окремо, використовуючи окремі бази даних відповідно до своєї компетенції Ці зміни дозволять привести законодавство у відповідність до європейських вимог та сприятимуть європейській інтеграції України.

Список використаних джерел:

1. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20 листопада 2012 р. // Офіційний вісник України від 14.12.2012 — 2012 р., № 93, стор. 122, стаття 3771, код акту 64640/2012
2. В. Карпусь Минздрав показал демо-версию электронного медицинского сервиса eHealth [Електронний ресурс]. – Режим доступу: <http://itc.ua/news/minzdrav-pokazal-demo-versiyu-elektronnogo-meditsinskogo-servisa-ehealth/>
3. Закон України «Про захист персональних даних» // Офіційний вісник України від 09.07.2010 - 2010 р., № 49, стор. 199, стаття 1604
4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: затв. рішенням Ради Європи 108/1981 [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/994_326
5. Указ Президента України "Про внесення змін до Положення про паспорт громадянина України для виїзду за кордон та визнання такими, що втратили чинність, деяких указів Президента України" // Офіційний вісник України від 01.04.2005 — 2005 р., № 11, стор. 12, стаття 519, код акту 31772/2005

6. С. Девіс Ідентифікаційні картки. Питання, що постають найчастіше [Електронний ресурс]. – Режим доступу: <http://khpg.org/index.php?id=944254901>

7. U.S. Department of State Singapore Country Report on Human Rights Practices for 1997, January 30, 1998 [Електронний ресурс]. – Режим доступу: <http://www.refworld.org/docid/3ae6aa1d18.html>

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

*Петряев С. Ю., заведующий кафедрой
информационного права и права
интеллектуальной собственности
КПИ им. Игоря Сикорского.*

СОЦИАЛЬНЫЕ РИСКИ КИБЕРСОЦИАЛИЗАЦИИ НА ПУТИ К КИБЕРЦИВИЛИЗАЦИИ

Развитие нашей цивилизации постоянно связано с появлением все новых и новых общественных отношений, часть из которых продолжает существовать и преобразовываться, другая часть отмирает, завершив свою роль общественного регулятора. Наиболее конфликтные общественные отношения, требующие правового регулирования, возводятся в законы, обеспечивая общественное согласие.

Сегодня информационные технологии активно наполняют общество информацией, которая формирует новые общественные отношения, обеспечивая ускоренное развитие цивилизации. Как и всякое новое, информационные технологии привели к разрушению устоявшихся правил социализации, ломая стереотипы, условия, формы и гармонию развития молодых людей, которые вырабатывались веками. IT-технологии погрузили общество в информационное пространство, разнообразие контента сформировало армию пользователей информационных сетей, обеспечив общество новыми знаниями и интересами, что повлияло на формирование новых условий социализации.

Объемы информации, которые окружают нас сегодня, кратно превышают период десятилетней давности и продолжают ускоренно расти.

Значительная часть этой информации по своему содержанию причисляют к информационному «мусору», выполняющему функции виртуального развлечения и коммуникации. К таким информационным ресурсам относят постоянно обновляющиеся новости, рекламы, переписка с друзьями в режиме онлайн, игры, описания частной жизни известных людей в области шоу бизнеса, политики, спорта, самореклама и многие другие ресурсы, создающие условия комфорта. Подобная информация не несет человеку ничего кроме захламления мозга. В научном мире этой информации придумано более мягкое название – «белый шум».

Ранее мы уже писали, что белый шум *поглощает все больше и больше свободное время личности, а значит и всего общества, отрывая от реальной жизни. Все ярче вырисовывается современная картина общественного бытия, когда не Интернет служит личности как инструмент решения различных социальных задач, а личность (общество) начинает подчиняться Интернету, который как спрут затягивает ее в бездну белой информации, из которой она уже не в силах выбраться [1].*

Память — это сложный познавательный процесс, благодаря которому человек может запоминать, сохранять и воспроизводить свой прошлый опыт. Загружая мозг белым шумом, происходит перегрузка памяти, мозг быстро устает и у человека наступает физическая усталость. Погружение в атмосферу белого шума, приводит к дезориентации во времени, что влечет за собой его растрачивание без какой-либо компенсации. Для усвоения полезной информации у человека уже не остается ни сил, ни времени.

Нахождение молодых людей в постоянном белом информационном поле, в частности, непрерывное «втыкание» в смартфон, доводит студентов до состояния мозговой и физической усталости. Если еще 7-10 лет назад концентрация внимания студентов при получении информации на занятиях длилось 60-45 минут, то сегодня, 10-15 минут. За тем наступает рассеянность внимания, появляется блуждающий взгляд, который переключает внимание на более мягкие раздражители.

Наблюдая за поведением молодых людей (студентов) на протяжении десяти лет, нами было отмечено, что моментом коренного перехода к поколению, теряющему способность к запоминанию и анализу информации, пришелся на поколение, рожденное после 1995 года. Именно с этого момента ярко проявились симптомы перехода от классической формы усвоения информации (через конспектирование лекций, учебников, научных первоисточников) к использованию информационных сетей, как «единственному» источнику ответов на все вопросы. Таким образом, смартфон становится для молодых людей (студентов) чуть ли не единственным источником получения научных знаний.

Общеизвестно, что именно классическая художественная литература, музеи классического изобразительного искусства, кинематография периода «золотого века» Голливуда, советского периода и др., носили *воспитательный характер, развивали образное и критическое мышление, формировали богатство и культуру речи, развивали интеллект и словарный запас, расширяли кругозор и креативность, формировали человеческие ценности и способствовали саморазвитию* [2].

На ежегодный вопрос к аудитории студентов, какие художественные книги вы прочитали за свою жизнь, с каждым новым годом ответы все ближе стремятся к нулю. И это закономерный результат реализации не только информационных технологий, но и политики государства. В частности, в средних школах на протяжении последних десяти лет по различным надуманным причинам происходит сокращение программ гуманитарного характера, в особенности освоения классической художественной литературы и упрощение форм ее усвоения [3]. В результате, перманентных реформ среднего образования в совокупности с информационными технологиями привели к снижению интеллектуального развития молодых людей.

Подводя итог сказанному, обозначим некоторые симптомы влияния информационных технологий, которые ярко проявляются у современного молодого человека. К ним следует отнести:

- преобладающе наполнение сознания молодых людей белой информацией;

- снижена умственная работоспособность, наступает быстрая утомляемость мозга (*мозг отказывается воспринимать информацию*) и общая физическая усталость, неспособность концентрации внимания на восприятие информации (*рассеянность внимания*);

- из-за растрченного времени и утомляемости снижается или утрачивается потребность в чтении художественной классики, которая всегда была основой развития образного и критического мышления;

- на этой основе происходит обеднение устной и письменной речи, что компенсируется нецензурной бранью, которая приобретает статус «нормальной» культуры речи;

- происходит торможение развития критического, образного и абстрактного мышления;

- снижается способность к удерживанию информации в сознании;

- утрачивается интерес и азарт к получению знаний и ощущения умственного развития (*удовольствие от познания*);

- снижается чувство соперничества и командной игры, развивается безразличие к сути происходящего, наступает своего рода «паралич души¹⁶»;

- интернет информация воспринимается как истина последней инстанции;

- на этой основе игнорируются учебники и научные первоисточники.

¹⁶ «Паралич души» - «Равнодушие - это паралич души» (из рассказа А. П. Чехова «Палата №6»).

Таким образом, происходит преобладание виртуальной социализации над традиционной социализацией.

Данная проблема характерна не только для Украины, но и для всех развитых стран, в которых присутствует высокий уровень использования IT-технологий. Например, *преподаватели итальянских вузов, ученые и журналисты обратились к властям с призывом принять скорейшие меры для повышения уровня грамотности среди школьников и студентов. "Годами известно, что к концу обучения в школе многие ребята плохо пишут по-итальянски, мало читают и с трудом изъясняются. Преподаватели вузов давно сталкиваются с языковыми пробелами у своих студентов, которые делают ошибки, допустимые разве что в третьем классе начальной школы. Кроме этого, в письме к властям содержится призыв пересмотреть школьную программу и ввести периодическую аттестацию в ходе всего обучения. Эти проверки подразумевают под собой орфографический диктант, пересказ текста, его грамматический анализ, задание на понимание лексики и даже письмо от руки [4].*

Американские ученые отмечают, что студенты покидают колледжи без интеллектуальных навыков, необходимых для обоснования сложных вопросов из-за низкой способности к критическому мышлению по причине непонимания его сущности и, соответственно, отсутствия навыков к последнему со стороны преподавателей. Лишь небольшое меньшинство преподавательского состава колледжей (19%) может дать четкое объяснение того, что такое критическое мышление. Более того, согласно их ответам, только 9% респондентов обучали критическому мышлению своих студентов [5].

Даже с таким социальным явлением, как преступность, за много веков мы научились бороться, если не правовыми методами, то наполеоновскими. Но как бороться с «добровольным согласием населения на всеобщую лоботомию», в виде тотального снижения интеллектуального уровня молодого поколения в условиях цифрового общества, ясного ответа пока нет.

Вместе с тем, общество, как и природа, самостоятельно начинает искать выход из сложившегося условия жизни. Наиболее мыслящие члены общества, понимающие, к чему может привести бесконтрольная форма потребления белой информации, основанной на IT-технологиях, самостоятельно предпринимают шаги в защиту своего потомства от превращения их в бездумных, полуобразованных, механических особей.

Сегодня становится распространенным явлением, когда родители отказываются отдавать детей в школы, а предпочитают учить их самостоятельно или нанимают частных преподавателей. Приучают детей читать классическую художественную литературу, обсуждая прочитанное, ведут разъяснительные беседы о достоинствах и недостатках информационных технологий, не позволяют смотреть телевизионные программы, мультфильмы, художественные фильмы, которые изменяют сознание и формируют психологические отклонения.

Список использованных источников:

1. «Киберцивилизация»: $A \neq A$, а в общем напоминают прежних... - Інформація і право. Науковий журнал НДІП НАПрН України. – №3(12). - 2014. – С.25-30. – [Электронный ресурс]. – Режим доступа:
2. 9 фактов о ценности чтения. – [Электронный ресурс]. – Режим доступа: https://weekend.rambler.ru/read/9-faktov-o-cennosti-chteniya-2017-04-11/?utm_campaign=brain&utm_medium=rec&utm_source=rambler&utm_content=weekend
3. В школах решили сократить русскую литературу. - [Электронный ресурс]. – Режим доступа: <http://vesti-ukr.com/strana/94453-v-shkolah-reshili-sokratit-russkuju-literaturu>
4. Итальянские ученые и преподаватели пожаловались на безграмотность молодежи. – [Электронный ресурс]. – Режим доступа: https://news.rambler.ru/world/36009194/?utm_content=news&utm_medium=read_more&utm_source=copylink
5. The State of Critical Thinking Today. – [Электронный ресурс]. – Режим доступа: <http://www.criticalthinking.org/pages/the-state-of-critical-thinking-today/523>

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

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАХОДИ ПРОТИДІЇ НЕГАТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ НА ДІТЕЙ В УКРАЇНІ

Негативні інформаційні та інформаційно-психологічні впливи на свідомість людини сьогодні є настільки потужними, що потребують кардинального перегляду державної політики щодо убезпечення своїх громадян з врахуванням новітніх викликів і загроз, а також модернізації системи забезпечення безпеки людини в інформаційному просторі. Враховуючи масштаби застосування цифрових технологій у житті сучасного суспільства, загроза від негативного інформаційного впливу є не лише для свідомості людини, але й, через вплив на прийняття нею рішень та втручання в роботу системи забезпечення функціонування інфраструктурних об'єктів, може становити небезпеку в сфері екології, енергетики, транспорту і загалом національної безпеки, що призведе до економічного та політичного послаблення нашої держави, а також становитиме загрозу для життя, здоров'я і добробуту її громадян.

