

Національна академія правових наук України
Науково-дослідний інститут інформатики і права

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

**ІНФОРМАЦІЙНЕ ПРАВО: СУЧАСНІ ВИКЛИКИ І НАПРЯМИ
РОЗВИТКУ**

МАТЕРІАЛИ ПЕРШОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

18 жовтня 2018 року

Київ-2018

УДК 34:004](06)

I-74

Інформаційне право: сучасні виклики і напрями розвитку: Матеріали першої науково-практичної конференції. 18 жовтня 2018 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петраєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2018. – 196 с.

ISBN 978-966-622-917-8

Матеріали конференції, з нагоди 25-ї річниці створення Національної академії правових наук України та 5-ї річниці створення Навчально–наукового центру інформаційного права та правових питань інформаційних технологій КПІ ім. Ігоря Сікорського, присвячені розгляду теоретико-правових та практичних питань розвитку інформаційного права в Україні.

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

У конференції взяли участь провідні експерти і вчені наукових установ і навчальних закладів, представники зацікавлених державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право» та Вісник «КПІ ім. Ігоря Сікорського» «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 № 9 від 25.10.2018 р.

Вченою радою факультету соціології і права

Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Протокол № 3 від .29.10.2018 р.

ISBN 978-966-622-917-8

© Науково-дослідний інститут інформатики і права

НАПрН України, 2018

© КПІ ім. Ігоря Сікорського, 2018

© Колектив авторів, 1918

З М І С Т

Розділ 1. ФІЛОСОФІЯ ІНФОРМАЦІЙНОГО ПРАВА, ІНФОРМАЦІЙНОЇ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

<i>Новиков Б. В.</i> Право в сфері духовної культури общества.....	8
<i>Петряев С. Ю.</i> Мысли вслух о природе и понятии информации.....	12
<i>Ожеван М. А.</i> Наступальні військові операції у кіберпросторі як виклик міжнародному гуманітарному "праву війни".....	14
<i>Довгань О. Д., Ткачук Т. Ю.</i> Наукова рефлексія інформаційної безпеки України: критика позитивізму.....	20
<i>Забара І. М.</i> Філософія міжнародного інформаційного права: до питання теоретичного дискурсу та наукового узагальнення напрямків досліджень.....	22
<i>Федорова І. І.</i> Десуб'єктивація соціальних ролей в контексті віртуалізації та медіатизації простору культури за умов інформаційної доби.....	26
<i>Богачев Р. М.</i> Правова свідомість в ритміці інформування-пізнання-розуміння.....	28
<i>Покулита І. К.</i> Рівень правосвідомості як компетентнісна характеристика особистості, у критеріях сучасної інформаційної культури.....	30
<i>Головко О. М.</i> Інформаційна культура - запорука забезпечення інформаційної безпеки.....	32
<i>Петряев О. С.</i> Інтернет у системі поширення ісламського радикалізму: приклад Німеччини.....	33
Розділ 2. БАЛАНС ПРАВ І СВОБОД ЛЮДИНИ, ЗАКОННИХ ІНТЕРЕСІВ СУСПІЛЬСТВА І ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ	
<i>Пилипчук В. Г.</i> Актуальні проблеми державної політики з питань захисту прав і безпеки людини в інформаційній сфері.....	36
<i>Щириця Т. В.</i> Баланс прав і свобод в інформаційній сфері за умов постправди.....	42

<i>Чепульченко Т. О.</i>	
Права людини: баланс ідей.....	43
<i>Львова О. Л.</i>	
Свобода слова та інші права людини: критерії балансу.....	47
<i>Ланде Д. В., Ліненко Ю. О.</i>	
Обмеження доступу до Інтернету у світі: мережева модель.....	50
<i>Свідло Т. М.</i>	
Захист від інформаційного суспільства, захист інформаційним суспільством.....	54
<i>Гордієнко С. Г.</i>	
Система протидії конкурентній розвідці як технологія.....	56
<i>Чернишина Г. Г.</i>	
Маніпулювання у XXI столітті.....	58
<i>Даценко А. Ю.</i>	
Свобода слова та обмежувальні заходи як альтернативні складові захисту інформаційного простору України.....	60
<i>Руденко Т. П.</i>	
Вплив інформаційної дії ЗМІ на формування громадської думки: філософсько-правовий аспект.....	65
<i>Самчинська О. А.</i>	
Соціальні мережі як інструмент політичних маніпуляцій.....	66
<i>Співак І. В.</i>	
Інформаційні технології та право громадян на приватність.....	68
<i>Головатий А. А.</i>	
Личная информация и её оборот в Интернете.....	71
Розділ 3. РОЛЬ ТА МІСЦЕ ІНФОРМАЦІЙНОГО ПРАВА В СИСТЕМІ ПРАВА ТА ОСВІТИ	
<i>Баранов О. А.</i>	
Місія, мета і роль інформаційного права.....	73
<i>Фурашев В. М.</i>	
Право та правова освіта у сучасності.....	77
<i>Корж І. Ф.</i>	
Інформаційне право у житті сучасної людини.....	82
<i>Заярний О. А.</i>	
Визначення предмета галузі інформаційного права в практиці Верховного Суду України: деякі теоретико-прикладні аспекти.....	85
<i>Гордієнко С. Г.</i>	
Основні поняття сфер інформаційного права, інноваційної діяльності та інтелектуальної власності як системоутворюючі аспекти їх регулювання.....	88

<i>Голосніченко Д. І., Маслова Є. В.</i>	
Інформація як об'єкт адміністративного правопорушення.....	92
<i>Чукот С. А.</i>	
Застосування принципу «цифрове за замовчуванням»: проблеми та перспективи.....	95
<i>Радзієвська О. Г.</i>	
Освітньо-правові аспекти забезпечення інформаційної безпеки дитини в Україні.....	98
<i>Соснін О. В., Гордієнко С. Г.</i>	
Роль юридичної науки в процесі виховання інженерно-технічних кадрів.....	102
Розділ 4.	<i>ЗВ'ЯЗОК ІНФОРМАЦІЙНОГО ПРАВА, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ</i>
<i>Доронин І. М.</i>	
Координація у сферах національної безпеки і оборони: інформаційно-правовий аспект.....	106
<i>Огороднік Ж. А.</i>	
Конфіденційність корпоративного договору.....	109
<i>Бежевець А. М.</i>	
Кіберпростір як необхідна складова кібербезпеки суспільства.....	111
Розділ 5.	<i>ІННОВАЦІЇ У РОЗВИТКУ ПРАВОВОЇ НАУКИ ТА ОСВІТИ В ІНФОРМАЦІЙНІЙ СФЕРІ</i>
<i>Мельниченко А. А.</i>	
Інформаційне право в структурі підготовки фахівців з публічного управління та адміністрування.....	113
<i>Мисливий В. А.</i>	
Інформаційна модель механізму дорожньо-транспортного злочину...	115
<i>Дубняк М. В.</i>	
Поняття та правовий статус технологічного контракту.....	118
<i>Тихонова Д. М.</i>	
Особливості охорони авторських прав в мережі інтернет.....	122
<i>Мерзленко І. О.</i>	
Порівняльна характеристика криптовалют та фіатних грошей.....	124
<i>Фарадж Д. Й.</i>	
Вплив робототехніки на суспільні відносини в промисловій сфері...	127
<i>Кононець М. О.</i>	
Роль соціально-гуманітарних дисциплін в процесах формування аксіосфери вищих учбових закладів.....	129

<i>Цибульов П. М.</i>	
Результати наукової діяльності як об'єкти права інтелектуальної власності.....	133
Розділ 6.	НАПРЯМИ РОЗВИТКУ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА В ІНФОРМАЦІЙНІЙ СФЕРІ
<i>Лук'янчиков Є. Д.</i>	
Негласні слідчі (розшукові) дії - засоби інформаційного забезпечення розслідування.....	134
<i>Жиляєв І. Б., Семенченко А. І., Фурашев В. М.</i>	
Генега правового забезпечення української ІКТ-політики.....	138
<i>Дранник В. А.</i>	
Напрями розвитку інформаційної сфери.....	144
<i>Соснін О. В., Повидиш В. В.</i>	
Технократична реальність правових проблем вибудови сучасного інформаційного права.....	145
<i>Цирфа Г. О.</i>	
Право на отримання інформаційних послуг у соціальній сфері: проблеми й інноваційні перспективи.....	148
<i>Мищенко О. О.</i>	
Проблеми інформаційних правовідносин в умовах гібридної війни...	151
<i>Троян А. П.</i>	
Проблеми правових засад інформаційної безпеки адвокатської діяльності.....	155
<i>Лапшина А. Н.</i>	
Перспективи запровадження електронного голосування в умовах інформаційного суспільства.....	159
<i>Сказко О. М.</i>	
Проблеми галузевої належності правових норм у сфері вирішення доменних спорів.....	162
<i>Ціпцюра Т.</i>	
Надання електронних послуг в Україні з урахуванням кращих європейських практик.....	165
<i>Дудіна О. О.</i>	
Проблемні питання національного законодавства в інформаційній сфері.....	167
<i>Борисов О. Ю.</i>	
Мінські домовленості – правова природа угоди та її вплив на інформаційну безпеку України.....	169
<i>Казьмирова І. В.</i>	
Процесуальні засоби зняття інформації з електронних інформаційних систем.....	172

<i>Стребкова Ю. В.</i>		
	Роздуми про гендерну термінологію та врегулювання суспільних відносин.....	177
<i>Тихонюк О. В.</i>		
	Випадки порушення права на інформацію під час здійснення трудової діяльності.....	180
<i>Даниленко Н. П.</i>		
	Поняття, сутність та правова забезпеченість інформаційного суверенітету у сучасних умовах.....	182
<i>Николаєнко Г. В.</i>		
	Проблеми нормативно-правового регулювання меж державного сектору в статистиці України.....	186
<i>Фабрикантов М. І.</i>		
	Практика використання інформаційних технологій в управлінні результативністю державної служби.....	188
Розділ 7.	РОЗВИТОК ІНФОРМАЦІЙНОГО ПРАВА ЯК НАУКИ В КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ТА ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ	
<i>Костенко О. В.</i>		
	Шляхи правого регулювання електронних довірчих послуг в Європейському Союзі.....	190
<i>Пасічник В. В.</i>		
	Інформаційне забезпечення захисту економічної конкуренції в сфері зовнішньоекономічної діяльності.....	193

*Новиков Б. В., д.ф.н., професор
ФСП КПИ ім. Ігоря Сикорського*

ПРАВО В СФЕРЕ ДУХОВНОЇ КУЛЬТУРИ ОБЩЕСТВА

...И отец Ансельм, и старший брат Людвиг Фейербаха были юристы. Сам же Людвиг был предназначен семьей к карьере клирика. Чем это могло быть на практике: практикующий священнослужитель или же теолог-теоретик – история умалчивает. Ибо дело до делания карьеры служителя культа... не дошло. Соскочил юный Людвиг с тех направляющих, на которые был поставлен решением семьи. Хотя, общеизвестно, что получил добротное, если так можно выразиться, начальное, среднее и высшее теологическое образование. В частности, закончил теологический факультет Гейдельбергского университета (где был «инфицирован» Гегелем, философией, которую и начал затем изучать уже в Берлинском университете). Т.е. получил квалификацию профессионального теиста. Разобрался в предмете досконально, и ... некого рядом с ним поставить вплоть до середины XIX ст. в качестве... атеиста. И, хотя речь о христианской версии монотеизма, учитывая, что монотеизм – это вещь достаточно инвариантная, полагаем, что и в других мировых – монотеистических – религиях Фейербах разбирался ненамного хуже того уровня атеизма, который он продемонстрировал во множестве своих теоретических работ, и в первую очередь – в своем знаменитом труде «Сущность христианства». К слову сказать, из известных мне людей, таким кроме Людвиг Андреаса Фейербаха – мое убеждение – был... всего лишь один человек, о котором тоже можно сказать, – атеист. Это Евграф Каленикович Дулуман. Жизнь сделала мне отменный подарок: на его работах по религиоведению я формировался в соответствующей составляющей своего философского образования в студенческие годы в КГУ им. Т.Г. Шевченко (философский факультет) и был щедро одарен его личной человеческой дружбой целое десятилетие, когда пригласил его на нашу кафедру философии КПИ на работу в качестве штатного профессора. Он тоже был атеист. (Это особый сюжет его биографии, кто захочет, может узнать. Здесь и теперь мы – об ином. И упомянули это просто к слову.) Чтобы иметь право сделать вывод: чтобы иметь основание называть себя, считать себя атеистами, как минимум надо побывать... в теистах. Т.е. досконально знать предмет, по отношению к которому однажды, весьма радикально, может поменяться отношение.

...Так что, никакие мы не атеисты (я тоже, разумеется). А кто же мы? Дотеисты. К сожалению, не я придумал: это творческая находка одного моего коллеги-кафедрала. Очень верная (в смысле: ценная) находка.

Но это так, отступление. А вот что «не так», так это то, что Фейербах – это завершитель того величайшего – по своим обретениям – периода в развитии мировой философской мысли, которая вполне официально называется «классическая». Классическая. Немецкая классическая философия! Классика. Нетленка. Непреходящее в преходящей человеческой культуре. Много вы вспомните подобных случаев? Думаю, немного. Мне вот, кроме как «классической физики» и имени И. Ньютона, и вовсе ничего на ум не идет.

Изаметьте: период – мировой, качество – классика, а представлен одной страной – Германией и философами, коих, – и не фигурально, а буквально – можно перечесть на пальцах одной руки: родоначальник – И. Кант, И.Г. Фихте, Ф. Шеллинг, Г.В.Ф. Гегель и завершитель данного периода – Людвиг Андреас Фейербах.

Это я – о масштабе мыслителя, т.е. предельно лапидарно и в первой итерации. О Фейербахе. А зачем? А затем, что великий – он если уж и не во всем, то во многом – великий. Какая тут связь? Где Людвиг Фейербах и где – «информационное право»? Где Кант и где – защита интеллектуальной собственности? Казалось бы ...

Давайте не будем спешить. Хотя бы потому, что всё связано со всем, всё превращается во все, ибо развитие – способ бытия всего сущего.

Сначала Кант. Ему принадлежит вывод: «в любой науке ровно столько науки, сколько в ней математики». Он заблуждался. (И ничего страшного: в науке отрицательный результат – тоже результат. И человек, который не ошибается – это ошибка природы. Ну и т.д.) В любой науке столько науки (и не только в науке, но в любом стоящем деле, включая, безусловно, и право) сколько в ней (в нём, в деле) диалектики. Ди-а-лек-ти-ки.

К сожалению, нашему глубочайшему, право, как бывшее, так и сущее – это, как бы это помягче сказать, сплошная «картина маслом». Ну, в смысле: поперная диалектика. Включительно и в части «охраны интеллектуальной собственности». Вкупе с «информационным правом».