Дитина є особливим суб'єктом суспільних відносин, що відповідно до національного та міжнародного законодавства, яке ґрунтується на Конституції України [1] та Конвенції ООН про права дитини [2], потребує особливого захисту та піклування з боку держави та основних її інститутів, на які покладено функції по забезпеченню найкращих інтересів дитини, направлених на задоволення її індивідуальних потреб відповідно до віку, статі, стану здоров'я, особливостей розвитку, життєвого досвіду, родинної, культурної та етнічної належності, а також вжиття заходів, спрямованих на забезпечення повноцінного життя, всебічного виховання, розвитку та захисту її прав (ст. 1 Закону України «Про охорону дитинства») [3]. Основною функцією, покладеною суспільством на дитину, є її навчання шляхом освіти

та самоосвіти для інтелектуального, духовного зростання і засвоєння суспільно необхідних навичок й умінь. Навчання – це «цілеспрямований процес передачі і засвоєння знань, умінь, навичок і способів пізнавальної діяльності людини» [4, с. 227], який в сучасних умовах невід’ємно пов’язаний із роботою з інформацією та інформаційними ресурсами. Навчальний заклад, як основний освітній та соціалізаційний інститут держави сьогодні повинен не лише забезпечувати особу інформацією, але й, в першу чергу, навчити її працювати з нею: знаходити, виокремлювати, аналізувати, компілювати, використовувати для задоволення власних потреб та реалізації поставлених цілей. Проте чи не найважливішим навиком, який необхідний особі у високо розвинутому інформаційному суспільстві є вміння захищати власний інформаційний простір та протидіяти негативним інформаційним та інформаційно-психологічним впливам на свідомість. Дитина в силу вікового онтогенезу та недостатнього розвитку когнітивних і аналітичних здібностей є більш піддатливою до факторів ризику, що присутні в інформаційному просторі. У той же час вона є найактивнішим учасником суспільних відносин в інформаційній сфері та наймасовішим споживачем інформаційного продукту через особливості суспільної діяльності (накопичення знань) і природньої цікавості до всього нового, сучасного й прогресивного.

Зважаючи на той факт, що навчальний заклад є основною державною інституцією в сфері освіти, виховання та соціалізації дитини, то вміння і навички поведінки в інформаційному просторі, здатність убезпечувати себе від негативної дії інформації та забезпечувати інформаційну безпеку не провокуючи власними діями чи бездіяльністю небезпеку створення або реалізації інформаційних загроз, діти повинні здобувати саме тут, поряд із навичками і знаннями з інших предметів. Функції ж по забезпеченню та підвищенню інформаційної грамотності доцільним було б покласти на навчальний заклад, а сам навчальний заклад включити в систему забезпечення інформаційної безпеки дитини.

Водночас пропонується перегляд парадигми освіти та коригування ідеологій освітніх програм з врахування нових можливостей та викликів притаманних інформаційному суспільству. Вважається за доцільне підвищити значення інформаційної грамотності в системі початкової, середньої та вищої освіти. Пропонується запровадити курс «Інформаційна безпека особи», як окремий предмет або як розділ дисциплін «Основи життєдіяльності» та «Інформатика» в шкільну програму. Також важливим є рівень обізнаності викладачів, особливо вказаних дисциплін. Тому необхідним є перегляд навчальних програм вищих навчальних закладів педагогічного спрямування. Доцільним також є запровадження курсу «Інформаційні ресурси та робота з ними» для старшокласників та студентів для підвищення їх інформаційної грамотності.

Поряд з цим держава зобов'язана забезпечити систему моніторингу інформаційного простору задля недопущення розповсюдження матеріалів, що можуть становити загрозу психофізичному здоров'ю дитини. Завдання по моніторингу інформаційного простору покладені на силові структури держави, зокрема на новостворену кіберполіцію. Задля недопущення розповсюдження матеріалів, які містять жорстокість, насилля, порнографію та ті, що можуть зашкодити дитині, вважається за доцільне широке залучення громадянського суспільства для моніторингу інформаційного простору нашої держави.

Постійний контроль за фізичним та психологічним станом дітей органами охорони здоров'я також повинен стати елементом державної системи протидії негативним інформаційним та інформаційно-психологічним впливам і забезпечення інформаційної безпеки дитини. Саме вчасне виявлення психофізичних відхилень від норми у стані дитини може врятувати не лише її здоров'я, але, по-декуди, й життя. Тому доцільно розробити єдину систему маркерів інформаційної небезпеки психічному та психологічному здоров'ю дитини задля використання у контролі за її психофізичним станом.

Система моніторингу морально-психологічного стану дітей психологами та соціологами дозволить вчасно виявляти індивідуальні проблеми дітей, вираховувати загрози в інформаційному просторі та прогнозувати тенденції у розвитку небезпек.

Вчасне виявлення і нейтралізація загроз, здатність дитини протидіяти негативним інформаційним впливам та власноруч убезпечувати себе в інформаційному просторі – це лівова частка в системі інформаційної безпеки дитини. Проте не менш важливим є й інформаційна політика держави. Для розвитку успішної, правосвідомої, інформаційно грамотної особи з високим інтелектуальним рівнем необхідно наповнити інформаційний простір нашої держави якісним національним продуктом, що пропагував би національні й загальнолюдські цінності, направляв би на самовдосконалення та розвиток. Це також буде контпропагандним заходом та частиною боротьби проти інформаційної агресії із-за кордонів України. Боротьба з пропагандою сьогодні також є важливим елементом в системі протидії негативному впливу інформації на свідомість дитини, тому реалізація таких заходів силами державних інституцій та громадянського суспільства повинна стати системною та обов'язковою.

В умовах інформаційної агресії необхідно переглянути ступінь відповідальності учасників суспільних відносин в інформаційній сфері, особливо що стосується дій чи бездіяльності, що призвели до деструктивного інформаційного впливу та завдали шкоди неповнолітньому, на кшталт залучення у групи смерті, доведення до самогубства чи залучення до антидержавної діяльності через інформаційно-комунікаційні технології.

Насамкінець хотілося б звернути увагу, що будь-яка система працює лише тоді, коли існує чітке бачення її мети, цілей та алгоритмів. Лише тоді всі структурні елементи бездоганно виконують свої функції, зв'язки між ними забезпечують координацію і поставлена мета досягається. Для підвищення ефективності організаційно-правових заходів протидії негативним інформаційним впливам на дитину слід визначитися з

концептуальними підходами та доктринальними засадами забезпечення її інформаційної безпеки. Тому пропонується створити «Концепцію інформаційної безпеки дитини».

Список використаних джерел:

1. Конституція України [Електронний ресурс] : Закон від 28.06.1996 № 254к/96-ВР – Режим доступу : // <http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-D0%B2%D1%80>
2. Конвенція про права дитини : ООН від 20.11.1989. – [Електронний ресурс] – Режим доступу : http://zakon1.rada.gov.ua/laws/show/995_021
3. Про охорону дитинства [Електронний ресурс] : Верховна Рада України; Закон від 26.04.2001 № 2402-ІІІ. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/2402-14>
4. Гончаренко С.У. Український педагогічний словник. / Семен Устимович Гончаренко.— Київ: Либідь

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

*Петряєв О. С., аспірант
Національного інституту
стратегічних досліджень України.*

ПРОТИДІЯ ІНТЕРНЕТ-АКТИВНОСТІ РАДИКАЛЬНОГО ІСЛАМУ ЯК ПРОБЛЕМА КІБЕРБЕЗПЕКИ

Впродовж останніх десятиліть інтернет став методом впливу та пропаганди не тільки на державному рівні, але й на рівні різноманітних комерційних та некомерційних груп й організацій. Не всі з них є правослухняними. У цифровому просторі вистачає й представництв організацій радикального, екстремістського й терористичного спрямування.

Прикладом може бути Ісламська Держава Іраку і Леванту (ІГІЛ або ДАІШ), яка за допомогою інформаційних технологій пропагує свої ідеї, залякує супротивників та вербує у свої ряди нових членів. Водночас ідеї радикального войовничого ісламу пропагуються й традиційними засобами розповсюдження листівок або аудіо- відеозаписів. Перевагою інтернету є те, що він надає можливість вести пропаганду в будь якій частині світу, серед

різних верств населення та віросповідання, незалежно від місцезнаходження джерела інформації. Якщо у 1998 році у всьому світі нараховувалося тільки 12 сайтів, які пропагували радикальний іслам, то у 2005 році їх кількість зросла до 4800 з використанням різних мов, а у 2013 році їх вже стало приблизно 10 000 тисяч. [1]

Серед багатосторонніх напрямів пропаганди ІДІЛ неабияке місце відводиться методам залякування шляхом поширення відео та фотоматеріалів страт «ворогів» та «відщепенців», які проводяться з середньовічною жорстокістю. Так само поширюються відео і фотоматеріали боїв солдатів халіфату проти армій Сирії, Іраку та Курдських загонів Пешмерга.

Ще одним з напрямів пропаганди ісламістів є демонстрацію «чудового життя» на підконтрольних ісламістам територіях. Сюжети цих матеріалів доволі традиційні: ІГІЛовці роздають їжу населенню, відновлюють інфраструктуру, організовують порядок в невизнаній державі. Натомість пропагандист з ІДІЛ намагаються довести, що армії Сирії, Іраку, авіаційні групи Росії, США і їхня коаліція не сприяють побудові успішної сильної держави, а займаються виключно нищенням інфраструктури, вбивствами мирних громадян тощо.

Цільовою аудиторією агітаторів і пропагандистів ІДІЛ є молоді мусульмани, які проживають в країнах Європи і США, в РФ та інших пострадянських республіках і передусім – центрально-азійських – з переважанням мусульман. Розрахунок зводиться до того, що, перебуваючи в немусульманських країнах, молоді мусульмани відчуваю себе дискомфортно і шукають відповіді на багато питань, звертаючись до вчення ісламу. Таким чином вони є носіями подвійної ідентичності, поєднувати в собі лояльне до країни передування громадянство і релігію та культуру країн походження. Якщо ж при цьому молодим мусульманам не вдається досягти в західних країнах хоча б відносного життєвого успіху, то їм легко нав'язати думку, що

воюючи за халіфат, вони зможуть знайти майбутнє і побудувати нове успішне життя, досягти райського блаженства тощо [3].

Проблема вербування бойовиків ІГІЛ не обійшла й Україну. Агітатори ісламського халіфату концентрують увагу на мешканцях університетських гуртожитків, молодих українцях, які цікавляться східною культурою, ісламом, «романтикою» Близького Сходу.

Дистанційна агітація за допомогою інформаційних технологій призвела до появи нового різновиду терористів-одинаків. Такі люди, під впливом пропаганди ІГІЛ, жодного разу не побувавши в арабських або мусульманських країнах, спроможні самотужки здійснити теракт, прикладом чого є численні жертви в Європі як наслідок використання терористами-одинаками викрадених транспортних засобів з подальшим наїздом на групи людей [4].

Ще однією з проблем, з якою зустрілися фахівці з інформаційно-психологічних операцій, є мовні комунікативні бар'єри. Чимало сторінок в соціальних мережах, на яких розміщені матеріали екстремістського характеру, закриваються, якщо інформацію подано англійською, російською або іншими європейськими мовами. Але сторінки оформлені на арабській або турецькій мовах рідко блокуються [4].

Окрім блокування провайдерами небезпечних сторінок Інтернету, існує чимало інших ефективних методів боротьби з пропагандою ІГІЛ в інформаційному просторі. Передусім йдеться про питання належної ідентифікації, автентифікації та авторизації. Для полегшення ідентифікації користувача сторінки користувачів соціальних мереж повинні бути підкріплені паспортними та іншими персональними даними, що допоможе зупинити поширення пропагандистських матеріалів ІДІЛ на початковому рівні [4]. Звичайно міркування суспільної та державної безпеки наштовхуються у даному разі на міркування персональної та комерційної безпеки і є чимало правоохоронних організацій, які чинять спротив

контртерористичним заходам, керуючись різними «благими намірами». Гостроту цих політико-правових колізій було б неправильно применшувати.

Список використаних джерел:

1. Сулейманов Р. Методы и формы агитации ИГИЛ в социальных сетях в Интернете. [Электронный ресурс] / [Агенство Политических Новостей]. – Режим доступа: <http://www.apn.ru/publications/article34201.htm> (дата звернення 10.05.2017) – Название с экрана.
2. Geller E. Why ISIS is winning the online propaganda war. [Электронный ресурс] / [The Daily Dot]. – Режим доступа: <https://www.dailydot.com/layer8/isis-terrorism-social-media-internet-counter-violent-extremism/> (дата звернення 10.05.2017) – Назва з екрану.
3. Гаркуша Ю.О. Тероризм як окремий вид суспільно небезпечної діяльності, вчинений з використанням соціальних мереж. Право і суспільство. № 4 / 2016., С. 178-179.

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

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

**ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ В
ПРОЦЕСІ ПРИЙНЯТТЯ РІШЕНЬ ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ
КІБЕРБЕЗПЕКИ**

Загальні системні вимоги щодо властивостей та характеристик інформації надаються у визначенні інформаційної безпеки, під якою розуміють - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1].

Саме в першій частині цього визначення зазначається, що інформація якою користуються людина, суспільство та держава повинна бути повною, достовірною та своєчасною, в іншому випадку це призводить до зниження

ефективності їх діяльності, в тому числі, до зниження якості рішень, які приймаються на будь-якому рівні.