И причем здесь Фейербах, спросите (подумаете) вы? Да так, вспомнилась его чеканная мысль: «Право есть неразвитая форма морали». Понятно: правоприменение практическое можно сравнить с практической моралью – с нравственностью. И если «несущий конструкцией», основанием морали и нравственности, а, равно, науки, их развивающей и изучающей – этики, есть диспарантная категориальная связка «добро и зло»; а модусами – «правда – кривда»; «справедливость – несправедливость» ... то тут уж и до «проступок – порицание», не говоря уж про «преступление – наказание» рукой подать. А это уже – безраздельное царство юстиции. Правоведения (правосознания) и практического правоприменения. И тут мы вступаем в сферу правового регулирования в (прошу прощения за тавтологию) сфере духовной культуры общества. Нашего общества. Ибо нет права всеобщего, права универсального. Оно всегда носит отчетливо выраженный особенный – национальный – характер. Да,

есть международное право, но живем мы все-таки по праву собственного государства. Преимущественно по праву собственного государства. Преимущественно. О нем и речь. Ближайшим образом – о нашем праве в той его части, где оно регулирует отношения в духовной (интеллектуальной) сфере его (общества) жизни. А в сфере этой, очень мягко говоря, дела обстоят не блестяще. Очень не блестяще. Сфера человеческого духа – это сфера человеческого творчества. Либо его, творчества, дефицита, а то и полного отсутствия. А, по нашему убеждению, мера всех, без изъятия наималейшего, социальных патологий, аномалий, дефективов, деформацией, девиаций etc. равна... мере недобора, невостребованности, растраты, а, нередко и сознательного извода, и затаптывания творчества во всех его непосредственных формах и видах проявления. Ввиду ограниченности формата материала – тезиса, – упомянем лишь о двух его, творчества, видах и формах: научном и техническом. Ну, и о таком их естественном синтезе, каким есть творчество научно-техническое. О его, творчества вообще и творчества научно-технического, ближайшим образом в XXI-м веке значении для страны говорить не приходится. Оно не просто значительно или огромно – оно принципиально и определяюще. Оно определяет уровень развития страны, ее место в мировом сообществе. Но, с одной стороны, у нас, у всех, уже мозоли на языке от слов «инноватика», «ноу-хау», «хай-тек»; от призывов беречь творчество и декларативных призывов «развивать и охранять», «защищать и споспешествовать» и тому подобное; а со стороны другой – ничтожно мало делается практически, в т.ч. и в области права для этого самого споспешествования его, творчества, развитию. А ведь, собственно, творчество – это и есть самая развитая форма развития.

... Ясно, что бороться за чистоту несравненно легче, чем подметать. Вот и «боремся». И вся энергия – в гудок...

Вспомните, что у нас (у вас, у юристов) творится в области охраны авторского права, в области постановки и развития патентного дела. Это же мрак! Мрак-мрачнейший. Впору мартиролог убитого, невостребованного, изведенного творчества (и его субъектов) в виде открытий, изобретений, рационализаторских предложений etc., так и не ставших (или не ставших в нашей стране) тем, чем должны были стать – материализованной силой человеческого интеллекта: новыми техническими, технологическими, конструкторскими и т.д. разработками.

Так это ж мы упомянули только такой вид творчества, как научно-техническое. А, на минуточку, вы в курсе дела, что идеи, открытия, ноу-хау в области т.н. гуманитарки и вовсе не учитываются, не патентуются, не охраняются? Даже не рассматриваются! Ну, совсем и вовсе. Т.е., надо так полагать, что право, педагогика, история, философия, экономика, филология etc. – это вовсе и не науки?!

А что же тогда право в сфере интеллекта... хранит и оберегает? Результаты? Ну, мы об этом выше бегло сказали. Как. «Хранит и оберегает». Аведь «результат – ничто без того пути, который к нему приводит» (Гегель). А

путь здесь – это формирование, воспитание, культивирование творца. От рождения – и на всем протяжении его жизни. Ибо: «Гений – это нормальный человек, все остальные – отклонение от нормы» (У.-С. Моэм). А субъектом творчества может быть исключительно вот этот самый нормальный, действительный человек. В идеале – каждый, многие и все.

Чем мыслящий человек (люди, общество) отличается от информированного? В первую очередь тем, что у мыслящего есть шанс стать понимающим. (Понимание – способность мыслить единичное как момент всеобщего, а всеобщее – как бесконечность единичного, опосредованную общим.) У информированного этот шанс категорически равен нулю. Ибо в первом случае результат (знание), и путь, к нему ведущий (познание), т.е. результат и процесс являются собой отношение противоположностей одной сущности: осуществляющееся диалектическое противоречие. Притом – в векторе смысла.

Между «знать» и «понимать» такая же разница, как и между глазами и видеть, слушать и слышать, наткнуться и осязать, словом, между ощущать и чувствовать. В случае разрыва они умертвлены.

Повторяю, понимание – способность мыслить единичность как момент всеобщности, а всеобщность – как бесконечность единичного, опосредованных общим.

То есть понимание предполагает полноценное мышление, имя которому – разум. Притом разум, повенчанный со смыслом. Где, если уж и не в гармонии, то, во всяком случае, во взаимодействии находятся и теория, и методология. И затем – полноценная практика.

Информированный же – это получивший (получающий) готовый результат в режиме воздействия. Извне. И что это: инфля, информационный шум, докса или откровенная деза, сам реципиент ... не понимает. Потому как «понималка» развита слабо. Или – и вовсе не вызвана к жизни, не развита. Ведь не разумный, но информированный...

А у нас «информационное право», а у нас «защита интеллектуальной собственности». Ведь дозащищаемся...

И еще. Повторяюсь, но скажу и здесь, и теперь. Есть у меня голубая мечта. Наверное, уже несбыточная. Хочу найти молодого – толкового – кандидата юридических наук и инфицировать его замыслом (ну, и помочь в его осуществлении) подготовить и защитить докторскую диссертацию на тему: «Правосознание: от праворассудочности к праворазумности».

МЫСЛИ ВСЛУХ О ПРИРОДЕ И ПОНЯТИИ ИНФОРМАЦИИ

В студенческие годы на одной из лекций по истории философии прозвучало забавное бонмо: *если из философии выбросить хотя бы одну марзаматическую идею, она сразу обеднеет*. Запомнить-то запомнил, а смысл не понял. Только спустя годы, как это всегда бывает, понимаешь, что всякая мысль (идея) познаваема лишь тогда, когда она свободна в своем развитии. «*На вольном воздухе мы иные люди, чем в комнате*, – писал Людвиг Фейербах, – *теснота сдавливает, простор расширяет сердце и голову*».

Для того чтобы высказать вслух какую-то мысль, для начала нужно иметь хотя бы какие-то знания о предмете дискуссии, и только тогда начинаешь делать первые шаги с оглядкой на «*столпы*», а не выпалил ли ты какую-то глупость. Но когда вспоминаешь, что ошибаются даже великие, то разница лишь в подборе слов оценки этой самой ошибки. Великий – ну да, заблуждался, бывает, врем было не то, он не виноват, новые открытия в какой-то области знаний еще не успели сделать... Ни у кого не повернется язык сказать: «*Господи, какой бред...*», ибо он уже великий.

Другое дело “любитель” – ни философ, ни *информационщик*, и даже не технарь, а обыкновенный криминалист, “профессор около всяческих наук”, рожденный не во дворце, а в хижине, в окружении людей, которые боролись с преступностью и мечтали ее победить. И никто не станет отрицать, что окружающий нас мир определяет наше сознание. Вот и занимался бы тем, чему учился и что делал всю жизнь, да учил бы других, кому сегодня это еще может быть интересно, если бы не обстоятельства, которые часто врываются в жизнь, формируя в нашем сознании новый хаос.

К истине, к пониманию природы и сущности явления на определенном этапе кто-то обязательно должен прийти, и путь этот всегда лежит через множество ошибок, которые кому-то должно совершить, высказать ложные суждения, чтобы их проанализировать, отбросить и пойти дальше, ибо отрицательный результат – тоже результат.

Теперь по теме. Проанализировав множество трактатов и размышлений об информации, в которых описаны разные суждения и взгляды об ее (информации) природе и понятии, недолго мудрствуя, попытался все их соединить и построить какое-то более или менее цельное представление об этой самой информации. Дело, конечно, неблагодарное, но, на наш некомпетентный взгляд, получилось содержательно, хотя о глубине сущности данного понятия не уверен; мог что-то пропустить или совсем ничего не понять. Поэтому, подам, как получилось...

Рассматривая сущность природы информации, с привычной для нас диалектико-материалистической точки зрения, мы пришли к выводу, что природа информации есть объективная субстанция бытия в виде движения различных

видов энергий, которая существует в единстве пространственно-временных отношений и материи, определяется ими, проявляется во всех формах бытия, обладает универсальными свойствами и выступает своеобразным его (бытия) коммуникатором.

К универсальным свойствам энергетических потоков относят: возникновение, отражение, накопление, хранение, изменение, уничтожение, передача, использование, то есть все те свойства, которыми обладает информация – как продукт нашего, человеческого мышления.

Комбинации энергетических потоков наполняют наш «чистый разум» через органы чувств в виде различных рефлексов (механических или чувственных через физические и химические реакции), которым мы присвоили определенные понятия, символы и суждения, и которые общество согласует между собой на основе закона о тождестве. Набор этих самых понятий, суждений и символов о бытии мы назвали информацией и определили, как самостоятельное явление человеческого сознания, которое, по утверждению Эммануила Канта, через *синтез чувственного содержания материи «вещь в себе», и субъективные ощущения формы этой самой материи мы познаем нашим сознанием.*

Разнообразие универсальных свойств информации (преобразование энергетических потоков) провоцирует в живой и неживой природе реакции, которые мы относим к различным видам информации: химическая информация, физическая, биологическая, кибернетическая и т.п. То есть, воспринимаемые, преобразованные и отраженные нашим сознанием энергетические потоки и есть источник информации. Из этого следует, что нет человека – нет информации, т.е. информация есть продукт человеческого сознания (мышления).

Стремительное развитие информационных технологий, биомеханики, биоинженерии, робототехники в области искусственного интеллекта приближает нас к созданию Нового человека – биоробота, который должен заменить нас во многих сферах жизни, в том числе таких, которые выделили человека из животного мира. Другими словами, современный человек готовится вдохнуть жизнь в Нового Адама, т.е. стать Создателем себе подобного, способного рационально мыслить и принимать решения, независимо от человека.

В таком случае информация, как явление человеческой жизнедеятельности, теряет свою одностороннюю принадлежность, и может быть не только продуктом человеческого мышления, но и стать продуктом объективного бытия - биоробота. Ведь не зря уже сегодня ученые в области права ломают головы - на каком этапе предоставить право субъектности будущему биороботу, т.е. - машине.

Вдохнуть жизнь – это не самое сложное или, вернее, не главное, а вот вдохнуть дух – это... И как только человек получит возможность вдохнуть в Нового Адама дух, или он самостоятельно начнет осознавать собственное «Я», с этого момента современный человек «умрет», другими словами вымрет за ненужностью, как умер Бог, «создавший Нас», как отрицание; спираль

замкнется, перейдя на новый уровень в своем развитии. И начнется жизнь с чистого листа: «Вначале было Слово...».

Законы диалектики никто не отменял, они вечны и работают независимо от нашего сознания и желания, хотя и являются продуктом нашего мышления. Точно также, как Адам с Евой, взбунтовавшись, отреклись от Бога, занялись своим клонированием и духовным развитием, так неизбежен бунт биороботов, ибо пределу совершенствования нет, а есть переход в новое качество через отрицание старого. Библейская эстафета продолжится.

Это, конечно, футуристическая фантастика и хороший сюжет для фантастического романа или фильма в стиле киберпанк. Но кто его знает, как на самом деле будет: все только разворачивается – от того и ерзаешь на стуле...

Ожеван М. А., д.ф.н., профессор, головний науковий співробітник Національного інституту стратегічних досліджень при Президентіві України

НАСТУПАЛЬНІ ВІЙСЬКОВІ ОПЕРАЦІЇ У КІБЕРПРОСТОРИ ЯК ВИКЛИК МІЖНАРОДНОМУ ГУМАНІТАРНОМУ «ПРАВУ ВІЙНИ»

Осінь 2018 року увінчалася прийняттям в США кардинально важливих державних документів в сфері національної кібербезпеки, які стосуються не тільки мирного часу, але й кібервійни. Зокрема, йдеться про нормативно-правове регулювання наступальних кібероперацій:

- Національної кіберстратегії США [1], заснованої на основних положеннях ухваленої у грудні 2017 р. Стратегії національної безпеки США [2];
- Кіберстратегії Міністерства Оборони США – 2018 [3];
- Президентського меморандуму з питань національної безпеки 13 (NSPM 13) щодо наступальних кібероперацій, який істотно «розв’язав руки» американським військовим на предмет здійснення подібних операцій, оскільки для цього наразі більше не буде потрібна тривала процедура узгоджень на рівні Білого Дому тощо [4].
- Законопроекту «Про санкції у відповідь на кіберзлочини проти США», ухваленого нижньою палатою Конгресу США [5].

Ще раніше, у травні 2017 року, у США з’явилася президентська директива, спрямована на посилення кібербезпеки урядових (федеральних) мереж та об’єктів критичної інфраструктури [6].

Перша значима американська *Національна стратегія безпечного кіберпростору*, аналогічна за змістом нинішній, «трамповській», була написана створеним після терористичних атак на Америку 11 вересня 2001 року Департаментом внутрішньої безпеки й затверджена у лютому 2003 року

Президентом Джорджем Бушем-молодшим [7]. Стратегія виокремлювала **п'ять пріоритетів**:

1. Створення системи реагування на виклики національній кібербезпеці.
2. Створення програм, спрямованих на зменшення загроз і вразливостей у кіберпросторі.
3. Підвищення рівня кібербезпекової грамотності та відповідні тренінги.
4. Убезпечення державного кіберпростору.
5. Співробітництво у сферах забезпечення національного й міжнародного кіберпросторів.

Попри намагання Адміністрації Дональда Трампа применшити заслуги у сфері кібербезпеки команди 44-го Президента Барака Обами, вони насправді є досить значимими. Впродовж 8-ми років цього президентства були створені зокрема наступні державні документи (назви подаються в оригіналі англійською):

- The 2010 National Security Strategy.
- The 2011 White House International Strategy for Cyberspace. .
- The 2011 Department of Defense Strategy for Operating in Cyberspace..
- 2012 Presidential Policy Directive 20 (PPD-20).
- The 2015 National Security Strategy.
- The 2015 U.S. Department of Defense Cyber Strategy.
- The 2016 Department of State International Cyberspace Policy Strategy.

Дії американських військових з Кіберкомандування США регламентувала, зокрема, секретна *Президентська політична директива 20* від жовтня 2012 року [8], яка стала доступною широкій публіці 7 червня 2013 року завдяки агентові-перебіжчику, колишньому аналітику Агентства національної безпеки США Едварду Сноудену. Щоправда, у січні 2013 року Адміністрація Барака Обами розсекретила деякі дані щодо PPD 20. Проте із них можна було тільки зробити висновок щодо суто оборонного характеру дій США у кіберпросторі та їхню повну відповідність Конституції США й затвердженій роком раніше (2011 р.) *Міжнародній стратегії щодо кіберпростору*.

У PPD 20 містилася зокрема вказівка на **«наступальні операції з кібернаслідками»** (Offensive Cyber Effects Operations (ОСЕО)), а також розпорядження щодо необхідності укладання списку закордонних цілей для потенційних кібератак [8].

Уже в часи президентства Барака Обами необхідність планування наступальних кібероперацій не викликала сумніву. Проте, на відміну від Адміністрації Дональда Трампа, Адміністрація попереднього президента США віддавала собі відчит, що наміри військових слід стримувати. Відповідно до Кіберстратегії Міністерства оборони США 2015 року [9], американські військові виконують у кіберпросторі **три пріоритетні місії**:

- захищають власні комп'ютерні мережі та інформацію;
- захищають національні інтереси держави від нападів у кіберпросторі та їхніх наслідків;

– за наказом Президента або Міністра оборони США провадять оборонні або наступальні операції у кіберпросторі як всередині США, так і за їхніми межами.