Вбачається, що останні прогресивні тенденції підвищення якості рішень, які приймаються на будь-якому рівні (національному, регіональному або місцевому) зводяться в основному до максимального залучення громадян в процес прийняття рішень.

Відомо, що наявність недостатньої, викривленої, перекрученої або зміненої інформації різко зменшує ефект від залучення громадян в процес прийняття рішення. Тому, однією із умов ефективного залучення є забезпечення всіх учасників процесу прийняття рішень повною, достовірною та своєчасною інформацією, що сприятиме їх об'єктивному волевиявленню.

Повнота, достовірність та своєчасність інформації забезпечується насамперед ефективністю інформаційної взаємодії всіх суб'єктів, які залучені до прийняття рішень.

Таким чином, однією із базових умов інформаційної безпеки є наявність ефективної інформаційної взаємодії між всіма суб'єктами, які приймають участь в процесі прийняття рішень, особливо на місцевому рівні, адже саме тут сконцентровано більшість інтересів населення, а з урахуванням процесу децентралізації, кількість рішень, що будуть прийматись, значно збільшиться.

Відповідно до кращих європейських практик та стандартів для забезпечення участі громадян в процесі прийняття рішень використовуються більше 20 основних видів різноманітних інструментів інформаційної взаємодії.

Наприклад, в Австрії вважають, що правові механізми залучення повинні забезпечувати: ідентифікацію громадян за інтересами та регіонами, де вони проживають; інформаційні умови для відображення широкого спектру думок щодо різних варіантів вирішення проблемних питань. Крім того, відповідальні особи повинні мати обов'язок з врахування результатів участі громадян в прийнятті рішень. "Врахування" означає, що результати

участі включаються в проекти рішень, висунуті аргументи розглядаються зі змістовної точки зору, обговорюються з учасниками, оцінюються способом, що дозволяє відстеження динаміки, після чого вони стають частиною політичного курсу, плану, програми або правового інструменту [2, с. 19].

Порівняльно-правовий аналіз свідчить, що в українському законодавстві використовується лише невелика кількість подібних інструментів. Однак, навіть їх правове регулювання є недосконалим, зокрема, законодавством не передбачено обов'язкового врахування рішення громадської ради щодо вивчення громадської думки, не передбачено критеріїв до змісту та форми звітів, які надаються посадовими особами, а отже порівняти та оцінити результати роботи органу чи комісії в ретроспективному аспекті складно.

Таким чином, відсутність вимог до критеріїв, змісту і форми надання та врахування інформації всіма суб'єктами в процесі інформаційної взаємодії створює умови для погіршення стану інформаційної безпеки в місцевому самоврядуванні. Крім того, правове закріплення вимог до критеріїв, змісту і форми щодо обробки інформації забезпечить методологічну основу для оцінки рівня захищеності, оскільки, потенційно здатні забезпечити кількісні критерії для оцінки ступеню можливих загроз.

Для виявлення особливостей правового регулювання необхідно здійснювати глибокий аналіз змісту правовідносин, які існують в процесі інформаційної взаємодії, а також їх суб'єктного та об'єктного складу. Доцільно звертати увагу на повноту визначення прав, обов'язків та відповідальності всіх суб'єктів інформаційної взаємодії в процесі використання будь-якого інформаційного інструменту на будь-якому етапі прийняття рішень. Чутливим питанням є повне та вичерпне визначення обов'язків посадових осіб суб'єктів владних повноважень, оскільки сприятиме зниженню дискреції в їх діяльності.

Зауважимо, що в процесі формування пропозицій щодо вдосконалення відповідного законодавства критичним є визначення єдиних правових

позицій – спеціальних принципів інформаційного права в частині інформаційної взаємодії в місцевому самоврядуванні.

Особливої уваги заслуговує правовий режим обігу інформації в системі «орган влади — громадянин», оскільки норми європейського законодавства передбачають правове регулювання багатьох інструментів залучення, акцентуючись саме на обов'язках органу влади при наданні структурованої, повної та своєчасної інформації.

Зауважимо, що в сучасних умовах наявності значної кількості членів громади, максимальне залучення для прийняття рішень широких верств населення можливо забезпечити лише за умови використання комп'ютерних та телекомунікаційних технологій в процесі забезпечення інформаційної взаємодії всіх суб'єктів місцевого самоврядування.

Відповідно до визначення кібернетичної безпеки під нею розуміється інформаційна безпека в умовах застосування комп'ютерних та телекомунікаційних технологій [3, с. 61]. Отже, проблематика кібербезпеки має безпосереднє відношення до правового регулювання інформаційної взаємодії між всіма суб'єктами, які приймають участь в процесі прийняття рішення на місцевому рівні.

Таким чином, вдосконалення національного законодавства на основі положень міжнародно-правових документів та кращих практик європейських країн щодо правового регулювання інформаційної взаємодії суб'єктів процесу прийняття рішень необхідно проводити з урахуванням вимог нормативно-правових актів щодо кібернетичної безпеки, що дозволить створити умови для забезпечення кожного громадянина та посадових осіб своєчасною, структурованою, змістовною та повною інформацією.

Список використаних джерел:

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V / Верховна Рада України // Відомості Верховної Ради України. — Офіц. Вид. — 2007. — № 12. — ст.102. — URL: <http://zakon5.rada.gov.ua/laws/show/537-16>

2. Standards of Public Participation (2008; adopted by the Austrian Council of Ministers on 2 July 2008) — URL:
http://www.partizipation.at/fileadmin/media_data/Downloads/Standards_OeB/oebs_standards_engl_finale_web.pdf

3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. — № 2(42). — 2014. — С. 54-61

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

*Іванова М. В., науковий співробітник
відділу з охорони інтелектуальної
власності Національної бібліотеки
України ім. В. І. Вернадського.
Голосніченко Д. І., д.ю.н., професор
кафедри господарського та
адміністративного права ФСП КПІ ім.
Ігоря Сікорського.*

ІНФОРМАЦІЯ ЯК ПРОДУКТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Право на інформацію є одним із природних прав людини, тому відносини щодо одержання, розповсюдження та захисту інформації повинні бути урегульовані законом відповідно до сучасних умов правової реальності. Відповідно до ст. 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Стратегія розвитку інформаційного суспільства в Україні визначає мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні. В нашій державі сформовано основні правові засади побудови інформаційного суспільства шляхом прийняття ряду нормативно-правових актів, які, зокрема, регулюють суспільні відносини у сфері сприяння розвитку громадянського суспільства, створення інформаційних електронних

ресурсів, захисту прав інтелектуальної власності на такі ресурси, гарантій та механізму доступу до публічної інформації, електронного документообігу, інформаційної безпеки тощо [1]. В інформаційному суспільстві акценти все більше переміщуються з виробництва у сферу інтелектуальної, творчої діяльності. Інформатизація суспільства передбачає правомірність використання інтелектуальних надбань людства. Забезпечення належної охорони прав інтелектуальної власності є однією з найважливіших умов успішного розвитку інформаційного суспільства [2, с. 441].

В умовах переходу до інформаційного етапу розвитку суспільства інформація стає одним із основних продуктів суспільства, яка має бути якісною, оперативною і відповідати потребам розвитку цього суспільства. Тому, захист інформації є важливою запорукою розвитку суспільства.

В Законі України «Про інформацію» під інформацією розуміють – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Таке ж визначення міститься в ст. 200 Цивільного кодексу України. В Законі України «Про захист економічної конкуренції» визначається, що інформація – це відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості. В свою чергу, відповідно до ст. 8 ЗУ «Про авторське право і суміжні права» об'єктами авторського права є твори у галузі науки, літератури і мистецтва, зокрема: літературні письмові твори белетристичного, публіцистичного, наукового, технічного або іншого характеру (книги, брошури, статті тощо); комп'ютерні програми; бази даних; музичні твори з текстом і без тексту; аудіовізуальні твори; фотографічні твори, у тому числі твори, виконані способами, подібними до фотографії тощо. Вбачаємо, що частина інформації може виступати об'єктом

інтелектуальної власності. Щоб визначитись яка інформація може відноситись до права інтелектуальної власності, необхідно розібратись: як поняття «інтелектуальна власність» відрізняється від поняття «інтелектуальна діяльність».

Інтелектуальна діяльність – це розумова (творча, духовна) праця людини в галузі науки, техніки, літератури, мистецтва, художнього конструювання тощо. Творча праця спрямована на створення та впровадження інновацій. Інтелектуальна діяльність втілюється і виявляється у певних результатах – інтелектуальних продуктах. Не всяка інтелектуальна діяльність є творчою працею, водночас будь-який творчий результат – продукт інтелектуальної діяльності. Творча діяльність – це діяльність, внаслідок якої народжується щось якісно нове, що вирізняється неповторністю, оригінальністю і суспільно–історичною унікальністю. Творчість властива лише людині, яка є єдиним суб'єктом творчої діяльності. Творча діяльність - це поняття більш широке, ніж інтелектуальна діяльність. Результати інтелектуальної діяльності, стосовно яких здійснюється правова охорона (які мають властивості охороноспроможності), є об'єктами інтелектуальної власності [3, с. 20–21].

А. І. Марущак акцентуючи увагу на ознаках інформації як складової цивільних правовідносин, вказує, що підставами виникнення права власності на інформацію є: створення інформації своїми силами і за свій рахунок; договір на створення інформації; договір, що містить умови переходу права власності на інформацію до іншої особи [4, с. 33–36.]. Аналогічні підстави існують при створенні об'єктів інтелектуальної власності.

В ряді законодавчих визначень, де використовується поняття «інформація», можемо спостерігати терміни, які можна віднести до інтелектуальної діяльності. Наприклад, інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) (Закон України «Про Національну програму інформатизації»); інформаційний ринок – це система економічних, організаційних і правових

відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг (Закон України «Про науково-технічну інформацію») інформаційні ресурси науково-технічної інформації – це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях (Закон України «Про науково-технічну інформацію»); інформаційні ресурси спільного користування – це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання (Закон України «Про науково-технічну інформацію») тощо.

Підсумовуючи розгляд співвідношення інформації та об'єктів права інтелектуальної власності слід зазначити, що термін «інформація» має широке застосування в сучасному суспільстві, інформація виступає об'єктом охорони цивільного права, може виступати результатом інтелектуальної діяльності та охороняється законодавством як об'єкт інтелектуальної власності.

Список використаних джерел:

1. Стратегія розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р // Офіційний вісник України – 2013. – № 44. – Ст. 1581.
2. Іванова М. Електронні інформаційні ресурси конституційно-правової тематики у фондах НЮБ НБУВ / М. Іванова // Наукові праці Національної бібліотеки України ім. В. І. Вернадського. – 2015. – Вип. 41. – С. 441– 454.

3. Право інтелектуальної власності: навчальний посібник / Еннан Р. Є., Кулініч О. О., Мазуренко С. В., Менсо І. В., Романдзе Л. Д. – К. : Алерта, 2016. – 492 с.

4. Марущак А. І. Цивільні права на інформацію / А. І. Марущак [Електронний ресурс] // Юридичний вісник – 2009 – № 3 – С. 33–36. – Режим доступу:

http://law.nau.edu.ua/images/Nauka/Naukovij_jurnal/2009/statji_n3_12_2009/Marushjak_33.pdf

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

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

АКТУАЛЬНІ ПІДХОДИ ЩОДО СТВОРЕННЯ ВИЩОГО СУДУ З ПИТАНЬ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УКРАЇНІ

У різних країнах світу, до якої б системи права не належала країна, чи не найважливіша увага приділяється судовій практиці у сфері інтелектуальної власності.

Судова практика з питань захисту прав інтелектуальної власності має в Україні свою національну історію.

В рамках визначеної теми спробуємо прослідкувати а також проаналізувати теоретичні і практичні аспекти формування спеціалізованого суду з розгляду спорів у сфері інтелектуальної власності.

1 червня 2016 року було схвалено Концепцію реформування державної системи правової охорони інтелектуальної власності в Україні [1].

2 червня 2016 року прийнято зміни до Конституції України в частині правосуддя, цією ж датою (2 червня 2016 року) прийнято новий Закон України «Про судоустрій і статус суддів» [2]. Цей Закон передбачає створення вищих спеціалізованих судів (Вищого суду з питань інтелектуальної власності та Вищого антикорупційного суду).

Слід зазначити, що до аналізу перспектив створення в Україні суду з питань інтелектуальної власності (патентного суду) долучилося багато науковців, вчених різних галузей права, а також практики України та

зарубіжні практики-юристи. Зокрема: Г.Андрощук, Д.Притика, Г.Добриніна, О.Дорошенко, С. Пархомчук, В.Орлова. Деякі з них досить ґрунтовно дослідили особливості і правові підстави створення патентного (інтелектуального) суду.