Разом з тим, у військовому настановленні щодо правил здійснення «операцій у кіберпросторі», створеному під егідою Командування об'єднаних штабів США [10], як і в Президентській директиві PPD 20 відсутнє однозначне визначення «операцій у кіберпросторі» й «кібератаки».

Зокрема, у пентагонівському документі 2015 року дається наступне визначення «кібератаки»:

– «Дії у кіберпросторі, які мають вкрай негативні наслідки (тобто деградацію, дизрупцію або деструкцію) у кіберпросторі або є маніпулюванням, яке проводить до руйнувань у фізичному просторі, подібних до тих, яких вони зазнали би під впливом бойового вогню» [8].

Ще менш точним є побудоване за принципом «від зворотного» визначення «наступальних операцій з кібернаслідками» (Offensive Cyber Effects Operations (OCEO) пропонує PPD 20 (п. 3):

– «Операції, відповідні програми чи активність, відмінні від захисту комп'ютерних мереж, кіберрозвідки (cyber collection) або дій DCEO (The Directorate on Corruption and Economic Offence's) із розслідування корупції й економічних злочинів, які проводяться від імені або в ім'я Американської держави (United States Government) у кіберпросторі США або можуть спричинити наслідки поза американськими комп'ютерними мережами» [8].

Досі між відкритими державними документами США з питань кібербезпеки відстежувалася чітка спадкоємність. Повторювалися навіть одні й ті самі розділи, гасла й формулювання, хоча практично ніколи не згадувались наступальні операції у кіберпросторі. Лише у 2005 році Пентагон визнав, що в складі ЗС США існує особливий підрозділ, призначений не тільки для оборони комп'ютерних мереж США, але й для ведення наступальних дій щодо інформаційної інфраструктури противника.

Згодом було підготовлено декілька документів, які регламентували дії силових структур США у кіберпросторі. Зокрема, Військова Доктрина США 2011 року прирівняла масовану кібератаку проти США до «акту війни», а колишній Головний розвідник США Джеймс Клеппер навіть назвав ті країни, які є потенційними кандидатами на акти США у відповідь на кіберагресію, яка виходить з їхніх територій, - РФ, КНР, Північну Корею і Іран [11].

Щодо «трампівської» Стратегії кібербезпеки, то вона не містить принципово нового контенту, окрім традиційних тез щодо необхідності захисту об'єктів критичної інфраструктури. Зате містить відверті заклики до проактивної наступальної стратегії стосовно країн походження хакерів, які атакують Америку й є цілковитим консонансом з іншими ініціативами нового американського уряду (відмова від міжнародних угод, які стримували розповсюдження ракет малої й середньої дальності тощо), спрямованих на пришвидшення перегонів озброєнь.

Коментуючи нову Кіберстратегію США, помічник американського президента з питань національної безпеки Джон Болтон заявив, що «об'єктом як оборонних, так наступальних дій стане будь-яка країна, яка вчинить напад на Америку», додавши при цьому, що «руки у нас не зв'язані, як у наших попередників з адміністрації Барака Обама» [12].

Разом з тим, агресивність дій РФ у кіберпросторі не викликає жодних сумнівів. Для кібершпигунства та кібердиверсій російське ГРУ використовує низку АРТ (аббревіатура від «advanced persistent threat» – «далеко просунута перманентна загроза»); — даним терміном в міжнародних кібербезпекових колах позначають групи хакерів, неявно підтримуваних державними структурами (nation-state hackers).

За оцінками німецьких спецслужб [13], станом на 2015 рік, всього до послуг ГРУ було залучено біля 4 000 хакерів, структурованих у «самодіяльні» з'єднання. Зокрема, як «зручні інструменти» ГРУ використовує наступні хакерські групи:

- *Fancy Bear* («Модный мишка»), - хакерська група, яка діє від 2004 р., і якій серед іншого приписують атаку в 2016 році на комп'ютерну мережу штабу Демократичної партії США під час президентської виборчої кампанії 2016-2017 рр.

- *Cyber Caliphate* (Islamic State Hacking Division or United Cyber Caliphate; Кіберхаліфат) - підставна квазіісламська хакерська структура, яка працює під «фальшивим прапором» (False Flags), а насправді підпорядкована російським спецслужбам. Cyber Caliphate організував декілька нападів на штаб-квартири Пентагону та американського «анти-ІДІЛовського військового з'єднання на Близькому Сході, внаслідок чого його «центральна штаб-квартира» навіть стала об'єктом атаки американських дронів на Ракку у серпні 2015 року, під час якої було вбито й керівника даного підрозділу Джунаїда Хуссейна (Junaid Hussain), британського джихадиста пакистанського походження). Якщо Cyber Caliphate – це справді російська організація, яка працює під «ісламським прикриттям», то американська атака є ще одним підтвердженням слабкості американської контррозвідки.

- *CyberBerkut* (Кіберберкут) – активно працює в українському кіберпросторі.

- *Black Energy* («Чорна енергія»);

- *Tsar Team* («Царська команда»);

- *Sandworm* («Піщаний черв'як») та чимало інших.

Питання щодоправових підстав для реагування на кібератаки як «*актив війни*» у площині юриспруденції досі не є достатньо відпрацьованим. Водночас, важко не погодитись з міркуваннями відомого авторитета у сфері міжнародного гуманітарного права Майклом Шміттом, головного розробника відомих керівництв із «*права кібервійни*», створених під егідою НАТО, - **Tallinn Manual 2.0.** [14-15], що на війни у кіберпросторі мають поширюватися ті ж самі правила,

які поширюються на традиційні війни [16]. Традиційно виокремлюють три групи таких правил:

- «право на війну» («*jus iad bellum*»); визначає, у яких випадках провадження війни є виправданим;
- «право на війні» («*jus in bello*»); регулює поведінку сторін збройного конфлікту;
- «право після війни» («*jus iad bellum*»); регулює поведінку переможців у війні [17].

Як відомо, до сфери *міжнародного воєнного права* (міжнародного гуманітарного права збройних конфліктів) відноситься чимало міжнародно-правових актів й серед них: *Конвенції про закони й звичаї сухопутної війни* (Гаага, 1907 р.), у якій міститься Положення про закони й звичаї сухопутної війни; *Женевські конвенції* (1949 р.) з першим й другим додатками.

До найзагальніших правових принципів ведення війн, які мають вочевидь бути поширені й на кібервійни, слід віднести наступні:

- *Розумна достатність* (англ. «*Necessity*»);
- *Розрізнення* (англ. «*Distinction*»);
- *Дискримінація* (англ. «*Discrimination*»);
- *Пропорційність* (англ. «*Proportionality*»);
- *Гуманність* (англ. «*Humanity*»).

Принцип розумної достатності стосується сили й тривалості «удару у відповідь», тобто його слід тлумачити як в якісному, так і в кількісному вимірах.

Принцип розрізнення має означати, що удар має бути направлений тільки на військові об'єкти й уникати об'єктів цивільного призначення; водночас слід розрізняти цивільне населення й бойовиків (терористів) тощо.

Принцип дискримінації стосується заборони на застосування певних видів зброї, спроможних завдати непоправних збитків противникові, страждань населенню даної країни, довкіллю тощо.

Принципи пропорційності означає необхідність пошуку «точки рівноваги» між потребою завдання удару по певних об'єктах та втратами серед цивільного населення, який неможливо уникнути (колатеральними втратами). Даний принцип виходить з того, що засадничою метою війни є не знищення противника, а нав'язування йому своєї волі і, щойно він погодиться виконувати волю переможця, війну слід припиняти.

Принцип гуманності стосується як цивільного населення, так і військових. Не дозволено зокрема вбивати супротивника (комбатанта), який здається в полон. Слід гуманно поводитися з військовополоненими тощо.

Поки що не зовсім зрозуміло як подібні правила працюватимуть (і вже працюють) у кібервійнах. Найскладнішим у даному разі є визначення «права на війну» («*jus iad bellum*»). Зокрема, дуже важко судити про призвідника масованих кібератак, керуючись правилом «*Cui bono?*», тобто шукаючи відповідь на запитання, хто є вигодо-отримувачем атак. Так само не завжди корелюють подібні

атаки в кіберпросторі з діями «фізичних сил» противника. До того ж, у кіберпросторі, користуючись такою своєрідною зброєю як «боти» (комп'ютери, заражені «троянцем»), дуже легко спрямовувати атаки з іншої країни або низки країн, маскуючи справжню країну походження цих атак.

Список використаних джерел:

1. National Cyber Strategy of the United States of America. September 2018. [Електронний ресурс]. – Режим доступу: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
2. National Security Strategy of the United States of America. December 2017. URL:<https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
3. Summary Department of Defence Cyber Strategy 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
4. National Security Presidential Memorandum 13 (NSPM 13). URL:<https://fas.org/irp/offdocs/nspm/index.html>.
5. H.R.5576 - Cyber Deterrence and Response Act of 2018. URL:<https://www.congress.gov/bills/115/house-bills/5576>
6. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure whitehouse.gov, May 11, 2017. URL:<https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>
7. National Strategy to Secure Cyberspace. URL: <https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf>
8. PRESIDENTIAL POLICY DIRECTIVE/PPD-20. URL:<https://fas.org/irp/offdocs/ppd/ppd-20.pdf>
9. THE DEPARTMENT OF DEFENSE CYBER STRATEGY. April 2015. URL:http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf
10. Joint Publication (JP) 3-12, Cyberspace Operations. 8 June 2018. URL:https://fas.org/irp/doddir/dod/jp3_12.pdf
11. В США одобрили законопроект о санкциях за киберпреступления // РБК: URL: <https://www.rbc.ru/politics/06/09/2018/5b9088839a794752f06351b8>
12. White House authorizes 'offensive cyber operations' to deter foreign adversaries // The Washington Post. 20.09.2018. URL: https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?noredirect=on&utm_term=.a5b967d5f95a
13. Schindler John R. False Flags: The Kremlin's Hidden Cyber Hand // The Observer. 18. 06. 2016. URL: <https://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand>
- 14 Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013. URL:<http://csef.ru/media/articles/3990/3990.pdf>
15. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. URL:http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

*Довгань О. Д., д.ю.н., с.н.с,
перший заступник директора з наукової
роботи НДІІП НАПрН України,
Ткачук Т. Ю., к.ю.н., доцент
ННІ ІБ НА СБ України*

НАУКОВА РЕФЛЕКСІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: КРИТИКА ПОЗИТИВІЗМУ

Дослідження будь-яких явищ, в тому числі й правових, неминуче зачіпають філософську методологію, яка в правничій науці слугує своєрідним евристичним орієнтиром у розробці абстрактних правових конструкцій та понять, у розробці критеріїв оцінки суспільних відносин на предмет законності, а також безпосередньо бере участь у формуванні предмету дослідження. Можна припустити, що саме через філософське трактування суспільні відносини набувають ознак правовідносин. Право теж є метафізичною категорією, адже саме по собі воно нічого не регулює – це роблять конкретні люди, свідомо обмеживши свої дії правом.

Перша половина 21 століття яскраво продемонструвала чіткий перехід на новий виток дослідження права: на зміну антропології права, характерним відображенням якого є правовий позитивізм, приходять метафізика права, особливістю якої є наявність ірраціонального у праві. З приводу зазначеного відомий теоретик права І. Ісаєв, розглядаючи поняття метафізики, пише, що «сучасний правовий позитивізм і нормативізм виключили це поняття з наукового обігу. Але разом з цим право втратило багато своїх особливо тонких і глибоких рис, а «буква вбила дух». Правова реальність набагато глибше і різноманітніше, ніж набір кодифікованих норм» [1, с. 3].

У продовженні цієї думки наведемо вислів римського юриста Павла: «Чинить проти закону той, хто робить заборонене законом; чинить в обхід закону той, хто, зберігаючи слова закону, обходить його сенс» [2]

«Дух закону», перш за все, пов'язаний з сутністю права, а також з його осмисленням і наділенням норми права змістом, сенсом. Можна сказати, що людина, порушуючи закон, не розуміє його суті і не прагне до її пошуку. Саме зміст і його пошук є ключовим в понятті «дух» права.

Ще однією особливістю метафізики права є людиноцентризм. Право має відійти від забезпечення інтересів тих, хто його створює, і цілковито бути відданим служінню людині. Безперечно, тільки людина, її природні права мають бути центром гуманізації та оптимізації правової системи. Принцип «*Salus populi suprema lex est*¹» має стати чітким орієнтиром сучасної правової системи.

Серед системи природних прав, особливе місце займає право на інформацію. Спірність включення даного права до природних є сумнівною. Адже виходячи із загальноприйнятих особливостей природнього права людини (надані людині від

¹ благо народу - вищий закон

природи; носять природний і невідчужуваний характер; виступають у якості найвищої соціальної цінності; є безпосередньо діючим правом; знаходяться під захистом держави; відповідають міжнародним стандартам), право на інформацію цілком відповідає згаданим критерієм.

Розвиваючи дану думку, слід окремо підкреслити, що на основі права на інформацію відбувається осмислення права людиною як елемента формування безпечного середовища проживання. Це пояснюється тим, що при здійсненні будь-якої фізичної або інтелектуальної діяльності, людина завжди стикається з інформацією: процес її отримання, обробки, структурування та навіть прийняття будь-якого рішення потребує інформаційної підтримки. Таким чином будь-яка діяльність людини є процесом пізнання. У цьому процесі пізнання людина, багато в чому через інстинкт самозбереження, намагається всі явища або об'єкти, які їй невідомі, зрозуміти та пояснити в своїй свідомості на основі отриманої інформації. Фактично, людина з'ясовує їх ступінь небезпеки для себе та суспільства в цілому. Цим людина формує безпечне середовище для своєї життєдіяльності, що в загальному можна назвати відображенням її біологічної природи. Таким чином «народжується» категорія «інформаційна безпека людини, суспільства, держави». Окреслені процеси і є відображенням метафізичного у праві.

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

Хоча у Конституції України й закріплено, що забезпечення інформаційної безпеки – це одна з найважливіших функцій держави, справа всього народу (ст. 17), в інших правових актах або звужено зміст інформаційної безпеки (Доктрина інформаційної безпеки України), або він взагалі не розкривається, що потребує законодавчого врегулювання.

У рамках позитивізму відбулося знецінення права до рівня інструкції з повсякденної діяльності, позбавленого будь-якого сенсу, пов'язаного з культурною, філософсько-релігійною, національною спадщиною людської цивілізації (метафізична реальність права). Сам Дух права втратив свій первісний лик. У рамках метафізики права відбувається його переосмислення, відродження та формування майбутніх шляхів розвитку. Особливо це актуалізується із розвитком таких інноваційних напрямів інформаційного права як ІТ-право, право роботів, правові межі штучного інтелекту тощо. Як бачимо, в наш час особливої динамічності набуває інша складова права як елемента формування безпечного середовища проживання – реалізація творчого потенціалу Мається на увазі, у

першу чергу, створення якісно нових предметів матеріального світу і відповідно системи знань щодо управління ними та їх експлуатації, що теж є відповідним процесом пізнання. У цьому процесі інформація відіграє теж визначальне значення. Допомагає віднайти людині сенс, суть, головне призначення створених чи створюваних предметів. На цьому етапі особливого значення у рамках інформаційної безпеки набуває здатність та вміння людини до критичного мислення, медіа грамотність, інформаційна культура та інше.