Найбільшою причиною замислення і пошуків шляхів вдосконалення вже існуючої практики в Українських судах є саме недоліки у сфері судового захисту прав інтелектуальної власності.

Відомо, що в Україні, система правової охорони інтелектуальної власності формувалася за європейським зразком.

З того часу, як було створено Держпатент України і Державне агентство України з авторських і суміжних прав, пройшло 25 років, протягом яких постійно відбувалися зміни (чергові, так звані, реформи). Поряд із Держпатентом було створено Державне підприємство «Інститут промислової власності». У 2000 році на базі цих інституцій було створено Український інститут промислової власності. Указом Президента України «Про оптимізацію системи центральних органів виконавчої влади» № 1085/2010 від 9 грудня 2010 року було створено Державну службу інтелектуальної власності – центральний орган виконавчої влади, до сфери управління якої було передано Український інститут промислової власності. Тоді так само підкреслювалось важливість реформи у сфері інтелектуальної власності. Але час показав, що реалізація державної політики у цій сфері вимагала прийняття чисельних змін до законодавства задля продовження процесу реєстрації прав на об'єкти інтелектуальної власності. До того ж, реформа була причиною відтоку з цієї сфери висококваліфікованих фахівців.

І ось, реформа 2016 року знов спіткала систему правової охорони інтелектуальної власності. Тепер Державну службу інтелектуальної власності України ліквідовують, а всі її повноваження переходять до Міністерства економічного розвитку і торгівлі (Мінекономрозвитку) України і при цьому створюється Вищий суду з питань інтелектуальної власності в Україні.

Але реформа для реформи, щоб зробити щось на зразок Американської моделі для України не потрібна. На думку багатьох дослідників в такій складній і важливій сфері як інтелектуальна власність слід починати з напрацювання дієвого законодавства. І в першу чергу, для цього вкрай необхідно розробити і прийняти окремий процесуальний закон, на підставі якого має здійснюватись правосуддя у спорах з питань інтелектуальної власності.

Без сумніву можна сказати, що ідея створення Вищого суду з питань інтелектуальної власності в Україні, принаймні, створення патентного суду, досить не нова. У цьому напрямі було зроблено не мало.

У 2000 році було сформовано Судову палату Вищого господарського суду України з розгляду справ у господарських спорах, пов'язаних із захистом права на об'єкти інтелектуальної власності. Відповідно було створено колегії у складі місцевих та апеляційних господарських судів.

Указом Президента України від 27 квітня 2001 року Кабінету міністрів України було доручено вивчити питання щодо створення спеціалізованого патентного суду [3].

Ще в одному Указі Президента України «Про Основні напрями конкурентної політики на 2002–2004 роки» від 19 листопада 2001 року, аналогічно міститься вказівка Кабінету Міністрів України, міністерствам, іншим центральним органам виконавчої влади всебічно вивчити питання про доцільність створення спеціалізованого конкурентно-патентного суду.

Теза про необхідність створення спеціалізованого суду міститься у Концепції розвитку державної системи правової охорони інтелектуальної власності на 2009–2014 роки.

Ще більшим поштовхом до такого аналізу, безумовно, стало і створення суду з інтелектуальної власності в Російській Федерації де такий судовий орган почав діяти в межах системи арбітражних судів з першого січня 2013 року. Спеціалізовані суди з інтелектуальної власності існують у

багатьох інших державах, зокрема, Австрії, Німеччині, Великобританії, Швейцарії.

Однак, думки фахівців у цій сфері і науковців-дослідників щодо необхідності створення спеціалізованого суду розділилися. Деякі з них вказують на недоцільність створення судових органів інтелектуальної юрисдикції і пояснюють це тим, що кількість судових спорів у сфері інтелектуальної власності не настільки необ'ємна, щоб створювати окремий суд. Аргументами цих дослідників і фахівців-практиків є те, що на сьогодні у національній правовій системі суди вирішують усі категорії спорів, зокрема і ті що стосуються всіх без виключення об'єктів інтелектуальної власності. При цьому зауважується важливість такого органу, як Апеляційна палата Державної служби інтелектуальної власності, яка здійснює адміністративний захист прав інтелектуальної власності в Україні. Виходячи з цього підкреслюється комплексність і багатоаспектність захисту. Тобто, у будь який час при адміністративному розгляді спорів з питань інтелектуальної власності заінтересована особа може звернутися за захистом свого права до судових органів. Є і інші аргументи, що вважаються цією частиною дослідників переконливими.

Друга частина вчених та практиків-дослідників вказує на необхідність запровадження розгалуженої системи спеціалізованих судів що дасть можливість вирішувати практично всі спори, що виникають у сфері інтелектуальної власності. Адже в системі юрисдикції на сьогодні багато заплутаності.

Навіть судді погоджуються, що спори у сфері інтелектуальної власності традиційно належать до одних із найбільш складніших. **Складність у розгляді справ у сфері інтелектуальної власності полягає ще й у тому, що слід захищати не тільки ідеї, але і фактичну форму, в якій вони передаються, тобто – особисте немайнове право автора.** Рішення у таких справах доволі часто скасовуються або переглядаються судами вищих

інстанцій та й розглядаються такі справи довго і часто не якісно. При цьому, в першу чергу страждають сторони у процесі.

І постає головне питання, а чи відбудеться забезпечення прав і свобод людини і громадянина у результаті цієї реформи?

У цьому зв'язку не можна не згадати судову реформу 2010 року. Доречи, одним із важливих етапів судової реформи 2010 року стало створення нового органу судової влади – Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ. Однак хочеться підкреслити, що вже тоді було погіршено ситуацію з доступом людей до правосуддя та було закладено низку загроз незалежності суддів.

Прийнятий другого червня 2016 року Закон України «Про судоустрій і статус суддів», знов залишає багато питань без відповіді, а деякі з фахівців вказують на перспективу і подальшої заплутаності в системі юрисдикції з таким підходом.

Зокрема, постає питання чи будуть розглядатись порушення авторських і суміжних прав. На сьогодні в судах таких справ на порядок більше ніж тих, що стосуються порушень патентних прав.

Також багато питань до статусу суддів. Якщо аналізувати майбутній **суддівський корпус то слід** порівняти статті 33 і 28 нового Закону. Зокрема ст.33 визначає вимоги щодо суддів спеціалізованого суду з питань інтелектуальної власності, а стаття 28 - щодо суддів апеляційного суду. Питання виникає щодо професійної діяльності у справах інтелектуальної власності.

Дивним видається й те, що Закон не зобов'язує суддів Вищого суду з питань інтелектуальної власності мати або отримувати додатково технічну освіту. Це значить, що як і раніше, потрібно буде проводити судові експертизи в кожній справі.

Адже відомо, що суддя, який розглядає спір у сфері інтелектуальної власності, змушений, по-перше вирішувати суто правові питання (про наявність або відсутність права, факту правопорушення, розміру заподіяння

шкоди тощо) і, по-друге, йому необхідно також досліджувати технічні аспекти, що належать до предмета доказування (наприклад, питання рівня техніки, сукупності ознак винаходу за патентом, застосування сукупності суттєвих ознак промислового зразка тощо). У такому випадку не можна обійтись без призначена судової експертизи об'єктів інтелектуальної власності.

Однак судова експертиза у більшості впливає на тривалість (затягування) розгляду справи. Доволі часто трапляється неоднозначність висновків судових експертиз (що пояснюється, як стверджують, знову ж таки фахівці, відсутністю єдиних методологічних засад. То ж, мабуть призначення експертиз при розгляді спорів у сфері інтелектуальної власності не повинно бути панацеєю.

Якщо ж звернутися до досвіду іноземних держав: практично у всіх патентних судах багатьох країн вимога технічної освіти існує. Наприклад, в Німеччині до складу суддівського корпусу Федерального патентного суду входять так звані «технічні судді» (*technische Richter*), які мають технічну і юридичну освіту. Судді патентних судів Великобританії та Швейцарії також повинні мати дві освіти: юридичну і технічну [4].

То ж і українському судді спеціалізованому суду з питань інтелектуальної власності технічна освіта була б доцільною і логічною.

Отже, якщо погоджуватися з баченням окремих дослідників з цього питання, які вважають актуальним створення спеціалізованого суду з питань інтелектуальної власності, як окремої ланки в судовій системі, на нашу думку, слід продовжувати пошуки нових шляхів у напрямку підвищення рівня захисту прав інтелектуальної власності.

При цьому слід вдосконалювати існуючі напрацювання в судовій практиці, особливо щодо захисту авторського і суміжних прав у мережі Інтернет, де найбільше проблем. Практика спеціалізованого суду повинна сформувати єдиний уніфікований підхід у вирішенні справ щодо захисту прав інтелектуальної власності.

Список використаних джерел:

1. Див.: Розпорядження Кабінету Міністрів України від 1 червня 2016 р. № 402-р. Про схвалення Концепції реформування державної системи правової охорони інтелектуальної власності в Україні – [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/402-2016-%D1%80/print1475258232108180>
2. Закон України «Про судоустрій і статус суддів» . – [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/1402-19>
3. Див.: Указ Президента від 27.04.2001 Про заходи щодо охорони інтелектуальної власності в Україні – [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/285/2001>
4. Марія Коваль Чим буде корисний Вищий суд з питань інтелектуальної власності. Українські перспективи та досвід іноземних держав. – [Електронний ресурс]. – Режим доступу: <http://forbes.net.ua/ua/opinions/1419572-chim-bude-korisnij-vishchij-sud-z-pitan-intelektualnoyi-vlasnosti>

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

*Гоголь Б. М., доцент кафедри
публічного та приватного права
Київського університету імені Бориса
Грінченка, к.ю.н., доцент.*

**КОМЕРЦІЙНА ТАЄМНИЦЯ ТА КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ:
ОКРЕМІ ПРОБЛЕМИ СПІВВІДНОШЕННЯ**

В наш час інформація є товаром та об'єктом правовідносин, на що неодноразово звертали увагу в юридичній літературі [1, с. 3; 2 с. 5]. Деяка інформація має особливу комерційну цінність через невідомість її третім особам. Володільці такої комерційної інформації, яка не є загальновідомою, досить часто вживають значних заходів щодо збереження її секретності з метою використання інформації у підприємницькій діяльності або надання її іншим особам на платній основі. Відповідно вони не зацікавлені в тому, щоб така інформація була отримана іншими особами без їх згоди.

Дії третіх осіб, спрямовані на отримання секретної комерційної інформації поза волею її володільців, традиційно розглядаються як недобросовісна конкуренція та порушення прав інтелектуальної власності.

Так, відповідно до статті 39 Угоди про торговельні аспекти прав інтелектуальної власності (надалі – «**Угода ТРІПС**») при забезпеченні ефективного захисту проти недобросовісної конкуренції, як передбачено статтею 10-bis Паризької конвенції (1967), Члени повинні надавати захист нерозголошуваної інформації.

Також вказана стаття передбачає, що фізичні та юридичні особи повинні мати можливість перешкоджати тому, щоб інформація, яка законно знаходиться під їх контролем, розголошувалась, збиралась або використовувалась іншими особами без їхньої згоди у такий спосіб, який суперечить чесній комерційній практиці.

Національне законодавство України фактично містить два механізми охорони нерозкритої інформації, що має комерційну цінність, а саме: інститут комерційної таємниці як одного з об'єктів права інтелектуальної власності та інститут конфіденційної інформації як одного з видів інформації з обмеженим доступом.

Так, відповідно до статті 505 Цивільного кодексу України комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Вказане визначення комерційної таємниці відповідає критеріям охорони нерозголошуваної інформації, які закріплені у статті 39 Угоди ТРІПС.

Такими критеріями є:

1. секретність інформації;

2. комерційна цінність інформації;
3. вжиття володільцем інформації необхідних заходів з метою збереження її секретності.

Визначення комерційної таємниці також закріплено у Господарському кодексі України (надалі – «ГК України»).

Відповідно до статті 36 ГК України відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону.

Аналіз статті 505 ЦК України та статті 36 ГК України дає підстави стверджувати, що вказані нормативно-правові акти мають різні підходи до визначення комерційної таємниці, що негативно позначається на регулюванні цієї сфери суспільних відносин.

Тому ми вважаємо необхідною уніфікацію визначень комерційної таємниці, які містяться у ЦК України та ГК України. При цьому більш доцільним видається використання підходу до розуміння комерційної таємниці, який міститься у статті 39 Угоди ТРІПС та був втілений у статті 505 ЦК України.

Також можна стверджувати, що чинне законодавство України передбачає можливість охорони комерційно-цінної нерозкритої інформації в правовому режимі конфіденційності.

Так, відповідно до статті 20 Закону України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Згідно зі статтею 21 вказаного закону інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Схоже визначення конфіденційної інформації міститься у статті 7 Закону України «Про доступ до публічної інформації».