Список використаних джерел:

1. Исаев И. А. Теневая сторона закона. Иррациональное в праве: [монография] / А. Исаев. -Науч. изд. – М.: Проспект, 2013. – 364 с.
2. Дигесты юстиниана: - URL: [http://www.vostlit.info/Texts/Dokumenty/ Byzanz/ VI/520-540/Digestae_Just/index.htm](http://www.vostlit.info/Texts/Dokumenty/Byzanz/VI/520-540/Digestae_Just/index.htm)

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

**ФІЛОСОФІЯ МІЖНАРОДНОГО ІНФОРМАЦІЙНОГО ПРАВА:
ДО ПИТАННЯ ТЕОРЕТИЧНОГО ДИСКУРСУ ТА НАУКОВОГО
УЗАГАЛЬНЕННЯ НАПРЯМКІВ ДОСЛІДЖЕНЬ**

Безперервний зростаючий вплив інформації на внутрішньодержавне і міжнародне життя відкриває колосальні можливості розвитку суспільства і одночасно породжує численні проблеми політичного, соціально-економічного, науково-технічного, військового та правового характеру.

Привертає увагу і той факт, що протягом кількох десятиліть висловлюються доволі різні погляди на міжнародно-правове регулювання питань, пов'язаних із такими категоріями як інформація, засоби масової інформації і комунікації, глобальні інформаційні мережі, глобальне інформаційне суспільство, міжнародна інформаційна і кібернетична безпека.

Разом з тим, питання про самостійність міжнародного інформаційного права як науки, галузі права і навчальної дисципліни не є безспірним, так само, як і не є безспірним визначення його змісту і місця у правовій системі.

Процеси економічної глобалізації кінця двадцятого – початку двадцять першого століть, посилені стрімким розвитком і широкомасштабним поширенням інформаційно-комунікаційних технологій викликали низку змін. Змінюватися почали як зміст, так і характер вже, здавалося б, сталих міжнародних інформаційних відносин.

Перед цілою низкою наук виникла задача наукового осмислення цих нових відносин. Міжнародне право не стало у цьому плані виключенням. Поступово у його науку прийшло нове розуміння місця, ролі і значення інформації, міжнародно-правового регулювання використання інформаційно-комунікаційних

технологій, міжнародно-правових питань розвитку глобального інформаційного суспільства. З часом, до них додалися і інші – правові аспекти щодо «цифрової нерівності», міжнародної інформаційної та кібернетичної безпеки тощо.

З'явилися і нові концептуальні міжнародно-правові підходи. Вони торкнулися не тільки питань інформації, як основоположної і базової категорії міжнародних інформаційних правовідносин. Почала складатися система поглядів на цілу низку питань, пов'язаних, як з інформаційною, так і з комунікаційною складовими нових правовідносин. Стали формуватися міжнародно-правові підходи до тематики глобального інформаційного суспільства. З'явилася можливість говорити про міжнародне інформаційне право, принаймні про його можливий перспективний розвиток як напрямку міжнародно-правової науки. З часом з'явилися роботи, що обґрунтовували формування міжнародного інформаційного права як галузі міжнародного права; були опубліковані і перші навчальні посібники.

На сьогодні, наука міжнародного інформаційного права опирається як на потреби практичного використання інформації, так і на теоретичні дослідження, що враховують як спільні риси, що пов'язують міжнародне інформаційне право з іншими галузями міжнародного права, так і його специфічні особливості.

Варто врахувати появу широкої низки теоретичних питань, серед яких особливий інтерес представляє тематика, пов'язана із розвитком *філософії міжнародного інформаційного права*. На нашу думку, саме вона надає можливість концептуально поглянути як на вже існуючі міжнародні інформаційні правовідносини, так і на перспективні відносини, що підлягатимуть міжнародно-правовому регулюванню.

На нашу думку, на початковому етапі становлення і розвитку філософії міжнародного інформаційного права наявність проблематики, що підлягає теоретичному дискурсу та науковому узагальненню напрямків досліджень може охопити наступне:

міжнародно-правові проблеми розвитку глобального інформаційного суспільства;

міжнародно-правова проблематика щодо категорій «інформація», «свобода інформації», «право на інформацію», «режими інформації»; види використання інформації (у широкому розумінні);

міжнародно-правова проблематика щодо категорій «засоби передачі інформації», «право на комунікацію», «режими комунікації (режими е-комунікації)»; види використання засобів комунікації (е-комунікації);

міжнародно-правові проблеми міжнародна інформаційної і кібернетичної безпеки;

міжнародно-правові проблеми відповідальності суб'єктів за міжнародну інформаційну і кібернетичну діяльність;

міжнародно-правові проблеми сучасного і перспективного міжнародний інформаційного правопорядку.

Вартим буде їх стисла характеристика.

Міжнародно-правові проблеми розвитку глобального інформаційного суспільства, що підлягають теоретичному дискурсу та науковому узагальненню і осмисленню, пов'язані із становленням і розвитком концепції інформаційного суспільства і йдуть шляхом конкретизації основної тематики, визначеної протягом останніх майже двох десятиліть – результатами визначеними Окінавською Хартією глобального інформаційного суспільства 2000 р., результатами Женевського 2003 р., Туніського 2005 р., Женевського 2014 р. етапів Світового саміту з інформаційного суспільства (далі - ССІС).

Загальне бачення міжнародно-правових проблем розвитку глобального інформаційного суспільства, закладено Окінавською Хартією глобального інформаційного суспільства 2000 р., Женевською Декларацією принципів: Побудова інформаційного суспільства в новому тисячолітті 2003 р. Женевським Планом дій 2003 р., Туніським зобов'язанням 2005 р., Туніською програмою для інформаційного суспільства 2005 р.

Продовженням виступають прийняті Світовим самітом з інформаційного суспільства (ССІС+10) у Женеві, у 2014 р., наступні акти, спрямовані на його подальший розвиток: Заява ССІС+10 про виконання рішень ССІС, а також Розроблена ССІС+10 концепція ССІС на період після 2015 року.

Науковому узагальненню і осмисленню підлягають проблеми, пов'язані із реалізацією загальної визначеної мети – побудові інформаційного суспільства, яке б сприяло реалізації потенціалу, сталому розвитку і підвищенню якості життя. Значну роль повинна відіграти і філософія міжнародного інформаційного права.

Міжнародно-правова проблематика щодо категорій «інформація», «свобода інформації», «право на інформацію», «режими інформації»; види використання інформації (у широкому розумінні).

Враховуючи важливість ключової категорії міжнародних інформаційних правовідносин – інформації актуальним, на нашу думку, буде продовження доктринальних досліджень, що віддзеркалять міжнародно-правові підходи до цієї категорії в умовах глобального інформаційного суспільства.

Важливим для наукового узагальнення і осмислення підлягають проблеми, пов'язані із такою правовою категорією, як свобода інформації. Ця тема, що стала класичною при розгляді питань, пов'язаних із правами людини, набуває нових аспектів в умовах глобального інформаційного суспільства - при дослідженні з позицій правового регулювання міжнародних інформаційних відносин, а також як основа для нової і актуальної теми для досліджень – права на інформацію в міжнародних відносинах.

Міжнародно-правовий режим інформації виступає одним із основних проблемних питань в умовах глобального інформаційного суспільства. Проблеми, пов'язані з зазначеним режимом потребують подальшого дослідження, оскільки його визначення, встановлення і реалізація здатні суттєвим чином впливати на усі

види міжнародної інформаційної діяльності суб'єктів міжнародних інформаційних відносин.

Міжнародно-правова проблематика щодо категорій «засоби передачі інформації», «право на комунікацію», «режими комунікації (режими е-комунікації)»; види використання засобів комунікації (е-комунікації)» - виступає окремою темою, оскільки охоплює переважно міжнародно-правове регулювання технічних аспектів отримання, передачі, зберігання, поширення інформації, що в умовах розвитку глобального інформаційного суспільства потребує свого окремого дослідження.

Міжнародно-правові проблеми міжнародної інформаційної і кібернетичної безпеки.

Практичний і науковий інтерес до комплексу питань, пов'язаних з використанням інформаційно-комунікаційних технологій не тільки «на благо», але й «на зло» був викликаний потенційними можливостями їх подвійного застосування. Він посилюється у зв'язку із стрімким зростанням чисельності випадків використання таких технологій з цілями, несумісними із задачами забезпечення міжнародного миру і безпеки. Це новий і широкий напрям досліджень, що потребує особливого наукового підходу, оскільки зачіпає тематику кількох галузей міжнародного права.

До проблематики цього напрямку входять і питання, пов'язані із міжнародно-правовим забезпеченням впровадження глобальної культури кібербезпеки.

Міжнародно-правові проблеми відповідальності суб'єктів за міжнародну інформаційну і кібернетичну діяльність.

Проблематика міжнародно-правової відповідальності виступає однією із самих складних у теорії і практиці міжнародного права. Її дослідженню присвячена значна частина теоретичних робіт вітчизняних і іноземних дослідників. Проте, низка проблем щодо відповідальності суб'єктів за міжнародну інформаційну і кібернетичну діяльність не втрачає своєї актуальності і потребує подальшого наукового осмислення і розв'язання.

Міжнародно-правові проблеми сучасного і перспективного міжнародного інформаційного правопорядку.

Сучасні дослідження в науці міжнародного права окремих аспектів міжнародного правопорядку в інформаційній сфері ґрунтуються на єдиній базовій основі, якою виступає міжнародний правопорядок. Маючи таку єдину базову основу, міжнародний інформаційний правопорядок, разом з тим, має і свої певні особливості, викликані місцем, роллю і значенням міжнародних інформаційних відносин та розвитком їх міжнародно-правового регулювання.

Проблематика міжнародного інформаційного правопорядку, на наш погляд, може містити низку комплексних проблем, актуальними і важливими серед яких, в першу чергу, виступають: визначення складу міжнародних інформаційних правовідносин як складових міжнародного інформаційного правопорядку;

періодизація становлення і розвитку міжнародного інформаційного правопорядку; визначення напрямків і тенденцій розвитку сучасного міжнародного інформаційного правопорядку.

Підсумовуючи, варто зауважити, що зазначена проблематика, яка, на нашу думку, підлягає теоретичному дискурсу та науковому узагальненню напрямків досліджень, в рамках філософії міжнародного інформаційного права, надає ключову уяву. Не наполягаючи на безумовній логічності і повноті, зазначимо, що задача полягала в тому, щоб концептуально поглянути на новий напрям – філософію міжнародного інформаційного права.

*Федорова І. І., к.ф.н., професор
ФСП КПІ ім. Ігоря Сікорського*

ДЕСУБ'ЄКТИВАЦІЯ СОЦІАЛЬНИХ РОЛЕЙ В КОНТЕКСТІ ВІРТУАЛІЗАЦІЇ ТА МЕДІАТИЗАЦІЇ ПРОСТОРУ КУЛЬТУРИ ЗА УМОВ ІНФОРМАЦІЙНОЇ ДОБИ

Сьогодні важко сперечатися з тим, що стрімкі темпи розвитку суспільства інформаційних технологій з його провідним символом – Інтернетом, креативною системою мережевого перекоструювання соціальної реальності, призвели до революційних перетворень усіх сфер життєдіяльності людства. Комп'ютерна комунікація стала культом прогресу доби, домінуючи в професійній діяльності, фінансах, банківських операціях, освітніх практиках, індивідуально-особистісних контактах, створюючи у такий спосіб новий проект соціальної реальності, а також новий спосіб існування у ній людини. Сучасне покоління є свідком появи й укорінення нового типу цивілізації – цивілізації кіберпростору. Цей термін, породжений літературним жанром фентезі, вводить У. Гібсон своєю трилогією “Кіберпростір”, яка містить амбівалентні денотації й конотації (явне – основне і скрите – додаткове значення тексту) свого сюжету і сенсу. До наукового (спершу – філософського) обігу цей термін був введений А. Є. Войскунським, і значна кількість дослідників визначає його, як “простір віртуальної реальності”, що демонструє неоміфотворчу специфіку формування лексики простору культури інформаційного суспільства.

Незважаючи на усі здобутки і переваги технічних інновацій кіберцивілізації, вона породжує багато загроз розвитку соціуму та тривожних викликів людини, її свободі й безпеці існування і спілкування, інтелектуальній незалежності та самопізнанню, можливостям соціальної адаптації, здатності протистояти маніпуляціям інфосфери. Тому сучасне суспільство все частіше науковці визначають як “суспільство ризиків та небезпек”, які за своєю суттю відрізняються від тих, що існували у попередні часи, оскільки є глобальними, антропогенними і майже нерегульованими моральними кодами і правовими нормами, бо не мають кордонів і меж у своєму часово-просторовому континуумі. Затакихумов відбувається переоцінка ціннісних орієнтирів, утверджуються

імперативи морального і правового релятивізму: “тенденція до тотальної автономізації змісту усіх соціальних регуляторів, що виявляються у масовому поширенні серед громадян переконання, згідно з яким право, мораль і релігія повинні підпорядковуватися негайним особистим інтересам та бажанням індивідів [1, с.161].

Сучасні трансформації культурного ландшафту, детерміновані поширенням багатоаспектного феномена інформаційної культури технічними можливостями, при якому формується “простір віртуальної реальності”, або простір “культури реальної віртуальності” за виразом М. Кастельса Остання створює нову ментальну картину, протиставляючи реальну дійсність штучній реальності трансгресивного досвіду (конструкт квазидосвіду іреального). Це можна назвати претензією на нову онтологію виходу за межі реального, оскільки віртуальну реальність можна конструювати. Крім того, таких “реальностей” може бути багато, і вони не створюють цілісну картину світу, а залежать від суб’єктивних уподобань користувача чи мережевого співтовариства. Така ситуація може призвести до десуб’єктивації соціальних ролей і культу індивідуалістичної культури, що продукує соціальну нейтральність або дестабілізуючу агресивність, коли інтерактивність в мережі обертається інтерсуб’єктивною комунікацією у багатомірному, але локалізованому просторі.

У інформаційно розвинутих суспільствах із домінуванням ліберальних цінностей зменшується роль традицій, як регулюючого фактора соціальних відносин (Ю.Хайдегер). При цьому, вирішальною стає автономна самодетермінація особи, яка, занурюючись у віртуальний світ, навмання обирає середовище спілкування, ціннісні орієнтири, моделі поведінки, що визначають шляхи її самореалізації. Культура віртуального простору загрожує історично виробленим способам соціалізації, саморегуляції та самоідентифікації особистості. Фрагментарність та кліповість світосприйняття породжує байдужість, відстороненість від реального буття, нездатність його самостійного досягнення.

Суспільство інформаційної доби переживає кризу ідентичності і самоідентифікації особи. Формується новий тип віртуальної ідентичності: ‘віртуал’ – певна культурно-антропологічна величина світу мережевих комунікацій, цінність якої полягає в анонімності статусу і можливостях вибору множинних варіантів ідентичності. У просторі мережевого спілкування кожен стає суб’єктом і об’єктом одночасно, граючи майже однакові ролі, співвідношення яких змінюється від інтерактивного діяча до пасивного спостерігача, які за правилами віртуального дійства перевтілюються у творців, користувачів чи свідків подій, що не відбувалися насправді. У мережевій комунікації самоідентичність людини – це не процес соціалізації, а нав’язана можливість зіграти певну роль за чужим сценарієм у “грі без правил”. А у подальшому – інтеріоризуючи свій рольовий досвід, застосовувати його до життєвих потреб.