Отже, суб'єкти приватного права мають можливість обмежити доступ третіх осіб до належної їм комерційно-цінної нерозкритої інформації, охороняючи її в режимі конфіденційності.

В цьому аспекті слід зазначити, що Закон України «Про інформацію», який можна вважати системним нормативно-правовим актом в сфері правового регулювання інформаційних відносин, взагалі не згадує про такий вид нерозкритої інформації як комерційна таємниця. В свою чергу, ЦК України та ГК України не містять визначення такого виду охоронюваної інформації як конфіденційна інформація. Це ускладнює встановлення співвідношення юридичних категорій «комерційна таємниця» та «конфіденційна інформація» та прав, які виникають на той чи інший вид нерозкритої інформації.

На підставі аналізу положень статті 505 ЦК України, статті 36 ГК України та статті 21 Закону України «Про інформацію» можна дійти висновку, що поняття конфіденційної інформації є більш широким і включає в себе комерційну таємницю як нерозкрити інформацію, що має комерційну цінність, та інші види нерозкритої інформації, які не мають комерційної цінності.

Схожі погляди були висловлені в юридичній літературі. Так, С.Г. Гордієнко щодо співвідношення інформації, яка захищається за допомогою законодавства про інтелектуальну власність, та конфіденційної інформації зазначає: конфіденційна інформація не обов'язково є об'єктом

інтелектуальної власності, однак інформація, що захищена законодавством про інтелектуальну власність, може бути визнана конфіденційною [3, с. 234].

Підсумовуючи викладене, можна констатувати, що законодавство України в сфері охорони прав на комерційно-цінну інформацію є несистематизованим та суперечливим. Враховуючи зазначене, вважаємо доцільним закріплення в законодавстві України єдиної класифікації всіх видів інформації, які підлягають правовій охороні. Для цього доцільним є комплексне дослідження правового регулювання інформаційних відносин та відносин щодо об'єктів інтелектуальної власності.

Список використаних джерел:

1. Петров Є. В. Інформація як об'єкт цивільно-правових відносин : автореф. дис. на здобуття наук. ступеня канд. юрид. Наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / Є. В. Петров. – Харків, 2003. – 18 с.
2. Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в Україні: автореф. дис. на здобуття наук. ступеня доктора юрид. наук: спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / О.В.Кохановська. – К., 2006. – 34 с.
3. Конфіденційна інформація та "таємниці": їх співвідношення / С. Г. Гордієнко // Часопис Київського університету права. - 2013. - № 4. - С. 233-238.

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

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

БАНКІВСЬКИЙ КІБЕРПРОСТІР ЯК МІСЦЕ ВЧИНЕННЯ ЗЛОЧИНУ

Кримінальний кодекс України не містить поняття складу злочину, а також багатьох його складових, що не завжди сприяє однаковому розумінню цих кримінально-правових категорій, а тому важлива роль в їх тлумаченні належить теорії та практиці кримінального права. Це, зокрема, стосується такої ознаки об'єктивної сторони злочину, як «місце вчинення злочину».

Загальноновизнано, що поняття «місце» означає певну територію, точку, пункт, площину, в якій або на якій щось відбувається [1, с. 662]. Виходячи з цього, в юридичних виданнях зазначається, що місце – це визначена територія, яка описана в диспозиції кримінально-правової норми, на якій було вчинено суспільно небезпечне діяння чи настав злочинний результат [2, с. 434].

У більш широкій інтерпретації під місцем вчинення злочину вважається територія, інше місце, яке характеризується фізичними, соціальними і правовими критеріями, де було розпочато, продовжено чи припинено злочинне діяння [3, с. 133].

Думається, що вказані визначення хоча й можуть задовольняти прикладне поняття місця вчинення злочину, проте у певних випадках вони будуть залишатися дещо «вузькими», оскільки лише поняття території замало для характеристики деяких видів злочинної поведінки, а запропоноване визначення – «інше місце, яке характеризується фізичними, соціальними і правовими критеріями», на наш погляд, не завжди виглядає предметним.

І хоча кримінальний закон пов'язує вчинення злочину з «територією України» або іншою територією «поза межами України» чи «за межами України» (статті 6-10 Кримінального кодексу України), можна визнати не парадоксальним, а навпаки обґрунтованим те, що у навчальній і науковій літературі цей підхід щодо дії кримінального закону усталено визначається як чинність закону про кримінальну відповідальність у *просторі* (курсив наш – В.М.).

Отже, місце вчинення злочину – це місце у просторі, де було розпочато, закінчено злочин, або де настав його злочинний наслідок. У контексті предмета нашого розгляду поняттю «простір» належить предикатне значення, яке в абстрактно-теоретичному вигляді воно сформульовано як об'єктивна реальність. Цілком обґрунтованим вдається те, що визначення місця вчинення злочину необхідно для встановлення меж дії

кримінального закону, в тому числі щодо діянь, обумовлених сучасним науково-технічним прогресом.

Зокрема про зв'язок теоретичного та практичного аспектів визначення місця вчинення злочинів, які пов'язані з використанням електронно-обчислювальної техніки, можуть свідчити типові приклади посягань на власність, предметом яких стають грошові кошти, що знаходяться у такій розвинутій ланці сучасної банківської системи, як мережа банкоматів.

Так, у судовій практиці існують різні підходи, пов'язані із визначенням місця вчинення вказаних злочинів, зокрема коли винний, протиправно заволодівши банківською платіжною картою потерпілого, викрадає через банкомат його грошові кошти. При цьому дії винного нерідко кваліфікують за ч. 3 ст. 185 Кримінального кодексу України як крадіжку з проникненням у сховище. Тобто в даному випадку досудове слідство та суд визнають місцем вчинення злочину розташування банкомату відповідної банківської установи.

Разом з цим, у судовій практиці така позиція судів щодо визначення місця вчинення даного злочину не завжди визнається обґрунтованою з наступних підстав. Банкомат – це програмно-технічний комплекс, призначений для здійснення операцій з одержання коштів у готівковій формі, а також виконання інших операцій (оплата товарів, послуг). Грошові купюри в банкоматі розміщуються в касетах, що містяться у спеціальному сейфі, а отже банкомат за кримінально-правовим визначенням дійсно є сховищем для грошей [4].

Проте якщо винний, отримавши у неправомірний спосіб банківську платіжну картку, користуючись нею, викрадає з банкомату чужі кошти, він фактично не здійснює проникнення ані у сховище банківської установи, ані в інше сховище, яким є банкомат. Адже користуючись такою банківською платіжною картою та проводячи відповідні маніпуляції з клавіатурою цього комплексу, він отримує доступ не до сейфового відділення банкомату, а зв'язується з операційною системою банку-емітента, а отже отримує доступ до рахунку потерпілого. Таким чином фізичного проникнення до сховища

(сейфу банкомату) не відбувається, оскільки отримання готівки при її викраданні полягає у списанні коштів з банківського рахунку в банківській установі, а не в місці розташування банкомату.

Вказаний висновок має принципове значення для правильної кваліфікації вказаних злочинів, оскільки розглянута крадіжка за своїм способом та місцем не може вважатися поєднаною з проникненням у сховище.

Таким чином, використання засобів електронно-обчислювальної техніки, пов'язане з різними системами суспільних відносин (економічними, банківськими, фінансовими, торговельними тощо), засвідчує необхідність врахування сучасних технологій та особливостей їх функціонування в кібернетичному просторі при оцінці відповідної злочинної поведінки та запобігання помилок при застосуванні кримінально-правових норм.

Список використаних джерел:

1. Новий тлумачний словник української мови. У чотирьох томах. 42 тисячі слів. Том 2. – Київ : «Аконіт», 1998. – 910 с.
2. Энциклопедия уголовного права. Т. 4. Состав преступления. – Издание профессора Малинина, СПб., 2005. – 798 с.
3. Мороз В. Г. Поняття місця вчинення злочину як ознаки об'єктивної сторони злочину // Юридична наука. – 2014. – № 5. – С. 122-136.
4. Про платіжні системи та переказ коштів в Україні. – Закон України від 5 квітня 2001 року [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2346-14>.

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

*Кириленко О. Г., заввідділу НБУВ,
к.і.н., доцент.*

*Литвинова Л. А., науковий
співробітник НБУВ, кандидат наук із
соц. комунікацій.*

ВІДКРИТИЙ ДОСТУП ДО ЗНАНЬ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ В КОНТЕКСТІ ГААЗСЬКОЇ ДЕКЛАРАЦІЇ

Однією з найбільш важливих тем для обговорення серед наукової спільноти є відкритий доступ до результатів наукових досліджень в умовах розвитку інформаційного суспільства. За версією всесвітньо відомого наукового видання Nature це одне з п'яти найважливіших наукових подій останнього десятиліття. Тому громадська підтримка відкритого доступу до результатів наукових досліджень проголошена в міжнародних політичних заявах, відкритих до приєднання (Будапештська ініціатива «Відкритий доступ», Заява в Бетезді про публікації відкритого доступу, Берлінська декларація про Відкритий доступ до наукових та гуманітарних знань, декларація Міжнародної бібліотечної федерації (IFLA) «Відкритий доступ до наукової літератури та дослідницької документації», Сальвадорська декларація «Відкритий доступ: з точки зору світу, що розвивається», Бангалорська декларація з національної політики відкритого доступу для країн, що розвиваються, «Петиція за гарантований доступ до результатів наукових досліджень, виконаних за рахунок коштів держбюджету» Євросоюзу і т.д.).

Термін «відкритий доступ» вперше був згаданий на Будапештській конференції з відкритого доступу (Budapest Open Access Initiative, www.budapestopenaccessinitiative.org) в лютому 2002 р. З того часу його сенс практично не змінився: Open Access визначається як безкоштовний (free), оперативний (immediate), постійний (permanent), повнотекстовий (fulltext), онлайнний (online) доступ до наукових публікацій.

Новий підхід до виявлення знань має вирішальне значення в той час, коли суспільству загрожує великий потік даних. Цифровий всесвіт або дані, які ми створюємо і копіюємо подвоюється кожні два роки і до 2020 року досягне 44 зеттабайт, або 44 трильйона гігабайт¹. Хоча переваги доступу до даних і використання методів, таких як інтелектуальний аналіз тексту і даних (TDM), отримали широке визнання, проте існують серйозні бар'єри, що перешкоджають в умовах інформаційного суспільства широкому доступу до знань. Ці проблеми включають в себе відсутність правової визначеності, обмежувальні ліцензії, що надаються видавцями, розрив в кваліфікації і відсутність інфраструктури.

Ця ситуація створила необхідність в узгодженні різних дисциплін і секторів щодо реальних переваг TDM. Потрібна стратегія для просування вперед з точки зору створення умов для реалізації цих вигод таким чином, щоб забезпечити позитивний соціальний вплив. «Швидко змінюється цифрове середовище, збільшується обчислювальна потужність і величезна кількість даних, які створюються, роблять необхідним для дослідників і суспільства можливість використовувати сучасні методи і інструменти, щоб допомогти їм робити нові відкриття. Дослідницька практика може бути революціонізована, і життя може бути буквально врятоване, якщо ми зможемо досягти кращого доступу до знань, що містяться у великих масивах даних», - підкрислила Кристина Хормия-Путанен, президент LIBER (Асоціації європейських дослідницьких бібліотек).