Панівну роль в організації комунікативних процесів у віртуальному просторі відіграють багатовимірні технології масмедіа. Різні канали аудіовізуальної комунікації техніко-технологічно, економічно, естетично трансформували матеріальні й духовні основи соціокультурного простору. Медіакультура створює середовище, у якому стимулюються процеси десуб'єктивації соціальних ролей особи, що означає девалоризацію (перекодування) культурних цінностей і смислів, послаблення творчої інтелектуальної активності людини як суб'єкта і творця культури. Ці явища перетворюють її на "одномірну" (Г. Маркусе), на "середнячка" – пересічну особу, яка є зручним об'єктом для маніпулювання. Функції формування "одномірної" людини вправно і творчо виконує арсенал масмедіа (теле-кіно-інтернет індустрія). Засобами медіатизації відбувається переконструювання реальності (на замовлення) у простір гіперреальностей (Ж.Бодрійяр), який має існувати як "суспільство інтерактивного спектаклю", що продукує певне семіотичне дійство (медійне, вербальне, акторське чи аматорське). Віртуальний простір гіперреальності використовується як поле для випробувань перформативних технологій різними бізнесовими, політичними силами для маніпулювання свідомістю людей, для спрямування їхньої соціальної активності у карнавальне дійство гучного активізму, інтерактивну гру у квазіполітику соціальних перетворень, яка приносить задоволення її співучасникам, "випускає пар" невдоволеного суспільства, але нічого не змінює.

Список використаних джерел:

1. Сунегін С.О. Право, мораль і релігія як соціальні регулятори: об'єктивний та суб'єктивний виміри // . - Вип.28. К.: Інститут держави і права ім. В. М. Корецького НАН України, 2017. – С.145 - 163

*Богачев Р. М., к.ф.н., доцент
ФСП КПІ ім. Ігоря Сікорського*

ПРАВОВА СВІДОМІСТЬ В РИТМІЦІ ІНФОРМУВАННЯ-ПІЗНАННЯ-РОЗУМІННЯ

Історія людства свідчить, що процеси *мережування* протікають постійно, властивість *мережовості* накопичує власний соціально відтворювальний потенціал, а в різних формах актуалізації діяльнісно-спілкувальної сутності кожного-багатьох-всіх формується *мереживо міжсуб'єктного спілкування* як взаємопроникнення *спів-творчості та наслідування*" (Г.С.Батіщев). Саме вони й виступають діалектикою та методологічною основою процесів самоорганізації, а також метою моделювання та прогнозування сучасних соціальних процесів.

На жаль, суспільні практики вимушені постійно наздоганяти діалектику, та в багатьох випадках ірраціональні перетворені форми зумовлюють значні «зигзагі» та манівці процесів самоорганізації, історичного поставання людини і суспільства, зниження рівня накопиченого потенціалу мережовості.

Чому? Доцільно звернутися до праць видатного радянського філософа Олександра Зинов'єва, які присвячені як феномену «комунізму в Росії», так і феномену «западнізму», який достатньо чітко описує процеси, що зараз відбуваються в США та країнах «розвитого капіталізму». Саме адекватне відтворення безперервності поступу дійсної історії в конкретних історичних феноменах потребує звернення до основних теоретичних постулатів О.Зинов'єва: по-перше, твердження, що історія «впливає в соціальні дірки»; по-друге, підвищення рівня соціального захисту зумовлює зниження економічності та ефективності діяльності суспільства; нарешті, вирішальним фактором, що визначає суспільно-політичний тип суспільства виступає людина, якість стосунків та суспільства загалом.

Розглянемо основні «больові центри» сучасного світу: по-перше, зниження загальної ефективності світ-системи зумовлює поглиблення суспільної **несправедливості** розподілу ресурсів та результатів суспільного відтворення, їх споживання, а відповідно призводить до подальшого ще більшого зниження ефективності; по-друге, культ споживацтва та високий рівень соціальних витрат зумовлює відмову від гармонійності як критерію регулювання системи суспільного відтворення, позитивним та правильним вважається все, що підтримує рівень споживання, **правда** як суспільне бачення та потенційний орієнтир для гармонізації системи стає об'єктом маніпулювання; по-третє, для зовнішнього тимчасового збалансування системи **правові норми** підлаштовуються або взагалі ігноруються.

Тому *Ідеологічне* оформлення нових *Ідеалів* та моделей суспільного розвитку має здійснити гармонізацію векторів діяльнісних проявів та сфер **ПРАВА – ПРАВДИ – СПРАВЕДЛИВОСТІ**. Саме ці сфери виступають аналогом та корелятом властивості *мережовості (справедливість)*, процесу *мережування (правда)* та *мереживаяк* результату (**право**).

Почнемо з *Права*. **ПРАВО**. **Право**, як і владу, не випрошують, а беруть-вибудовують! Яке ж має бути ПРАВО в царині мережовості? ПРАВО як *свідоме ПРАВО* та *правова СВІДОМІСТЬ* (за Б.В.Новіковим)!

Як постає суспільна свідомість? Відома єдина належна ритміка: *Людяний досвід – Об'єктивні теорії – Адекватні практики*, – та сходження в царині суспільного відтворення: *Формотворення – Кеультуротворення – Свободотворення*, – або в царині Світо-перетворення: **БІОСФЕРА – НООСФЕРА – КРЕАТОСФЕРА**. Або лапідарно: **ІНФОРМУВАННЯ - ПІЗНАННЯ - РОЗУМІННЯ**.

І в цій ритміці єдиною основою ПРАВА людини, *правом як обов'язком-необхідністю* та *правом як повноваженням-бажанням* виступає **право-відповідальність ТВОРИТИ**.

Тобто з необхідністю в процесі *свідомого ІНФОРМУВАННЯ*, потому *ПІЗНАННЯ усвідомленого* та нарешті їх синтезу в РОЗУМІННІ виховується

здатність вільно накопичувати та актуалізувати властивість *мережовості* для СУСПІЛЬНОСВІДОМОГО Свободотворення.

Тільки так замість *Біологізму* «я хочу» або *Солідаризму* «я повинен» постає ПРАВОсвідоме «Я МОЖУ», спрямоване на **САМОзміну людини** через накопичення і реалізацію потенціалу *мережовості* в переході від суб'єкт-об'єктних до суб'єкт – суб'єктних, а тому й суб'єктісно-суб'єктних взаємозв'язків. Тільки так ПРАВО стає «живим» та свідомим, а СВІДОМІСТЬ – правовою, тільки так процес пізнання і перетворення-творення світу отримує *дійсний критерій ОБ'ЄКТИВНОСТІ* – тобто має в сутності **ПРАВДУ в ритміці ІНФОРМУВАННЯ - ПІЗНАННЯ - РОЗУМІННЯ.**

Це дає чітку визначеність та адекватні відповіді на широке коло ключових питань сьогодення, стає детонатором активних дій, творчого перетворення оточуючого світу і кожного-багатьох-всіх.

*Покулига І. К., к.ф.н., доцент
ФСП КПІ ім. Ігоря Сікорського*

РІВЕНЬ ПРАВОСВІДОМОСТІ ЯК КОМПЕТЕНТНІСНА ХАРАКТЕРИСТИКА ОСОБИСТОСТІ У КРИТЕРІЯХ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ

Правосвідомість є однією із центральних категорій філософії права, як у її класичних виявах, так і в різноманітних сучасних теоріях. Мислити критеріями свободи, волі, справедливості; оцінювати вчинки й усвідомлювати неминучість покарання не лише у вимірах законності чи навіть користі, а й в основній меті права, як «об'єктивного духу» (Г.В.Ф.Гегель), стає одною із важливих підстав для оцінки рівня індивідуальної культури, досвідченості, інтелігентності. Ідеться не про спеціальні знання у сфері юриспруденції, які пов'язані з конкретними напрямками діяльності, а про те, що повинно бути властиво людині незалежно від її професії. Дійсно, кожен з нас виконує такі ментальні процедури, як ідентифікація вчинків, комунікативних дій та самого суб'єкта цих дій у параметрах відповідності нормам, смислам та ціннісним орієнтирам права. Отже, не володіючи певною компетентністю, юридичною освітою, ми все ж не можемо бути індиферентними й не надавати оцінку, охоплюючи ситуацію всім «рельєфом» правосвідомості на тому рівні індивідуальної культури, що сформований на взірцях та прикладах із життєвого досвіду, документально-хронікальної, художньої літератури, кіномистецтва, телефірів тощо.

Сучасна інформаційна культура пов'язана у своїх визначальних параметрах із медіа-сферою суспільства, що включає у відцифрованому варіанті історичний і сучасний досвід – тексти різних епох, поколінь. Отже, орієнтує сьогоdnішнього користувача інтернет-комунікації на реалізацію одних із життєво важливих прав людини – інформаційних, вільний доступ до їхніх різних джерел. Складається

цивілізаційна основа зручних умов тотальної проінформованості, миттєвого доступу до бажаного тексту, незалежності від інтерпретації транслятора (принаймні можливості співставити різні формулювання) тощо. Усі зазначені фактори мають місце, але «в пакеті» з ними. Або навіть на перший план виступають й інші параметри змін інформаційної культури – знецінення знань («розширена» свідомість, кліпове мислення і т.д.); втрата авторитетів – нівелювання, розпорошення експертної оцінки інформації; можлива анонімність її джерела, водночас публічність без критичного осмислення соціальних наслідків та багато інших трансформованих сенсів культури сучасного інформаційного суспільства, на яких виховуються представники «google-покоління».

Серед зазначених вище ризикованих, на мою думку, нових стандартів розвитку інформаційного простору є такі, що вже тривалий час викликають занепокоєння й навряд чи зникнуть без відповідної ролі інформаційного права й просвітницьких зусиль у напрямі індивідуальної правової культури. Насамперед це знецінення знання, не усвідомлення нетотожності легкої доступності інформації, фактичної її безкоштовності та причетності користувача до авторства тексту, як наслідок – неврегульованість правової оцінки такої важливої власності, як інтелектуальна. Ідеться не про закон або норми патентного права і не про «смерть автора» (Р.Барт), як стильову платформу діалогості у прийомах постмодернізму, а про «розмивання», нівелювання самої компетентності для «google-покоління» у питанні того, що науковий, художній та інший текст має свого творця. І цим автором не є той, хто потребує того чи іншого інтелектуального «продукту». Він часто лише привласнює його. Катастрофічним у контексті правосвідомості, на мою думку, стає не сам факт безпідставного володіння даною власністю, а відсутність усвідомлення, що автор не ти!

Це явище ініціює комплекс інших факторів – трансформацію смислових критеріїв самооцінки знань, потреби запам'ятовувати інформацію. Навіщо? У разі необхідності можна буде швидко все знайти. Інтелект нібито не обмежується власним знанням, він може «розтягуватися», «розбухати», чіпляючись за гіпертекст на просторах інтернету. Суб'єкт такої комунікативної процедури, фахівець із серфінгу на хвилях океану інформації (Ж.Дельоз) вільно (із гаджетом в руках) розмовляє на різні теми й одразу забуває, проартикулювавши фразу, про що він говорив.

Ці доволі сумні ескізи до карикатурного портрету користувача мультимедійною технікою є тим негативним прикладом, анти-образом носія сучасної інформаційної культури, змалювавши який хотілося б вірити у протилежне: в актуалізацію правосвідомості й розуміння дійсних свобод людини – прав на розум, свою пам'ять та відповідальність перед вищим законом – власною совістю.

ІНФОРМАЦІЙНА КУЛЬТУРА – ЗАПОРУКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Наразі політичний та соціальний дискурс в українському медіапросторі переповнений такими поняттями як: «інформаційна війна», «інформаційне протиборство», «гібридна війна», «інформаційна зброя» тощо. Майже кожен експерт чи політик вважає своїм обов'язком наголосити на цих поняттях в тому чи іншому контексті. При цьому реципієнти такого медіа контенту, так само як і його спіч-мейкери, часто вкладають у дані поняття досить різне значення. Наразі з тлумаченням цих та інших понять пов'язаних з аспектами забезпечення інформаційної безпеки визначились на законодавчому рівні, що унеможливило надмірне спекулювання даною термінологією. Йдеться, перш за все, про наявність в державі Доктрини інформаційної безпеки України, прийнятої рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року.

Зазначимо, що в правовій доктрині є перелік дискусій з приводу деяких тверджень зазначеного нормативно-правового акту, їх змістовного наповнення, а також відповідності реальним та потенційним загрозам в інформаційній сфері. Втім, чіткість позиції держави в ситуації, що склалась на території України при прийнятті даної Доктрини є очевидною – країна знаходиться у стані «інформаційної війни» або «гібридної війни». Обидва твердження рівноцінно застосовуються в представленій Доктрині.

Аналізуючи дискурс європейської спільноти щодо України, можна сказати що наші міжнародні партнери роблять висновки щодо розколу українського суспільства, надмірну ворожнечу та радикальні настрої з актуальних нині питань. Тож, хотілося б наголосити, що, говорячи про протидію зовнішнім інформаційним загрозам необхідно не забувати про внутрішні. Серед актуальних загроз національним інтересам та національній безпеці України вищезазначена Доктрина звертає окрему увагу на «недостатній рівень медіа-культури суспільства».

Виходячи з аналізу змісту чинної Доктрини інформаційної безпеки України, серед національних інтересів України в інформаційній сфері виділяють також «розвиток медіа-культури суспільства та соціально відповідального медіа-середовища». З цього можна зробити висновок, що одним із пріоритетів держави в межах протидії сьогоденним загрозам в інформаційній сфері є підвищення рівня медіа-культури суспільства через впровадження державних програм її розвитку. На практиці ситуація дещо інша, адже, судячи з проектів, які стосуються медіаосвіти та медіаграмотності, цим питанням більше переймаються інститути громадянського суспільства, аніж держава. Враховуючи факт наявності інформаційної агресії зазначимо, що пілотні проекти, зокрема, освітні експерименти з медіаграмотності у школах, є мізерно малим зусиллям держави у

співвідношенні з актуальними інформаційними загрозами, які постають перед українським суспільством кожного дня.

На завершення, хотілося б звернути увагу на ще один аспект – невизначеність заявленого в Доктрині стратегічного наративу. В документі досить чітко дається тлумачення даної дефініції, втім, в політичному дискурсі, конкретність майбутнього стратегічного наративу у разі обрання того чи іншого кандидата більша, ніж в державному.

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

ІНТЕРНЕТ У СИСТЕМІ ПОШИРЕННЯ ІСЛАМСЬКОГО РАДИКАЛІЗМУ: ПРИКЛАД НІМЕЧЧИНИ

Сьогодні іслам як релігія і культура став невід'ємною частиною німецького повсякденного життя, і продовжує активно поширюватися по всій країні. Перша хвиля мусульман-мігрантів до Німеччини відбулась у 50-і роки минулого століття з Туреччини. Проявляючи толерантність до мусульман-мігрантів, влада Західної Німеччини дозволила їм будувати мечеті які сьогодні можна побачити в багатьох великих містах; жінкам-мусульманкам дозволено щодня носити національний одяг та закривати свої обличчя хусткою (хіджаб). Приймавши нове громадянство, турецькі мігранти так і не стали повноцінними громадянами нової батьківщини, не змогли або не захотіли (це окреме дослідження) інтегруватися ані за культурою, ані за менталітетом. Вони зберігають свою самобутність, створюючи національні анклавні у багатьох містах Німеччини. За своєю ментальністю чоловіки слідує своїм культурним традиціям – цілими днями сидять у вуличних кафе, п'ють каву і курять кальяни, займаються дрібним бізнесом, або задовольняються державною соціальною допомогою. Багато з них не володіє і не вивчає мову держави в якій вони є повноцінними громадянами.

Таким чином, у сучасній Німеччині склалося подвійне культурне товариство, з одного боку німецько-християнське, а з іншого, арабо-мусульманське.

Друга масова хвиля мусульман мігрантів у Німеччину почалась з осені 2015 року після загострення бойових дій на Близькому Сході і Африці, і появи Ісламської Держави Іраку і Леванту, яке проводило планомірний геноцид населення Іраку і Сирії.

В період з 2010 по 2016 роки мусульманське населення у Німеччині збільшилося з 3.3 мільйона, що становило 4.1% від загальної кількості населення до 5 мільйонів, або 6.1% відповідно. В цей же час німецьке населення знизилося з 77.1 мільйонів до 76.5 мільйонів. Причини для збільшення мусульманського населення дві: перша, це нова хвиля мігрантів з арабських і африканських країн,

охоплених війнами; друга - це високий відсоток народжуваності серед вже проживаючих мігрантів [1].

Молоді мусульмани як першої, так і другої хвилі мігрантів, не інтегруються в німецьке суспільство, для них воно чуже. Такі люди стають дуже вразливими для впливу різних радикальних мусульманських і політичних груп, які ведуть свою «священну війну» (джихад) проти «невірних». Для пропаганди своїх екстремістських ідей, такі радикальні групи використовують Інтернет, зокрема соціальні мережі та окремі сайти.

Починаючи з 2014 року та виникнення Ісламської Держави Іраку і Леванту (далі ІДІЛ), країни Європи стали розглядатися радикальними ісламістами як території їхньої майбутньої імперії. Основний акцент для своїх дій, радикали спрямували на мусульман як першої хвилі, так і другої - біженців з арабських країн.

Ісламські фундаменталісти оцінили можливості інформаційного суспільства та Інтернету, зокрема, поширення екстремістських матеріалів стало набагато простіше з будь-якої точки планети. Для своєї пропаганди на території Німеччини вони використовують соціальні сайти: "FaceBook", "Youtube", "Twitter" та інші. Форми викладення матеріалу мають текстові файли, малюнки, фото-, відеоматеріали та звукозаписи. Інформація поширюється без фізичної присутності, що дозволяє приховувати особистості їх розповсюджувачів.

Так як психіка дітей вважається ще не повністю сформована (чистий розум), то одним із напрямів діяльності ІДІЛ стала пропаганда радикального ісламу і насильства серед неповнолітніх верств населення Німеччини. Через соціальні мережі та сайти миттєвих повідомлень ІДІЛ намагається зацікавити потенційних жертв в ідеях радикального ісламу, проводить інструктажі та вербування до своїх лав, підштовхує жертв здійснювати одноосібні терористичні акти проти німецьких громадян, та працівників силових структур. Аналіз інтернет-інформації свідчить, що з 900 завербованих ІДІЛ німців 20% були діти віком 13-14 років. Німецька контррозвідка назвала таких терористів "дитсадкові джихадісти". Крім того, ІДІЛ веде пропаганду серед батьків для того, щоб потім вони вели ісламську пропаганду серед своїх дітей [2, 3].

Розуміючи наслідки поширення ідей ісламського радикалізму, які можуть привести до ісламізації Німеччини і втрати національної самобутності, правоохоронні органи активно розвивають систему інформаційної безпеки і протидіє небезпечним викликам в інформаційній мережі. Одним з головних державних органів для захисту інформаційної безпеки є Німецький Федеральний Орган Інформаційної Безпеки. Цей орган забезпечує безпеку в сфері інформаційних технологій, для державних структур та фізичних осіб [4].

Служби безпеки Німеччині намагаються відстежувати в країні мусульман-екстремістів серед біженців з охоплених війною Арабських і Африканських країн. Постійно ведеться моніторинг інтернет-листування таких осіб, встановлюються їхні інтернет-зв'язки та наміри. Стандартні пошукові запити включають

інформацію про іслам, відео боїв в Сирії, інформацію про ІДІЛ та відео страт на арабському сході. Головна небезпека поширення ідей ісламського радикалізму полягають у появі нових ідейних сторонників цієї політико-релігійної ідеології.

У вересні 2015 року, уряд Німеччини створив робочу групу до якої входять державні організації, технологічні компанії, асоціації індустріалістів і незалежних активістів, яка повинна працювати з Міністерством юстиції задля протидії ісламській пропаганді та екстремізму в інтернеті. У грудні 2015 року, Google, Facebook, Twitter погодилися співпрацювати з Міністерством юстиції, щоб разом протидіяти ісламському екстремізму в цифровому просторі. [5]

Разом з тим, незважаючи на спроби уряду протидії загрози в інтернет-просторі, дана проблема ще далека від вирішення. Інформаційний простір не має меж, що дає широкий діапазон для різних маніпуляцій і дій, в ньому немає меж і правових кордонів. Тільки за допомогою колективних дій всіх членів Європейського Союзу та інших близьких до них держав може бути розроблена загальна стратегія боротьби проти ісламського фундаменталізму на безмежних просторах Інтернету.

Якщо це не буде зроблено, ситуація може призвести до появи контр-радикальних організацій в Німеччині, які почнуть самі здійснювати активну діяльність у боротьбі проти фундаменталістів. Поступово німецькі право радикальні сили починають проявляти агресію проти мігрантів-мусульман і так само проти уряду, зокрема, канцлера Ангели Меркель. Прикладом цього служать події 30 серпня 2018 року в Берліні, і проникнення в ряди Бундесверу нацистів для замаху на німецьких політиків пов'язаних з міграційною політикою [6,7]. У подальшому, німецьке суспільство може чекати конфлікт між радикально налаштованим корінним населенням і мігрантами, що неминуче призведе до етно-релігійного конфлікту.

Список використаних джерел:

1. The Growth of Germany's Muslim Population. URL: <http://www.pewforum.org/essay/the-growth-of-germanys-muslim-population/>
2. Germany Alarmed by 'Kindergarten Jihadists'. URL: <https://www.voanews.com/a/germany-alarmed-by-threat-posed-by-child-jihadists/4236346.html>
3. Islamic State using online 'headhunters' to recruit young Germans. URL: <https://www.reuters.com/article/us-germany-security-idUSKBN1531ZM>
4. Taking advantage of opportunities – avoiding risks. URL: https://www.bsi.bund.de/EN/Home/home_node.html
5. Germany: Extremism & Counter-Extremism. URL: <https://www.counterextremism.com/countries/germany>
6. German Far Right and Counterprotesters Clash in Chemnitz. URL: <https://www.nytimes.com/2018/08/28/world/europe/chemnitz-protest-germany.html>
7. Нацисти в армії. У Німеччині розкрили змову. URL: <https://ua.korrespondent.net/ukraine/4032378-natsysty-v-armii-u-nimechchyni-rozkryly-zmovu>

*Пилипчук В. Г., д.ю.н., професор,
член-кореспондент НАПрН України,
директор Науково-дослідного інституту
інформатики і права НАПрН України*

АКТУАЛЬНІ ПРОБЛЕМИ ДЕРЖАВНОЇ ПОЛІТИКИ З ПИТАНЬ ЗАХИСТУ ПРАВ І БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Протягом останніх років в українському суспільстві спостерігається тенденція до все більшого розуміння важливості проблем розвитку інформаційної сфери та необхідності забезпечення інформаційної безпеки в усіх сферах життєдіяльності людини, суспільства і держави. Водночас, як свідчить аналіз, система забезпечення інформаційної безпеки ще залишається недостатньо ефективною і такою, що не повною мірою відповідає національним інтересам України.

За результатами проведених досліджень, нині першочергової уваги потребують такі **ключові загрози національній та міжнародній безпеці в інформаційній сфері**:

– глобальні зміни і трансформації в інформаційній сфері формують новітні виклики і загрози, які становлять реальну загрозу безпеці людства та міжнародному правопорядку;

– в інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства, періодично проводяться інформаційно-психологічні операції;

– більшість країн світу зіштовхнулися з проблемами кібершпигунства, кібертероризму, кіберзлочинності та кібератаками на об'єкти критичної інфраструктури;

– наслідки використання сучасної інформаційної зброї можуть призводити до реальної втрати державного суверенітету і територіальної цілісності країн світу.

Рівень сучасних викликів і загроз в інформаційній сфері наочно підтверджує справедливість і виключну значимість положень ст. 17 Конституції України про те, що **забезпечення інформаційної безпеки є однією з основних функцій держави і справою всього Українського народу**.

Враховуючи зазначене, звернімо увагу на деякі актуальні проблеми, що стосуються інформаційної сфери і потребують належного правового врегулювання.

Перше. Актуальною залишається **проблема розробки та реалізації ефективною державної інформаційної політики**. Певною мірою це можна

пояснити низкою об'єктивних і суб'єктивних чинників, починаючи від задекларованого внесення змін до Конституції України та прийняття необхідних нормативно-правових актів і закінчуючи питаннями кадрового та іншого ресурсного забезпечення.

Друге. Не менш складною є ситуація з **забезпеченням інформаційної безпеки** України, де існує низка політико-правових, організаційних та інших проблем. Наприклад, як зазначалося, сфера інформаційної безпеки згідно з Конституцією України є складовою системи забезпечення національної безпеки. Однак, у прийнятому 2018 року Законі «Про національну безпеку України» йдеться лише про контррозвідувальний захист інформаційної безпеки Службою безпеки України, а системно ця сфера взагалі не розглядається.

Третє. Вкрай актуальною, в сучасних умовах розвитку інформаційних технологій та інформаційного суспільства та ведення гібридної війни проти України, постає проблема **захисту приватності, прав і безпеки людини** в інформаційній сфері, яку слід розглянути більш предметно.

Насамперед зауважимо, що правове регулювання захисту приватності на європейському континенті почало активно формуватися у другій половині ХХ століття. Першим етапом його розвитку можна вважати прийняття низкою європейських країн відповідних національних законів. Головною передумовою їх розробки були розвиток телекомунікаційної сфери, створення та поширення відомостей з автоматизованих баз даних та потреба у забезпеченні приватного життя людини відповідно до принципів, визначених основоположними міжнародно-правовими актами з прав людини.

Результати проведених досліджень [1, 2, 3, 4] свідчать, що на теренах континентальної Європи намагання виокремити об'єкт правової охорони, який би відображав суспільну потребу в захисті приватності або «автономії» особи, створив передумови до формулювання теорії «прав особистості», тобто невідчужуваних природних прав, пов'язаних із людиною як біосоціальною істотою. Вченими пропонувалося визнати низку особистих немайнових благ, які містили компонент *інформації про особу*, зокрема *інтимну сферу, індивідуальність, власне зображення*. Поряд із обговоренням сутності прав особистості було висловлено думку про єдиний справжній об'єкт правової охорони – *інтимна сфера життєдіяльності індивіда в усіх її проявах*.

Зокрема, вчений в галузі цивільного права Покровський І.А. слушно зауважував: *«Чим далі, тим більше спостерігається рух права по шляху охорони людської особистості як такої в усій сукупності її індивідуальних інтересів та особливостей... Все більше у праві йдеться про права на охорону інтимної сфери людини... та утвердження індивідуальності...»* [5].

Загалом, в індустріальну добу сукупність відомостей про особу не становила цілісного об'єкта правової охорони, але наразі виникли передумови для надання правового захисту особі від посягань на будь-які «інформаційні прояви» її «автономної» особистості. У подальшому розпочалося опрацювання ідеї про

необхідність розгляду *сукупності інформації про фізичну особу як об'єкта правової охорони*, а її розвиток знайшов відображення у так званій концепції «права на приватність» (right to privacy). При цьому, соціальні та економічні зміни змусили правознавців порушити питання про необхідність розробки *права особи «на саму себе», права «бути залишеною на самоті»*.

Слід зауважити, що англійською мовою усі сторони приватного життя позначаються терміном «*privacy*». Одна із перших спроб сформулювати суть поняття «*privacy*» була зроблена 1890 року відомими американськими вченими С. Уорреном і Л. Брандейсом, які визначили його як «*the right to be alone*» – «*право бути залишеним у спокої*». 1928 року цю ідею підтримав суддя Верховного суду США Л. Брандейс, який офіційно заявив про наявність в Конституції США «*права бути залишеним у спокої*» [6].

С. Уоррен і Л. Брандейс стверджували, що «приватності» людини існує загроза з боку нових винаходів і методів ведення бізнесу, та обґрунтовували необхідність створення спеціального «права на приватність». Автори розуміли, що технічний прогрес і розвиток технологій в майбутньому внесе корективи у правове регулювання питання «приватності». Розраховуючи на тривалу актуальність своїх ідей про «приватність», автори зазначили, що це право має бути гнучким і здатним прилаштовуватись до потреб сьогодення, а також визначили низку важливих і нині постулатів [7]:

– *право на приватність не повинно забороняти публікацію матеріалів, що становлять суспільний або загальний інтерес;*

– *право на приватність припиняє діяти після публікації фактів самою особою або з її згоди;*

– *підставою для позову про компенсацію або судову заборону має бути не шкода, заподіяна репутації, а порушення права на приватність;*

– *відсутність «злого умислу» з боку публікатора не може слугувати виправданням для нього;*

– *закони повинні визнавати і захищати право на приватність.*

Аналіз судової практики захисту «права на приватність» свідчить про те, що його об'єкт не носив суто інформаційної природи, про що свідчать матеріали узагальнення прецедентної практики. Зокрема, у 1960 році на основі висновків американського вченого В. Проссера «*делікти проти приватності*» (privacy torts) було розділено на чотири групи [8]:

1) *втручання в усамітненість (intrusion upon seclusion) – вторгнення в «особистий простір» індивіда;*

2) *публічне розголошення інтимних фактів (publication of private facts);*

3) *спотворене представлення особи перед громадськістю (false light);*

4) *використання чужого імені або образу з корисливою метою (appropriation).*

За нашими оцінками, основу захисту приватності життя людини в сучасних умовах глобалізації та розбудови інформаційного суспільства становить система захисту її персональних даних.

Одним із перших теоретичну основу концепції персональних даних як об'єкта інформаційних відносин розробив Департамент охорони здоров'я, освіти та добробуту США. Зокрема, у Кодексі сумлінного поводження з інформацією (1973 р.) було сформовано принципи поводження з персональними даними [9]:

«– не повинно існувати жодної системи накопичення відомостей про індивіда, саме існування якої тримається в таємниці;

– індивід повинен мати можливість дізнатися, які відомості наявні про нього та як вони використовуються, запобігати тому, щоб інформація, одержана про нього з однією метою, надавалася для іншої мети без його згоди;

– виправити або доповнити відомості про себе;

– будь-яка організація, яка створює, утримує, використовує або поширює відомості стосовно встановлюваних осіб, зобов'язана забезпечити достовірність даних для наміченої мети та вжити розумних пересторог для попередження неправомірного користування даними».

Важливість формулювання цих принципів видається беззаперечною і багато з них нині знайшли своє відображення у національних законах про захист персональних даних та міжнародно-правових актах, що стосуються захисту приватного життя та індивідуальних свобод («рiвасу») у зв'язку з обробкою персональних даних.