За ініціативою Асоціації європейських наукових бібліотек (LIBER) 25 світових експертів з різноманітних галузей зібралися 9-10 грудня 2014 року в Гаазі для підготовки колективної заяви, націленої на сприяння виявленню нових знань в епоху цифрових технологій шляхом використання інтелектуального аналізу тексту і даних (TDM). На їх переконання ця Декларація допоможе сформувати етичну дослідницьку практику,

прискорити законодавчу реформу і розробку політики та інфраструктури відкритого доступу. Серед них наступні фахівці з інтелектуальної власності:

Майя Богатай (Maja Bogataj Jančič) - генеральний директор і засновник Інституту інтелектуальної власності (IPI) в Люблянці (Словенія), що спеціалізується на авторському праві, інтернет-праві та інтелектуальній власності;

Люсі Гібо (Lucie Guibault) - доцент Інституту Інформаційного права (IViR) Амстердамського університету (UvA). Вона спеціалізується на міжнародному та порівняльному авторському праві та інтелектуальній власності;

Мелісса Хагеманн (Melissa Hagemann) - старший програмний менеджер в Інформаційній програмі відкритого суспільства, де вона очолює ініціативи відкритого доступу до наукових досліджень та відкритим освітнім ресурсам. Вона брала участь у розвитку рухів «Відкритий доступ» і «Відкрита освіта», організувавши спільні зустрічі, які привели до Ініціативи Будапештського відкритого доступу (BOAI), рекомендацій BOAI 10;

Ігнасі Лабастіда (Ignasi Labastida) - кандидат фізико-математичних наук. На даний час очолює Управління з поширення знань і дослідницький відділ в CRAI (Бібліотека) Університету Барселони. Громадський лідер Creative Commons в Іспанії. Член робочої групи з авторського права LIBER і член Керівного комітету співтовариства ІТ-директорів LERU;

Ніл Річардс (Neil Richards) є визнаним в світі експертом з конфіденційності, першої поправки і інформаційного права. Його книга «Інтелектуальна конфіденційність» опублікована видавництвом Oxford University Press в 2014 році. Професор Річардс також є співкерівником конференції з міжнародного права конфіденційності в Вашингтонському університеті і Кембриджському університеті;

Алек Тарковськи (Alek Tarkowski) - директор Centrum Cyfrowe Projekt: Polska, однією з ключових організацій, яка виступає за реформу авторського права і відкриту політику. Громадський лідер Creative Commons в Польщі;

Пол Айріс (Paul Ayris) - директор з бібліотечних послуг в Університетському коледжі Лондону (UCL). Він також є співробітником з авторського права в UCL (University College London) і головою спільноти керівників інформаційних служб LERU (Ліга європейських дослідницьких бібліотек);

С'юзан Райлі (Susan Reilly) є виконавчим директором LIBER, де відповідає за інформаційно-пропагандистську діяльність в сферах TDM (інтелектуальний аналіз тексту і даних), відкритого доступу та авторського права. Працювала в проектах ЄС, що стосуються відкритого доступу, електронної науки і цифрових бібліотек;

Бенджамін Уайт (Benjamin White) - член Консультативного комітету ИФЛА з авторського права та інших правових питань (CLM). Керівник відділу інтелектуальної власності Британської бібліотеки Великобританії.

Після кількох місяців обговорення, консультацій, складання і переписування, Гаазьку декларацію з відкриття знань в епоху цифрових технологій (Hague Declaration on Knowledge Discovery in the Digital Age) Пол Айріс з Лондонського Університетського коледжу презентував в Брюсселі 6 травня 2015 року. Відкриття Декларації відбулося в день, коли Європейська комісія представила свою Стратегію єдиного цифрового ринку.

Декларація має зростаюче співтовариство прихильників і вже сьогодні до неї приєдналось 251 організацій і 659 приватних осіб, тому що вони також вважають, що інтелектуальна обробка даних може рятувати життя. Покращення лікування захворювань, відповіді на глобальні проблеми, такі як зміна клімату, і мільярди заощаджень уряду є одними з потенційних переваг, які можуть бути отримані, якщо уряди, бізнес і суспільство приймуть принципи, викладені у Гаазькій декларації. Декларація містить практичні рішення і визначає ключові області, які необхідно вирішити в даний час. Кінцева мета Декларації є усунення бар'єрів для доступу і аналізу даних, вироблених суспільством.

У преамбулі декларації представлено обставини і мотиви, що слугували підставою для її створення. Коротко їх можна сформулювати так: закони щодо охорони інтелектуальної власності створені задовго до винаходу інтернету обмежили можливості аналізу цифрового контенту, але під впливом інформаційних технологій, що змінюються, етика використання даних і інтелектуального аналізу контенту повинна розвиватися. Відкритий доступ до важливої інформації в сфері науки, економіки, соціального і культурного життя може допомогти: вирішенню глобальних проблем людства (наприклад, зміна клімату та епідемії); збільшенню темпів розвитку науки за допомогою нової інформації і зростанню ефективності досліджень; підвищенню прозорості діяльності урядів; розвитку інновацій та співпраці, розширенню впливу відкритої науки; створенню інструментів для освіти і дослідження і т.д.

В декларації сформульовано основні принципи відкритого доступу до наукових знань:

1. *Інтелектуальна власність створена не для регулювання вільного потоку фактів, даних і ідей, її основна мета - просування дослідницької діяльності.*
2. *У людей має бути свобода аналізувати і задовольняти дослідницький інтерес, не боячись контролю або наслідків.*
3. *Умови ліцензій та договорів не повинні обмежувати приватне використання фактів, даних і ідей.*
4. *Етичні норми під час використання технології аналізу даних необхідні для розвитку відповідно технологій, що змінюються.*
5. *Інноваційні та комерційні дослідження, що базуються на використанні фактів, даних і ідей, не повинні бути обмежені законом про інтелектуальну власність.*

В Гаазькій декларації викладено стратегічний план (Дорожня карта) втілення в життя її принципів, розписано конкретні кроки, які повинні робити дослідні організації, університети, комерційні компанії, бібліотеки в

даному напрямку. Так, університетам та дослідним організаціям запропоновано:

- гарантувати, захист інтелектуального аналізу контенту як методології дослідження;
- заохочувати тих, хто використовує нові технології (оголошувати подяку під час оцінки їх роботи);
- забезпечувати підтримку і розвиток інфраструктури для зберігання і надання доступу до публікацій, які можуть бути легально доступні для інтелектуального аналізу;
- надавати доступ до відповідної інфраструктури, щоб зробити доступними дослідницькі дані для інтелектуального аналізу контенту, де це законно та можливо з етичних міркувань;
- виступати за переваги інтелектуального аналізу контенту.

Гаазька декларація відкрита для всіх, вона вимагає кращого доступу до фактів, даних і ідей - в першу чергу через обов'язкове виключення авторського права для інтелектуального аналізу текстів і даних, в комерційних і некомерційних цілях. Вона є актуальною на сьогодні. Ось чому:

1. *Закон про захист авторських прав було розроблено в століття друкарського верстата і він більше не відповідає епосі цифрових технологій.* Потрібні закони з охорони інтелектуальної власності, які дозволяють читати не тільки людським оком, а й очима комп'ютерів.

2. *Поліпшення доступу до змісту (контенту) матиме численні вигоди для суспільства.* TDM (інтелектуальний аналіз тексту і даних) вже успішно використовується для різноманітних дослідницьких завдань: допомагає виявляти нові методи лікування захворювань, підвищувати прозорість уряду, виявляти тенденції в галузі культури і підвищувати ефективність бізнесу, покращуючи тим самим економіку і створення матеріальних благ.

3. *Реформа авторського права в даний час проводиться.*
Європейські політики обговорюють, як авторське право має змінитися.

Гаазька декларація закликає до поліпшення доступу до контенту, дослідники вже мають дозвіл на читання вручну - в першу чергу через обов'язкове виключення авторського права для текстів і інтелектуального аналізу даних в комерційних і некомерційних цілях. Плагіат як і раніше неприйнятний, як і видобуток конфіденційної інформації.

Організації та приватні особи, які бажають підтримати Декларацію, можуть додати свій підпис на офіційному сайті www.thehaguedeclaration.com. При цьому вони офіційно визнають величезний потенціал для відкриття знань, а також усвідомлюють, що необхідно вжити заходів, щоб кожен міг отримати вигоду з цього потенціалу. Підписання Гаазької декларації сьогодні є погодженням з тим, що поточний режим авторського права, непридатний для цифрової епохи і закликом до законодавців та політиків забезпечити правову визначеність, щоб інтелектуальний аналіз контенту не порушував авторських прав та суміжних прав. Це важливо для всіх, хто хоче поліпшити доступ до інформації і піклується про рішення великих проблем суспільства незалежно від того, чи є ви дослідником.

Список використаних джерел:

1. Data Growth, Business Opportunities, and the IT Imperatives. – [Електронний ресурс]. – Режим доступу:
<http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>

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

*Яременко О. І., завідувач кафедри
правових наук та філософії
Вінницького державного педагогічного
університету імені Михайла
Коцюбинського, кандидат наук з держ.
управління, доцент.*

ШКІДЛИВА ІНФОРМАЦІЯ В ЗМІСТІ ТВОРІВ ЯК ОБ'ЄКТІВ АВТОРСЬКОГО ПРАВА: ПРОБЛЕМА ПРАВОВОЇ ІДЕНТИФІКАЦІЇ

Розвиток інтелектуально-інформаційної сфери соціуму обумовлює необхідність подальшого вдосконалення нормативно - правового регулювання відносин інформаційної безпеки. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017, передбачає, що національними інтересами України в інформаційній сфері є життєво важливі інтереси особи, зокрема, захищеність від руйнівних інформаційно-психологічних впливів. Такі впливи можуть здійснюватися різними шляхами, одним із яких є створення та поширення творів, що містять шкідливу інформацію, у зв'язку з чим актуалізується науковий аналіз даної проблематики.

Метою статті є дослідження юридичних аспектів співвідношення понять «інформація» та «твір», а також проблеми правової ідентифікації шкідливої інформації в змісті творів, що є об'єктами авторського права.

Сучасна наука оперує значною кількістю визначень інформації, які базуються на різноманітних кваліфікаційних ознаках. В загальній теорії інформації найбільш поширеними є два підходи до цього феномену – атрибутивний та функціональний. Сутність атрибутивного підходу полягає в тому, що інформація вважається невід'ємною складовою матерії і вона проявляється у всіх об'єктах, явищах і процесах живої та неживої природи. Функціональний підхід передбачає, що інформація є результатом свідомої діяльності людини і в неживій природі не існує як така [1, с. 44].

Поліваріантність підходів до сутності інформації спостерігається і в юридичній науці та законодавчій практиці. В нормативно - правовому акті,

який покликаний виконувати системоутворюючу функцію в інформаційній сфері - Законі України «Про інформацію», вона визначається як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2]. Водночас, в законодавстві України містяться також інші визначення інформації. Белевцева В.В., проаналізувавши нормативні тлумачення, приходить до висновку, що поняття “інформація” зводиться до наступних предметних категорій: 1) інформація – це відомості про події та явища, що відбуваються у суспільстві, державі та у життєдіяльності окремих осіб; 2) інформація – це дані, які можуть зберігатися в будь-якій формі й вигляді; 3) інформація – це відомості, які є документованими або публічно оголошеними у порядку, встановленому законодавством; 4) інформація є об’єктом цивільних прав і відноситься до категорії нематеріальних благ; 5) джерелами інформації є передбачені та встановлені законом її носії: документи, інші носії інформації, які являють собою матеріальні об’єкти, що зберігають інформацію, повідомлення засобів масової інформації, публічні виступи [3, с. 8].

Сформульовані Белевцевою В.В. характеристики інформації базуються на методологічних засадах інформаційного права і є цілком обґрунтованими з позицій цієї науки. В той же час, вважаємо доцільним також здійснювати аналіз сутності інформації з використанням теоретичних та нормативних засад авторського права. На цій основі інформацію можна трактувати результат творчої діяльності людини в сфері літератури, мистецтва та науки. Такий підхід кореспондується із легітимним визначенням інформації, закріпленим в Законі України «Про захист економічної конкуренції», який розглядає її як відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп’ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості [4]. Ця нормативна дефініція

розширює коло джерел інформації та форм її об'єктивізації за рахунок включення результатів інтелектуальної творчої діяльності людини, які носять узагальнюючу назву «твори».

Слід зазначити, що легітимне визначення твору в нормативно – правових актах України відсутнє, хоча сам термін згадується неодноразово. Так, Цивільний кодекс України зазначає, що об'єктами авторського права є твори, і виділяє чотири їх види: літературні та художні твори, комп'ютерні програми, компіляції даних (бази даних) та інші твори [5]. Крім цього, Закон України «Про авторське право і суміжні права» виокремлює об'єкти, які хоча і є результатом інтелектуальної діяльності, але не охороняються авторським правом: повідомлення про новини дня або поточні події, що мають характер звичайної прес-інформації; фольклор; видані органами державної влади офіційні документи політичного, законодавчого, адміністративного характеру; розклади руху транспортних засобів, розклади телерадіопередач, телефонні довідники та інші аналогічні бази даних, що не відповідають критеріям оригінальності і на які поширюється право *sui-generis* (своєрідне право, право особливого роду) [6].

Поняття «інформація» і «твір» перебувають у складному діалектичному зв'язку, що знаходить свій прояв в кількох аспектах: по - перше, інформація і твори є результатом споріднених видів нематеріальної діяльності – інформаційно - інтелектуальної та творчо - інтелектуальної; по - друге, ці два об'єкти знаходяться в сфері правового регулювання двох близьких за природою видів суспільних відносин - інформаційних та авторських; по - третє, доволі часто форми об'єктивізації інформації співпадають з об'єктивною формою творів; по - четверте, процеси створення та обігу цих двох об'єктів базуються на принципах свободи, які закріплені на конституційному рівні; по - п'яте, обмеження свободи інформаційної та інтелектуальної діяльності мають спільну соціально - правову природу; по - шосте, основною сутнісною характеристикою твору є його зміст, тобто, інформація в художніх, мистецьких, наукових інтерпретаціях.