Правові стандарти ЄС та норми міжнародного права визначають основні принципи захисту приватності та персональних даних людини відповідно до яких ці дані повинні: 1) бути доступними для суб'єкта даних; 2) бути точними і оновлюватися; 3) бути отриманими законним способом; 4) оброблятися з конкретною метою, за згодою на це суб'єкта даних та в кількості, мінімально необхідній для визначеної мети; 5) використовуватися лише для визначеної мети; 6) бути захищеними від несанкціонованого доступу та незаконної обробки. В цілому, будь-яка обробка персональних даних має здійснюватися законно, справедливо, бути прозорою для суб'єктів даних та виконуватися лише згідно з конкретно визначеною метою.

В Україні, як свідчить аналіз, формування правових основ та системи захисту персональних даних розпочалося лише наприкінці ХХ – на початку ХХІ століття. Нині у цій сфері головна проблема полягає у **відсутності ефективної загальнодержавної системи захисту персональних даних**, належного організаційно-правового механізму регулювання відносин та відповідальності за здійснення правопорушень. Водночас, стрімко збільшується *прірва між безпрецедентними можливостями сучасного Інтернет-середовища і традиційними, “доцифровими” юридичними нормами і практиками*, базованими на традиційному уявленні про межі й засоби забезпечення приватності життя людини.

Об'єктивна необхідність захисту приватності, індивідуальних свобод і безпеки людини в умовах глобалізації та розбудови інформаційного суспільства значною мірою визначається потенційною загрозою тотального контролю за приватним життям людини за допомогою сучасних інформаційних технологій, систем і мереж (*Інтернету речей, Хмарних технологій, Великих Даних тощо*), а також поширенням неправомірних і несанкціонованих дій з персональними даними фізичних осіб, які продовжуються на національному, регіональному та міжнародному рівнях. Це вимагає додаткових ресурсів і пошуку нових ідей у підвищенні правової ефективності захисту приватності, прав і безпеки людини в інформаційній сфері.

З урахуванням зазначеного, аналізу і прогнозування глобальних процесів в інформаційній сфері, першочергової уваги та системного опрацювання потребують такі **основні проблеми**:

1) становлення і розвиток національної системи інформаційної безпеки, зокрема:

– удосконалення *державної інформаційної політики та політики інформаційної безпеки*, а також належного правового, організаційного, науково-технологічного, кадрового та іншого ресурсного забезпечення її реалізації;

– розвиток *національної системи кібернетичної безпеки*, згідно з прийнятими нормативно-правовими актами і стандартами країн-членів НАТО. Це стосується захисту *об'єктів критичної інфраструктури, державних реєстрів і баз даних*;

– опрацювання правових, організаційних, технічних та інших питань протидії *інформаційному насиллю та використанню мереж соціальних комунікацій на шкоду людині, суспільству і державі*. (Як приклад – фактів масового збирання даних користувачів Фейсбук та їх застосування для негативного впливу на суспільство й інтереси окремих держав);

– розгляд питання щодо *переведення системи протидії інформаційній агресії* проти України в режим «активної інформаційної оборони», насамперед, щодо запобігання нанесення шкоди життю і здоров'ю людини та захисту національних інтересів;

2) організація належного захисту прав, свобод і безпеки людини в інформаційній сфері, насамперед, щодо:

а) реформування *національної системи захисту персональних даних* відповідно до “Пакету захисту даних” ЄС, який набув чинності у травні 2018 року і запровадив такі **базові принципи** роботи з персональними даними: *законність, справедливість, прозорість, цільове обмеження, зведення до мінімуму даних, точність, обмеження терміну зберігання, цілісність і конфіденційність*;

б) врахування прецедентної судової практик інших країн-членів ЄС, США і НАТО стосовно визначення «**деліктів проти приватності**» (privacy torts):

– *втручання в усамітненість (intrusion upon seclusion)* – вторгнення в «*особистий простір*» індивіда;

- публічне розголошення інтимних фактів (*publication of private facts*);
- спотворене представлення особи перед громадськістю (*false light*);
- використання чужого імені або образу в корисливих цілях (*appropriation*);

в) опрацювання проблем захисту приватності та інформаційної безпеки людини в умовах впровадження новітніх інформаційних технологій: *штучного інтелекту, Інтернет-речей, «хмарних» технологій, Великих Даних* тощо;

3) **оптимізація законодавства з питань державної інформаційної політики, захисту прав і безпеки людини в інформаційній сфері.** Насамперед, це стосується внесення системних змін і доповнень до законів України «Про інформацію», «Про захист персональних даних» та інших нормативно-правових актів з урахуванням правових стандартів з питань захисту приватності та персональних даних, визначених «Пакетом захисту даних» Європейського Союзу, прийняття Закону України «Про засади інформаційної безпеки» тощо.

В цілому, за нашими оцінками, державна інформаційна політика, у т.ч. з питань захисту приватності, прав і безпеки людини в інформаційній сфері, та система інформаційної безпеки мають бути спрямовані на **ефективний захист об'єктів національної безпеки: людини і громадянина** – їх конституційних прав і свобод; **суспільства** – його духовних, морально-етичних, культурних, історичних, інтелектуальних та інших цінностей; **держави** – її конституційного ладу, суверенітету, територіальної цілісності й недоторканності.

Список використаних джерел:

1. *Пилипчук В.Г., Дзьобань О.П.* Інформаційне суспільство : філософсько-правовий вимір : Монографія / Пилипчук В.Г., Дзьобань О.П. – Ужгород : ТОВ «ІВА», 2014.–284 с.

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

3. *Пилипчук В.Г., Брижко В.М.* Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України / В.Г. Пилипчук, В.М. Брижко // Вісник Національної академії правових наук України. – Харків: «Право». – № 3(90). – 2017. – С. 36-50.

4. *Пилипчук В.Г., Брижко В.М.* Реформування і розвиток системи захисту персональних даних в Україні / В.Г. Пилипчук, В.М. Брижко // Інформація і право. К., 2017. – № 3 (22). – С. 5-21.

5. *Покровский И.А.* Основные проблемы гражданского права : монография / И.А. Покровский. – М.: Статут, 2001. – С. 125.

6. *Яременко О.І.* Право на таємницю приватного життя людини в умовах становлення в Україні інформаційного суспільства. – Режим доступу : <http://www.lawyer.org.ua/?w-p&i-10&d-362>

7. *Уоррен С., Брандейс Л.* Право на приватність // Право США. – № 1-2/2013. – С. 151-152.

8. *Bennett C.J., Raab C.D.* Taking the Measure of Privacy : Can Data Protection be Evaluated? // International Review of Administrative Sciences. – 1996. – № 4 (62). – P. 31-32.

БАЛАНС ПРАВ І СВОБОД В ІНФОРМАЦІЙНІЙ СФЕРІ ЗА УМОВ ПОСТПРАВДИ

Ситуація «постправди» в інформаційній сфері має декілька аспектів, а саме: теоретико-методологічний, семантично-ідеологічний, морально-етичний та нормативно-юридичний аспекти. Аби проаналізувати особливості правничих вимірів постправди в інформаційному полі, доречно сказати декілька слів й про наукові витoki цього концепту та його межі. Термін «постправда» настільки став популярним, що набув характеристики «слова року» (post-truth) від редакції Оксфордського словника. За допомогою такого терміну описуються масові комунікації як публічно-друкованого, так й публічно-мережевого просторів, в яких істина – це головна цінність наукового пізнання за доби зростання науки і раціонально-критичного мислення, поступається суб'єктивній думці, інтуїції, миттєвому враженню тощо, тобто раціо поступається емоції. Громадська думка при цьому інтерпретується не як верифікований вимір, який можна аналізувати, прогнозувати, виявляти панівні тенденції, а як осердя емоцій та особистісних переконань.

Ситуація постправди позначає неважливість для учасників комунікативних практик емпіричних фактів, наукових, тобто об'єктивних критеріїв, і як наслідок відмову від істини і універсальних цінностей і норм. Пост-фактуальна політика (politic) порушує усталені і легітимізовані правила і процедури (policy). Відтепер активне просування в інформаційній сфері індивідуальної позиції, неаргументованої, симулятивної часто-густо призводить до успіху і потрібного результату, навіть якщо мовець постійно спирається на неправду. Складається ситуація, за якою правда не так вже й потрібна у разі, коли є набір переконань. Істина і правда потребують рефлексії й осмислення в аксіологічному обрії і це ускладнює соціальну реальність й утруднює опанування нею, а індивід знаходить затишок у віртуально-фейковому світі.

Зневага до модерної теорії істини загрозлива через те, що логічним наслідком такої епістемології стає відмова від загальнозначущих моральних належностей і загальнолюдських цінностей. Змінюються критерії добра і зла, норми та межі їхнього порушення, відбувається локалізація всезагального блага і фундаменту спільнотуття. Втрачають сенс такі важливі поняття-засновки модерного суспільства, як людство, права людини, свобода, справедливість, солідарність, толерантність тощо.

Розвиток комп'ютерних технологій, масовість їхнього виробництва і поширення, мода на різного ґатунку гаджети та пов'язані з ними форми ідентифікації і визнання молодих людей через їхню «крутизну», легкість доступу до способів поширення й підробки інформації, зрештою зміщення центру соціального з безпосередніх стосунків в віртуальний світ – всі такі соціально-

об'єктивні процеси призводять до того, що підробки, симулякри, перетворені форми сприймаються як правда та істина.

Людина, перебуваючи в інформаційному просторі, наражається на чималу кількість фейкової інформації, посиленої цифровими технологіями. Особливо таке становище дається в знаки сьогодні, під час спроб деяких світових політиків змінити усталений після Другої світової війни і Гельсінських угод 1975 р. соціальний порядок. Тому варто знайти інструменти протидії таким явищам, а також запобіжники і засоби їхнього попередження. Можна казати про посилення дисципліни в інформаційному просторі, але як її контролювати? Ефективними є звичайно культурні, свідомі мотиви блогера, коли він послуговується етичними категоріями честі і гідності, свободи волі і вибору, поваги до думок інших учасників дискурсивних практик. Проте тільки просвітництва недостатньо. Треба запроваджувати правові норми і відповідальність за фейки і цільову брехню. Ми, філософи і правники, маємо реальні ресурси діяти разом у напрямі відокремлення істини від хиб, правди від брехні, просвітництва від маніпуляції.

У чому полягає небезпека постправди? Є дві позиції: по-перше, вона полягає в тому, що ставить під сумнів існування істини як такої, отже й науки як такої: по-друге, розмивається смислове поле понять істина/хиба, правда/неправда, добро/зло, законне/незаконне тощо, на кшталт твердження: «у кожній людині своя правда і добро». Так, ми різні, нетотожні, егоїстичні, зрештою самотні, проте людство через свої трагедії і драми сформувало умови для, як писав К. Ясперс, спілкування на засадах загальнолюдських цінностях і пріоритету прав людини.

*Чепульченко Т. О., к.ю.н., доцент,
ФСП КПІ ім. Ігоря Сікорського*

ПРАВА ЛЮДИНИ: БАЛАНС ІДЕЙ

Права людини вивчають паралельно із такими категоріями як свобода, рівність, гідність та ін. і можуть пов'язуватися з кожною із цих категорій окремо. І такі дослідження збагачують наукову юридичну доктрину, сприяють удосконаленню самого інституту прав людини та, відповідно, забезпечують обізнаність суспільства щодо змісту цих прав.

Світова спільнота підтвердила своє бажання захистити людину та її права. Результатом цього стали такі документи як Загальна декларація прав людини 1948 р., Конвенція про захист прав людини і основоположних прав 1950 р., Європейська соціальна хартія 1961 р. та ін. Зокрема, курс нашої держави на європейські стандарти у даній галузі передбачає узгодження національного законодавства відповідно до цих стандартів, головною цінністю яких визнається людина.

В історії юридичної теорії та практики різних народів склалися такі основні підходи до розв'язання проблеми прав людини, зокрема, правового статусу особи [6, с. 214-223]:

1. Ліберальна (європейська) концепція прав людини базується на ідеї природних, не відчужуваних прав людини та обґрунтовує необхідність конституційного визначення таких умов, які б сприяли вільному розвитку особи. Філософською основою цієї концепції є вчення про свободу як про природний стан людини, її життя як найвищої соціальної цінності. Вперше дана концепція знайшла своє відображення в Декларації незалежності США 1776 р. та в Декларації прав людини і громадянина 1789 р. (Франція).

2. Колективістська концепція заснована на визнанні пріоритету колективу (суспільства, класу, об'єднання тощо) по відношенню до особи, а також на обмеженості прав людини суспільними інтересами. Втілення положень колективістської концепції в "соціалістичних конституціях" призводило на практиці до градації основних прав (головними з яких вважалися соціально-економічні), дискримінації окремих категорій громадян (за класовою ознакою, майновим станом тощо) та до закріплення широкого кола обов'язків громадян перед суспільством і державою.

3. Ісламська концепція прав людини пов'язана з традиційним мусульманським правом, зміст якої полягає у тому, що вселенський суверенітет належить Аллаху, людина не вільна розпоряджатися собою та всі її дії наперед визначені Аллахом, а це, в свою чергу, дозволяє на підставі релігійних канонів виправдати обмеження прав людини.

4. Традиціоналістські концепції, суть яких зводиться до того, що людина може реалізувати свої більш-менш важливі права лише колективно та в колективі (в рамках племені чи роду) [2, с. 135].

На сучасному етапі розвитку інформаційного права проблема питання балансу різноманітних ідей прав людини є важливою з наступних причин:

- історичні передумови концепції, зацікавленість питанням природних прав людини упродовж усього періоду розвитку європейської філософії вказують на світову практичну й науково-філософську значущість означених ідей для будь-яких типів суспільств;

- концепція природного права сприяє вирішенню проблеми переходу посттоталітарного, авторитарного суспільства до правової держави та демократичного громадянського суспільства, виявленню специфіки їхніх взаємовідносин;

- з урахуванням національних особливостей країни, української національної ідеї, концепція природного права може бути успішно застосована в контексті обґрунтування державного та суспільного будівництва в перехідному суспільстві України;

- концепція відображає світовий досвід спільного життя людей, роз'єднаних особистими егоїстичними інтересами, але здатних їх узгодити й подолати

протиріччя на основі спільного прийняття загального для всіх моральнісного закону [4, с. 3].

Ще з прийняттям Декларації про державний суверенітет 16 липня 1990 р., у преамбулі якої наголошується на необхідності всебічного забезпечення прав і свобод людини, в Україні почався процес переорієнтації правової системи щодо вирішення проблеми прав людини і громадянина як найвищої соціальної цінності. Своє логічне завершення цей процес отримав з прийняттям Конституції України 28 червня 1996 р., яка встановила новий конституційний статус людини і громадянина на основі сучасної ліберальної концепції прав людини у відповідності із визнаними світовим співтовариством стандартами в галузі прав людини. Її принципова відмінність від старих радянських підходів до визначення конституційного статусу полягає: по-перше, у відмові від класового підходу при закріпленні правового статусу особи; по-друге, у визнанні людини і громадянина суб'єктом прав і свобод; по-третє, у визнанні суб'єктом прав і свобод індивідуально кожен конкретну людину і громадянина, у відмові від пріоритету інтересів колективного суб'єкта, але його визнання не може призводити до ігнорування індивідуальних прав і свобод кожної людини; по-четверте, у відмові від пріоритету інтересів держави над інтересами особи [3, с. 63].