На доктринальному рівні відмінність інформації від твору проявляється в тому, що перша є результатом інтелектуальної діяльності, а другий – творчої. Однак, інформаційні відносини дуже близькі за своєю природою до відносин інтелектуальної власності і досить часто мають спільний об'єкт. Нормативне підтвердження цього знаходимо в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 роки», який передбачає прийняття Інформаційного кодексу України, із включенням до нього розділів про правову охорону прав на зміст комп'ютерних програм, удосконалення захисту прав інтелектуальної власності, в тому числі авторського права при розміщенні та використанні творів у мережі Інтернет, про охорону баз даних, комерційну таємницю тощо [7]. В той же час, комп'ютерні програми, бази даних, комерційна таємниця є об'єктами інтелектуальної власності і регулюються Цивільним кодексом України, законом України «Про авторські та суміжні права» та іншими нормативними актами в цій сфері.

Очевидно, що твір, як цілісне явище, так всі його складові, є нічим іншим як сукупністю інформації. При цьому, слід відрізнити інформацію про твір (персональні дані автора, відомості про вид і характер твору, його назва, опис тощо) та твір, як носій певної смислової інформації. Комунікаційна місія твору полягає в доведенні до невизначеного кола осіб інформації, в специфічній художній формі, створеній автором, а рівень його інформативності залежить від характеру, призначення, об'єму тощо.

Варто відзначити, що інформація, викладена в художньому творі, доволі часто сприймається і засвоюється споживачем краще, ніж інформація, що міститься в інших джерелах. Виготський Л.С. відзначав, що мистецтво втягує в коло соціального життя найінтимніші і найособистіші складники нашої істоти. Для цього мистецтво володіє значним арсеналом специфічних засобів, відсутніх в інших формах людської свідомості. Ідеологічні аспекти в художньому творі, будучи органічно вплетеними в тканину живих, зримих

художніх образів, впливають на свідомість людини непомітно, як і на розум, почуття, волю [8, с. 73].

Виходячи з високого рівня впливу змісту твору на свідомість, він може нести загрозу інформаційній безпеці суспільства та особи, якщо носить шкідливий характер. Наприклад, як зазначають сучасні дослідники, більшість кінематографічної продукції є не що інше, як відверта пропаганда хижості, насильства, аморальності. На перший погляд у багатьох фільмах міститься явна критика агресивності, яка, однак, до добра ніяк не доводить. Але насправді під виглядом нібито боротьби з насильством на екранах з'являються типові, відверто хижі агітки. «Наймасовіше» мистецтво сильно знижує реальний імунітет людей до сприйняття справжніх вбивств і насильства в суспільстві, що уявляється буденним явищем [9, с. 144].

В свою чергу, телебачення моделює наше ставлення до світу реального, пропонує інтелектуальні, емоційні й поведінкові зразки, певні стандарти, які тією чи іншою мірою керують людиною. Рекламу на телебаченні спотворює природне сприйняття екранного оповідання. Рекламодавців цікавлять, головним чином, механізми впливу на підсвідомість людини: реклама управляє, перш за все, емоційною поведінкою, що вислизає від розумного контролю [10, с. 328].

Усвідомлення законодавцем шкоди, яку наносить зміст аудіовізуальних творів інформаційній безпеці, знайшло прояв в Законі України «Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України». Згідно з цим законом, в Україні забороняється розповсюдження і демонстрування фільмів, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що створюють позитивний образ працівників держави-агресора, працівників радянських органів державної безпеки, виправдовують чи визнають правомірною окупацію території України [11].

Водночас, ці заходи захисту від шкідливих творів є фрагментарними. Однією із ключових проблем в цій сфері є складності в ідентифікації

шкідливості інформації, що становить зміст твору. В юридичній науці пропонується шкідливу інформацію визначати як інформацію, що посягає на життєво важливі інтереси особи, суспільства і держави, характер і ступінь суспільної небезпеки якої обумовлюють необхідність ухвалення державою таких заходів, які б забезпечували належний правовий захист від втрат, що завдаються цим суб'єктам у результаті її розповсюдження [12, с. 9].

Законодавче регулювання відносин, щодо заборони обігу шкідливої інформації базується на нормах ст. 34 Конституції України, яка проголошуючи право на свободу інформації, встановлює, що здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Також, ст. 54 Конституції України гарантує громадянам свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності. Із формулювання даної конституційної норми можна зробити висновок про те, що законодавець не передбачив заборон щодо поширення шкідливої інформації в таких об'єктах як твори. Частково компенсується цей недолік заборonoю поширювати шкідливу інформацію в об'єктах із збірною назвою «продукція». Так, згідно із Законом України «Про захист суспільної моралі» забороняються виробництво та розповсюдження ряд шкідливої продукції, змістовну частину якої складає пропаганда війни, фашизму та неофашизму, бузувірства, блюзнірства, неповагу до національних і релігійних святинь, національної та релігійної ворожнечі тощо. Під продукцією розуміються як матеріальні, так і нематеріальні об'єкти - предмети, друкована, аудіо-, відеопродукція, реклама, повідомлення та

матеріали, продукція засобів друкованих та електронних засобів масової інформації. Водночас, в Кримінальному кодексі України, який встановлює відповідальність за такі ці діяння застосовується різні терміни – «матеріали», «твори», «заклики».

Таким чином, аналіз інформаційного законодавства та законодавства в сфері інтелектуальної власності свідчить про наявність суттєвих пробілів в питаннях ідентифікації шкідливої інформації в змісті творів, що є об'єктами авторського права. В Україні відсутні чіткі нормативні критерії для віднесення інформації до категорії шкідливої і мають місце проблеми у врегулюванні питань співвідношення свободи творчості та її законодавчого обмеження. Доктринально законодавство України спрямовано на захист особистих та майнових прав автора, в той час, як право споживачів інформації на захист від шкідливого контенту творів потребує детальнішого врегулювання.

Список використаних джерел:

1. Философские и научно-методологические проблемы современной информатики / К.К Колин // Открытое образование. – 2007. – № 3 (62). – С. 43- 51.
2. Про внесення змін до Закону України "Про інформацію": Закон України від 13 січня 2011 року N 2938-VI. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2938-17>.
3. Белєвцева В.В. Теоретико-правові підходи до визначення поняття "інформація" через інформаційні правовідносини / В. В. Белєвцева // Інформація і право. – 2015. – № 3. – С. 5 - 10.
4. Про захист економічної конкуренції: Закон України від 11.01.2001 № 2210-III. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2210-14>.
5. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. – Режим доступу <http://zakon3.rada.gov.ua/laws/show/435-15>.
6. Бондаренко С.В. Авторське право та суміжні права /С.В. Бондаренко. – К.: Ін-т інтел. власн. і права, 2008. – 288 с.
7. Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015: Закон України від 9 січня 2007 року N 537-V // Відомості Верховної Ради України. – 2007. – № 12. – ст. 102.

8. Культурологія. Українська та зарубіжна культура: навч. пос. / М.М. Закович, І.А. Зязюн, О.М. Семашко, О.Л. Шевнюк, Ж.О. Безвершук та ін. – 4-те вид., виправл. і доп. – Київ : Знання, 2009. – 592 с.

9. Дзьобань О.П. Інформаційне насильство: змістовний аспект / О.П. Дзьобань, О. Ю. Панфілов, С. М. Соболева // Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія. – 2016. – № 1. – С. 136-151.

10. Сащук Г. М. Інформаційне насильство в сучасному суспільстві / Г. М. Сащук // Гілея: науковий вісник. – 2016. – Вип. 111. – С. 326-329.

11. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України // Відомості Верховної Ради України. – 2015. – № 18. – ст.131.

12. Лисенко О.О. Правовий захист суспільства від шкідливої інформації: автореф. дис. канд. юрид. наук: 12.00.07 / О. О. Лисенко; Харк. нац. ун-т внутр. справ. – Х., 2011. – 20 с.

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

*Троцька В. М., завідувач сектору
суміжних прав відділу авторського
права і суміжних прав НДІ
інтелектуальної власності НАПрН
України.*

ВІЛЬНЕ ВИКОРИСТАННЯ ТВОРІВ ДЛЯ НАВЧАННЯ

Викладання навчальних предметів в освітніх закладах та отримання освіти будь-якою особою нерозривно пов'язане з використанням існуючих знань, умінь та навичок, опрацюванням матеріалу, що часто містить або є об'єктом авторського права. Поряд з тим, конституційним правом кожного громадянина є право на результати його інтелектуальної, творчої діяльності, ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом. Відповідно до ч. 1 ст. 32 Закону України «Про авторське право і суміжні права» (далі – Закон) автору та іншій особі, яка має авторське право, належить виключне право надавати іншим особам дозвіл на використання твору будь-яким одним або всіма відомими способами на підставі договору. В міжнародному та національному законодавстві передбачені винятки та обмеження з вказаних майнових прав суб'єктів авторського права, згідно з якими дозволяється вільне використання творів з

метою навчання, що сприяє безперешкодному доступі до творів з ціллю отримання інформації та знань. Таким чином створюється баланс між правами та інтересами творчих осіб, з одного боку, і правами та інтересами суспільства на освіту, з іншого.

Так, відповідно до ст. 21-25 Закону встановлені випадки вільного використання творів, коли дозволяється таке використання без дозволу суб'єктів авторського права і без виплати їм винагороди, з дотриманням відповідних умов. Зокрема, до таких випадків належить використання творів з метою навчання. З огляду на допустимість використання творів з вказаною метою, серед користувачів існує припущення, що будь-яке використання твору для навчання є вільним від виконання будь-яких формальностей, таких як укладання договору, виплати авторської винагороди. Проте, як засвідчує аналіз норм Закону та практики їх застосування, це не так.

Вільне використання творів дозволяється у випадках спеціально визначених Законом та при обов'язковому дотриманні відповідних умов. За приписами ст. 21, ст. 23 Закону без згоди автора (чи іншої особи, яка має авторське право), але з обов'язковим зазначенням імені автора і джерела запозичення дозволяється використання літературних і художніх творів в обсязі, виправданому поставленою метою, як ілюстрацій у виданнях, передачах мовлення, звукозаписах чи відеозаписах навчального характеру, а також відтворення уривків з опублікованих письмових творів, аудіовізуальних творів як ілюстрацій для навчання за умови, що обсяг такого відтворення відповідає зазначеній меті. Як бачимо правомірним вважається використання твору при дотриманні умов, а саме, якщо:

- 1) здійснюється використання твору з метою навчання та обсяг такого використання відповідає зазначеній меті;
- 2) використовуються уривки з твору як ілюстрації;
- 3) зазначається ім'я автора і джерело запозичення твору.

Та навіть при дотриманні перелічених умов додатково пересвідчитися чи використання підпадає під «вільне» можливо за допомогою так званого

«трюхступневого тесту», передбаченого ч. 6 ст. 15 Закону, а саме: обмеження майнових прав, встановлені ст. 21-25 Закону, здійснюються за умови, що вони не завдаватимуть шкоди використанню твору і не обмежуватимуть безпідставно законні інтереси автора.

Отже, лише при дотриманні всіх перелічених умов та відповідності вказаному тесту, можливо стверджувати, що використання твору не потребує отримання дозволу від суб'єкта авторського права та виплати йому винагороди, тобто є вільним.

Розглянемо наведене на прикладі з судової практики.

Науково-дослідний інститут звернувся до суду з позовом до Університету про використання фрагменту «Посібника. Словника» при створенні Університетом видання «Архівознавство: навч. посіб. для дистанційного навчання» без дозволу інституту [1]. В ході судового розгляду справи була призначена судова експертиза, за висновками якої встановлено, що мало місце використання фрагментів текстів із Посібника, а творча праця Університету полягала у доопрацюванні фрагментів тексту (розділів) з Посібника шляхом доповнення відповідними розділами, тощо. Загальний обсяг використання фрагментів текстів становив близько 80% від загальної кількості сторінок Посібника. Твердження Університету про те, що «Посібник є навчальним виданням, яке використовується виключно для внутрішнього безкоштовного користування студентами Університету, які навчаються за дистанційною формою навчання... Видання Посібника ... передбачає не комерційну, а навчальну мету» було не взято до уваги, оскільки позивач надав докази комерційного використання видання (копія накладної з магазину, який одержав книгу «Архівознавство» за ціною 25,00 грн. за один примірник). Позивач в позовній заяві зазначив про виплату йому компенсації, виходячи з того, що загальний наклад видання складав 1300 примірників. Згідно з рішенням суду визначено стягнути з Університету 35 000 грн. компенсації за порушення авторського права та вилучити з продажу видання.

Отже, наведений приклад судової практики підтверджує, що правомірним вважатиметься використання твору з навчальною метою при дотриманні всіх умов вільного використання твору. Зокрема, розповсюдження твору з комерційною метою стало однією з підстав для визначення використання твору неправомірним.

Наступним випадком вільного використання творів для навчання є копіювання чи «репрографічне відтворення» творів навчальними закладами. Відповідно до ст. 23 Закону допускається без згоди автора, чи іншої особи, яка має авторське право, репрографічне відтворення навчальними закладами для аудиторних занять опублікованих статей та інших невеликих за обсягом творів, а також уривків з письмових творів з ілюстраціями або без них за умови, коли: а) обсяг такого відтворення відповідає зазначеній меті; б) відтворення твору є поодиноким випадком і не має систематичного характеру. Виходячи з наведених норм Закону, якщо наприклад, з метою викладання матеріалу на учбовому занятті викладач зробив копію твору за допомогою ксерокопіювального пристрою, то це підпадає під вільне використання такого твору. Якщо ж в навчальному закладі особа (організація-посередник) надає систематичні послуги по копіюванню творів, наприклад здійснює копіювання навчальних посібників (чи їх частин) для викладачів, студентів, та відповідно отримує платню за такі послуги, то даний випадок не належить до вільного використання.

Наприклад, судова справа Basic Books v. Kinko's Graphics Corp, що розглядалася в суді США [2]. Група видавництв звернулася до суду з позовом про порушення їх авторських прав у зв'язку з тим, що мережа копіювальних центрів здійснювала репрографічне відтворення частин їх книг та формувала збірники для університетів і розповсюджувала їх серед студентів. При захисті прав корпорація зазначала, що здійснювала це відповідно до доктрини «добросовісного використання», передбаченої Законом про авторське право США. Суд визнав копіювання порушенням авторського права, зобов'язавши виплатити видавництвам штраф у розмірі - 510000 дол. США. Одним з

доводів того, що копіювання частин книг не підпадає під «вільне» відтворення стало те, що воно здійснювалося хоч і для навчання, проте шляхом розповсюдження збірників з комерційною метою.

Таким чином, наявність інституту вільного використання творів в авторському праві дозволяє бездогвірне та безкоштовне використання творів з метою доступу до знань, інформації та культурного надбання, чим забезпечується баланс інтересів і прав авторів та суспільства. Водночас, як засвідчує іноземна та національна практика застосування норм законодавства, важливим аспектом є врахування всіх умов, при дотриманні яких дозволяється вільне використання творів з метою навчання.

Список використаних джерел:

1. Рішення Господарського суду міста Києва від 16.01.2009 р. у справі №21/436. URL: <http://jurportal.org/writ/5129568>.
2. Basic Books, Inc. v. Kinko's Graphics Corp. URL: <https://www.copyright.gov/fair-use/summaries/basicbooks-kinko%27s-sdny1991.pdf>

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

Іванов Д. В., аспірант Міжрегіональної Академії управління персоналом.

ЗАВДАННЯ СУСПІЛЬНОГО МОВНИКА УКРАЇНИ У ЧАСИ ПОСТ-ПРАВДИ ТА В УМОВАХ ЗАТЯЖНОЇ АТО

Суспільний мовник України, як інструмент реалізації концепції суспільного мовлення, нині лише формує свою діяльність, експериментуючи з різним контентом, намагаючись знайти рецепт на рентабельність власної продукції та утримавшись від її комерціалізації. Зважаючи на еластичність концепції суспільного мовлення (наявність у ній не тільки сталих незмінних рис, але і змінних елементів, серед яких у тому числі завдання, що ставить держава у особі парламенту України перед організацією, що реалізує концепцію суспільного мовлення) слід зауважити, що особливий стан у державі має впливати на програмну політику організації суспільного мовлення.

На початку XX ст. під час страйків у Англії суспільний мовник Бі-Бі-Сі взяв на себе місію щодо примирення ситуації, сприяння громадянській злагоді задля національних інтересів.

Сьогодні у світлі тих змін, які впровадила у концепцію суспільного мовлення Рада Європи, відстоювання виключно національних інтересів недостатньо. Якщо виходити виключно з принципу відстоювання національних інтересів, то почнуть говорити про те, що Russia Today займається реалізацією концепції суспільного мовлення (що невірно і з інших причин). Рада Європи вже давно відійшла від національно-орієнтованого розуміння концепції суспільного мовлення. Наприклад, у Рекомендації 748 ПАРЄ 1975 року мова йде про національне мовлення, тоді як вже десятиріччям пізніше вживається виключно термін суспільне мовлення.

Відхід від національно-орієнтованої моделі і акцент на суспільному, не забарвленому так яскраво у націоналістичні кольори, пояснюється цінностями, які пропагує Рада Європи і які знаходимо у актах ООН, ЄС щодо прав та свобод людини, заборони дискримінації, толерантності тощо.

У цьому контексті доречним є переосмислення ролі діяльності організації суспільного телебачення і радіомовлення в Україні під час проведення затяжної антитерористичної операції. Комерційні мовники, що нині роблять акцент на стимулювання національної ідентичності, чіткому розподілі ролей на ворогів і друзів, своїх і чужих, підтримують державну політику актуально для часу ведення бойових дій. Зважаючи на наведене щодо політики Ради Європи у питанні концепції суспільного мовлення, видається некоректною роль суспільного, яке наслідують комерційних мовників у цьому питанні.

Необхідним є переосмислення не тільки ролі суспільного мовника у реалізації державного замовлення (визначених законодавством завдань суспільного мовлення), але і розуміння того, чим є концепція суспільного мовлення і як вона має бути реалізована в Україні.

Водночас державне замовлення передбачає і свободу редакційної політики – законодавець ставить завдання, а організація суспільного мовлення сама визначає як ці завдання реалізувати. Якщо говорити про бойові дії, то рішення щодо переосмислення діяльності мають впливати з такої парадигми, відповідно до якої кожній людині потрібно знати життєво-важливу інформацію, якої не дає комерційний мовник, проте яка впливає з концепції суспільного мовлення. За таких умов у програмах суспільного мовлення акцент має ставитися на просвітництві, а темами такого просвітництва мають слугувати: надання першої медичної допомоги, робота організму людини, анатомія і фізіологія, ознаки інформаційного протиборства у медіа, медіа-грамотності, правова-грамотність в умовах ведення у державі бойових дій тощо.

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

Николаєнко Г. В., аспірант, Науково-дослідний інститут інформатики і права НАПрН України.

РОЛЬ ЗАКОНОДАВСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ В РОЗВИТКУ ДЕРЖАВНОЇ СТАТИСТИКИ УКРАЇНИ

Активний процес гармонізації та адаптації національної правової системи до європейських стандартів зумовлює кардинальні зміни у методологічних підходах до побудови статистичної системи України, що дає змогу розглядати її в якості важливої складової європейської статистики. Наша країна поки не є членом Європейського Союзу і нормативні документи стосовно функціонування системи його статистики не є обов'язковими для застосування в національній статистичній практиці. Тим не менш, з огляду на стратегічну перспективу членства у Європейському Співтоваристві та необхідність отримання інформації для міжнародних порівнянь, цілком очевидно є необхідність адаптації європейських статистичних стандартів до національних умов.

На сьогодні законодавство України, що регулює державну статистичну діяльність є значно менш деталізованим і формалізованим, ніж законодавство Європейського Союзу. Найбільш суттєву роль у наближенні національної статистичної системи до міжнародних стандартів відіграв прийнятий у 1992 році Закон України «Про державну статистику». Нова редакція базового законодавчого акту досить суттєво відрізняється від Закону 1992 року як за змістом, так і за формою викладення. Він має на меті не лише регулювання правових відносин в галузі державної статистики, але також й визначення прав і функцій органів державної статистики, організаційних засад здійснення державної статистичної діяльності і, що найбільш важливо, – це приведення його основних статей до законодавчих вимог Європейського Союзу [1].

З огляду на потреби країн – учасниць Європейського Союзу статистична система розвивається у напрямку чотирьох чітко окреслених цілей: узгодження часу збору та підготовки даних; гармонізація методології показників; інтеграція з іншими частинами статистичної системи і, передусім, з системою національних рахунків; розширення сфери статистики підприємств за рахунок охоплення поряд із традиційними нових видів економічної діяльності (наприклад, сектору послуг) [2].

Гармонізація європейських статистичних даних проводилася спеціально створеним міждержавним органом – Євростатом. Серед основних завдань, що вирішуються Євростатом, можна виділити: розвиток норм та методів, що наближають статистику до базових принципів; забезпечення доступності статистики відповідно до означених принципів. В межах своєї компетенції Євростат відповідає за відбір наукових підходів, визначень та методології, що є найбільш придатними для забезпечення принципів та досягнення цілей, задекларованих основним законом.



Організація статистичних даних у цілому відповідає загальній офіційній моделі ієрархії законодавчих актів ЄС (Рис. 1).

Необхідно відзначити, що певний рівень уніфікації загальних принципів європейської статистики на рівні спільноти не заперечує наявність значних національних відмінностей між статистичними системами країн-учасниць. Тобто кожна національна статистична служба самостійно

Рис. 1. Модель ієрархії вирішує, у який спосіб вона забезпечить законодавчих актів ЄС виконання вимог Євростату. Ці відмінності обумовлюються національними історичними традиціями, економічними умовами, практикою функціонування адміністративної системи, масштабом країни, статусом офіційної статистики, рівнем її централізації тощо.

Базовим статистичним законом, на якому побудована статистична система Європейського Союзу, є Регламент Ради Європейської Комісії №322/97 від 17.02.1997р. Даний нормативний документ визначає основоположні принципи та задачі європейської статистики як єдиного цілого, що мусить задовольняти потреби ЄС в інформації щодо більшості аспектів їх соціально-економічного розвитку [3]. Під статистикою європейської спільноти розуміється кількісна, узагальнена і репрезентативна інформація, отримана на основі збору та систематичної обробки даних, які здійснюють відповідні національні установи та установи ЄС в межах впровадження Статистичної програми ЄС. Окремо виділяється виробництво статистики – це процес, що складається з усіх видів діяльності, необхідних для збору, збереження, обробки, синтезу, аналізу та розповсюдження статистичної інформації.

Спільна програма дій щодо створення системи європейської статистики має назву Статистичної програми Європейського Союзу [4]. Цей документ є робочими межами для виробництва всієї статистики ЄС і визначає підходи, основні сфери здійснення та цілі заходів, спрямованих на досягнення спільної мети. Правовий акт виділяє шість принципів якості статистики як у деонтологічному, так і професійному аспектах: безпристрасності, надійності, відповідності, ефективності витрат, статистичної конфіденційності та прозорості.

Виходячи з того, що основною метою офіційної статистики є задоволення потреб споживачів, документ окремо визначає порядок розповсюдження статистичної інформації. Під розповсюдженням розуміється діяльність статистичних установ щодо забезпечення доступності статистичних даних для користувачів. З огляду на значну кількість країн – учасниць ЄС та нерівномірність розвитку національних статистичних систем, значна увага приділяється застосуванню однакових принципів та оптимальної кількості стандартів.

В якості позитиву слід зазначити, що за результатами Адаптованої глобальної оцінки національної статистичної системи, проведеної представниками Європейської комісії, Європейської асоціації вільної торгівлі та Економічної комісії ООН для Європи, статистика України визнана такою, що значною мірою відповідає європейським вимогам, а інформація, що виробляється органами державної статистики, є продуктом високої якості у більшості галузей статистичного виробництва. Тому механізм запозичення європейського досвіду для регулювання відносин, пов'язаних з функціонуванням державної статистики в Україні має суттєве значення як для теорії, так і для практики. Разом з цим, потребує глибокого наукового аналізу та удосконалення наявна на сьогодні в Україні система суб'єктів адміністративно-правового регулювання державної статистики в Україні, яка носить досить розмитий характер. Під системою цих суб'єктів, на нашу думку доцільно вважати сукупність органів державної влади, які мають

повноваження щодо здійснення адміністративно-правового регулювання державної статистики з метою забезпечення збирання, опрацювання, аналізу, поширення, збереження, захисту та використання статистичної інформації.

Список використаних джерел:

1. Закон України «Про державну статистику»]. – [Електронний ресурс]. - Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2614-12>.
2. Methodology of industrial short-term indicators. (1996). 1st ed. Luxembourg: Office for Official Publications of the European Communities.
3. Офіційний вісник ЄС, L 87, с. 164-173. – [Електронний ресурс]. - Режим доступу: old.minjust.gov.ua/file/33143.
4. Legal texts relating to the European business statistical system. (1998). 1st ed. [S.l.]: Eurostat.

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