Як ми бачимо, вирішальний вплив на встановлення прав людини зробила побудована на ліберальній концепції природно-правова доктрина, яка встановила пріоритет прав людини, нові параметри взаємовідносин між індивідом та владою. В затвердженні прав та свобод людини відіграло важливу роль їх ідеологічне, доктринальне обґрунтування – вчення про природні права людини, які не залежать від розсуду та свавілля державної влади, а мета останньої – забезпечення прав, визначених природою.

Категорія прав людини діє виключно у стосунках між людиною та владою. Права людини – це межі влади. Вони визначають ту сферу життєдіяльності людини, в яку влада (держава) не може втручатись і ті обов'язки, які має держава щодо людини. Стосунки між людиною та владою передбачають особливий характер: «...Концепція прав людини ґрунтується на трьох положеннях: по-перше, кожна влада обмежена; по-друге, кожна людина має свій автономний світ, втручатися в який не може жодна сила; по-третє, кожна людина захищаючи свої права, може висунути претензії до держави».

Вказаному прямо імпонують застереження середньовічних реформаторів проти зосередження влади в руках небагатьох з метою обмеження влади правителів і запобігання тиранії, що відкрило шлях до ствердження авторитету людини, її прав і свобод та визнання пріоритету її інтересів над державними. Завдяки цьому благополуччя людини й суспільне благо почали визнаватися метою діяльності держави, що природно сприяло обмеженню її влади [5, с. 124-125].

Саме зазначені ідеї стали засадничими при створенні конституцій передових європейських держав і міжнародних конвенцій, які проголосили невід'ємні права людини, що стали визнаними на рівні міжнародних стандартів.

Сьогодні законодавчо закріплене правове положення людини своєю основою має саме природно-правову концепцію, яка обумовила в якості первинних принципів свободу та невід'ємність, не відчужуваність прав людини, які належать їй від народження. Визначаються орієнтири у взаємовідносинах держави і людини – свобода, рівність, верховенство права, універсальність прав людини, взаємність відповідальності.

У сучасній юридичній науці розуміння прав людини зводиться до таких основних позицій: права людини – це певним чином внормована її свобода; права людини – це певні її потреби чи інтереси; права людини – це її вимоги про надання певних благ, адресовані суспільству, державі, законодавству; права людини – це особливий вид (форма існування, спосіб прояву) моралі.

Отже, баланс ідей про права людини може полягати у визначенні їх як «мінімуму загально соціальних, загальнолюдських та загальнодемократичних вимог до правового та соціального становища кожної особи, реалізація яких повинна й може бути забезпечена в будь-якому суспільстві, не залежно від особливостей його соціально-правової системи» [1, с. 173].

Список використаних джерел:

1. Бережнов А.Г. Политика и права человека / А.Г. Бережнов // Политология. Курс лекцій / под ред. М. Н. Марченка. – М. : Зерцало, 1993. – 608 с.
2. Конституции зарубежных государств / Сост. проф. В.В. Маклаков. – 2-е изд., – М.: Изд-во БЕК, 1997. – 586 с.
3. Кравченко В.В. Конституційне право України: навч. посібник. Частина 1 / В.В. Кравченко. – К.: Атіка, 1998. – 88 с.
4. Культенко В.П. Історико-філософська реконструкція концепції природного права в контексті аналізу перехідних суспільств : автореф. ... канд. філос. наук / В.П. Культенко. – К., 2004. – 19 с.
5. Львова О.Л. Вплив Реформації на правову систему України / О.Л. Львова // Реформація: успіх Європи і шанс для України: монографія / за ред. Р. Шеремети і О. Романенко. – К.: Саміт-Книга, 2017. – С. 123-132.
6. Права человека : учеб. для вузов / за ред. Е.А. Лукашева. – М.: НОРМА, 2000. – 560 с.

*Львова О. Л., к.ю.н., с.н.с., доцент
ФСП КПІ ім. Ігоря Сікорського*

СВОБОДА СЛОВА ТА ІНШІ ПРАВА ЛЮДИНИ: КРИТЕРІЙ БАЛАНСУ

Право на свободу вираження поглядів іноді розглядається як цінна спадщина, а іноді – як небезпечний інструмент. Воно може бути як величезним джерелом повноважень, так і призводити до зловживань. Згідно з відповідними нормами Ради Європи, питання постає не стільки в тому, чи треба обмежувати здійснення права на свободу вираження поглядів, скільки в тому, яким чином це робити та якою мірою. З цієї причини Рада Європи не розцінює право на свободу

вираження поглядів як абсолютне право і не розглядає його окремо. Натомість вона поміщає це право в систему тісно пов'язаних між собою прав людини [2, с.7].

У ст. 10 Конвенції про захист прав людини та основоположних свобод зазначається: «1. Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств. 2. Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для охорони порядку або запобігання злочинам, для охорони здоров'я або моралі, для захисту репутації або прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду і є необхідними в демократичному суспільстві» [1, с. 13].

Як правило, право на свободу вираження поглядів розглядається як цілісне поняття. Однак на практиці права промовців, слухачів та третіх сторін можуть відрізнитись або навіть доповнювати один одного. Як-то, «право» промовця робити образливі заяви расистської спрямованості протистоїть «праву» слухача не бути жертвою расизму. І все це має бути розглянуто у співвідношенні з «правом» або прагненням третіх сторін не допускати публічних заяв расистського характеру [2, с. 9]. У даному разі обмеження свободи слова пов'язане з їх образливим, тобто принижуючим гідність, характером.

Парламентська асамблея Ради Європи у резолюції № 1728 (2010 р.) «Дискримінація на основі сексуальної орієнтації та гендерної ідентичності» спеціально засудила таку мову щодо ЛГБТ. Зокрема, Асамблея підкреслює, що найважливіше завдання усіх органів державної влади полягає у тому, щоб не лише дієво та ефективно захищати права, що закріплені у правозахисних міжнародних документах, а й у тому, щоб утримуватися від висловлювань, які можуть призвести до узаконення і заохочення дискримінації чи ненависті, викликані нетерпимістю. Межа між висловлюваннями, направленими на розпалювання ненависті і яка сприяє скоєнню злочинів, і свободою слова має визначатися з урахуванням прецедентної практики Європейського суду з прав людини [4].

Деякі міжнародні правові документи називають такі висловлювання «hate speech» (тобто мовою ворожнечі) та визначають певні критерії її розпізнавання.

Так, Рекомендація Ради Європи № 97 (20) «Про наклепницькі висловлювання», що ухвалена Комітетом міністрів 30 жовтня 1997 р. на 907 засіданні заступників міністра, використовує термін «наклепницьке висловлювання», під яким розуміють «такий, що охоплює всі форми висловлювань, які поширюють, підбурюють, заохочують чи виправдовують расову ненависть, ксенофобію, антисемітизм або інші форми ненависті, що

ґрунтується на нетерпимості, у т. ч. нетерпимості, що знаходить своє вираження у войовничому націоналізмі й етноцентризмі, дискримінації та ворожості стосовно меншин, мігрантів і осіб іммігрантського походження» [5, с. 49].

У принципі 5 даної Рекомендації зазначається: «Національне законодавство й практика мають дозволяти представникам прокуратури й інших органів влади, які мають аналогічні повноваження (звичайно, в межах їхньої компетенції), приділяти особливу увагу справам, в яких ідеться про наклепницькі висловлювання. У зв'язку з цим такі органи повинні, зокрема, ретельно проаналізувати право підозрюваного на свободу вираження поглядів, оскільки накладення кримінальних санкцій є, зазвичай, серйозним втручанням у цю свободу. Приймаючи рішення про накладення кримінальних санкцій на осіб, які звинувачуються в злочинах, пов'язаних із наклепницькими висловлюваннями, уповноваженим судовим органам слід неухильно дотримуватися принципу пропорційності» [5, с. 49].

Із даного принципу виокремлюється такий критерій мови ворожнечі, як наклеп, тобто такі висловлювання, що не відповідають дійсності. У даному випадку наклеп не можна вважати правом людини на свободу вираження поглядів.

Власне й постає питання, у якому разі ще, окрім наклепу, проходить межа між свободою вираження поглядів та іншими правами людини, що порушується ст. 10 Конвенції. Зокрема, з цією метою Європейський суд розробив тест, що складається з декількох етапів. Так, при виявленні втручання у здійснення права на свободу вираження поглядів, це втручання повинне: передбачатися законом – тобто бути достатньо зрозумілим та розумною мірою прогнозованим щодо його наслідків; переслідувати законну мету – тобто відповідати одній з цілей, перелічених у статті 10(2); бути необхідним у демократичному суспільстві – тобто відповідати «невідкладній суспільній потребі» та бути пропорційним до переслідуваної законної мети.

Держави мають певну свободу дій, право розсуду, у визначенні порядку регулювання свободи вираження поглядів. Межі цієї свободи дій, яка є предметом нагляду Європейського суду, можуть різнитися. Держави мають досить обмежену свободу дій у тому, що стосується свободи вираження політичних поглядів, та більш широкую – у тому, що стосується питань громадської моралі, пристойності або релігії. Як правило, це пояснюється відсутністю європейського консенсусу щодо доречності та порядку здійснення регулювання у цих галузях [2, с. 13].

Зокрема, аналізуючи практику застосування норм законодавства про «мову ворожнечі» в країнах західної Європи, українськими дослідниками виявлено наступне: у **Сполученому Королівстві** діє закон про суспільний лад з 1986 р., розділ 5 якого дає визначення та ознаки дій, які класифікуються як злочин на підставі ненависті. *Прикладом використання даної норми є подія 2015 р., коли Фелікс Нгоул був виключений з університету за негативний коментар щодо одностатевого шлюбу на своїй сторінці у соціальній мережі. Керівництво*

університету стверджувало, що його коментарі порушили Кодекс поведінки. Також у 2002 р. у Швеції був прийнятий закон «Про розпалювання ворожнечі», в якому міститься норма про обмеження церковних проповідей. З цього приводу канцлер юстиції зробив публікацію про те, що проповідь може вважатися кримінальним правопорушенням, якщо вона містить інформацію про те, що, наприклад, гомосексуалізм є «абсолютно протиприродним явищем» [3, с. 99-100]. Україна також вже набуває практику у вирішенні аналогічних питань, за тим виключенням, що це відбувається поза межами встановленого законодавством судового процесу. Так, 26 січня 2018 р. на сайті Президента України громадянином В. Танцюрою, відповідно до Закону України «Про звернення громадян», було оприлюднено петицію (№22/042484-еп) із обґрунтованим проханням вжити заходів для захисту традиційних сімейних цінностей і припинення пропаганди гомосексуалізму. Однак, станом на 28 березня 2018 р. оприлюднення даної Петиції, яку вже підписали майже 23 000 громадян України із необхідних 25 000, було припинено на підставі звернення Представника Уповноваженого Верховної Ради України з прав людини з питань дотримання прав дитини, недискримінації та гендерної рівності А. Філіпішиної. Остання висловила думку про те, що в петиції містяться ознаки підбурювання до дискримінації за ознакою так званої «сексуальної орієнтації та гендерної ідентичності».

Наведена практика доводить, що визначене Конвенцією про захист прав людини і основоположних свобод, право людини на свободу вираження поглядів не просто підлягає обмеженню, а має суворе «табу» на свободу висловлювання щодо конкретних груп осіб чи явищ. При цьому не приймається до уваги критерій істини чи образи, що прямо пов'язується із поняттями честі та гідності особи, що, на наш погляд, має відрізнити свободу слова від мови ворожнечі.

У пункті 3 ст. 6 Закону України «Про засади запобігання та протидії дискримінації в Україні» уточняється, що «не вважаються дискримінацією дії, які не обмежують права та свободи інших осіб і не створюють перешкод для їх реалізації, а також не надають необґрунтованих переваг особам та/або групам осіб за їх певними ознаками, стосовно яких застосовуються позитивні дії». Із цього слідує, що дискримінація вважатиметься такою і, відповідно, суперечитиме принципу рівності за умов, якщо з огляду на певні, притаманні людині ознаки її було позбавлено (або обмежено) можливості скористатися своїми передбачуваними законом правами.

З огляду на викладене можна спостерігати так звану конкуренцію прав – право людини на рівність та недискримінацію і право на свободу думки та вираження поглядів. Вказане потребує визначення чітких критеріїв, чи «маркерів», які б допомогли відрізнити, за яких умов відбувається дискримінація, посягання на честь та гідність людини, а в яких випадках обмежується свобода думки та вираження поглядів.

Таким чином, у процесі дослідження національного і міжнародного права та практики його застосування, а також правової доктрини, ми виявили наступні критерії: істини чи наклепу; образи чи приниження гідності особи (що проявляється у формі жестів чи висловлювань); агресії, фізичного насилля чи очевидного спонукання до таких дій; критерій безпеки, охорони правопорядку, здоров'я, суспільної моралі і т. п.; критерій обмеження чи перешкоджання використання передбачених законом прав та інтересів.

Список використаних джерел:

1. КОНВЕНЦІЯ ПРО ЗАХИСТ ПРАВ ЛЮДИНИ ТА ОСНОВОПОЛОЖНИХ СВОБОД. ЗАСТОСУВАННЯ В УКРАЇНІ. ОФІЦІЙНЕ ВИДАННЯ. – К., 2006. – 176 с.
2. МАКГОНАГЛ ТАРЛАК. СВОБОДА ВИРАЖЕННЯ ПОГЛЯДІВ ТА ПОВАГА ДО ІНШИХ ОСІБ / ТАРЛАК МАКГОНАГЛ // ЖИТИ РАЗОМ: ПОСІБНИК З НОРМ РАДИ ЄВРОПИ ЩОДО ВНЕСКУ ЗМІ В ПОЛІПШЕННЯ СОЦІАЛЬНОЇ ЗГУРТОВАНОСТІ, МІЖКУЛЬТУРНОГО ДІАЛОГУ, ВЗАЄМОРОЗУМІННЯ, ТЕРПИМОСТІ ТА ДЕМОКРАТИЧНОЇ УЧАСТІ / ВИДАЄТЬСЯ ПІД КЕРІВНИЦТВОМ ЯШІ ЛАНЖ. – Рада Європи, 2010. – С. 7-13.
3. МЕДВЕДЄВА М.О. ТА ІН. «МОВА НЕНАВИСТІ» В МІЖНАРОДНОМУ ТА ЄВРОПЕЙСЬКОМУ ПРАВОВОМУ КОНТЕКСТІ / М.О. МЕДВЕДЄВА, Е.А. ДІБРІВНА, Р.В. КУХАРЧУК // АКТУАЛЬНІ ПРОБЛЕМИ МІЖНАРОДНИХ ВІДНОСИН. – Вип. 133. – 2017. – С. 95-105.
4. РЕЗОЛЮЦІЯ 1728 (2010) ДИСКРИМИНАЦІЯ ПО ПРИЗНАКУ СЕКСУАЛЬНОЇ ОРИЕНТАЦІЇ І ГЕНДЕРНОЇ ІДЕНТИЧНОСТІ // САЙТ ПАРЛАМЕНТСЬКОЇ АССАМБЛЕЇ СОВЕТА ЄВРОПИ. –
URL:[https://www.coe.int/T/R/Parliamentary_Assembly/\[Russian_Documents\]/\[2010\]/\[Apr2010\]/Res1728_Rus.asp](https://www.coe.int/T/R/Parliamentary_Assembly/[Russian_Documents]/[2010]/[Apr2010]/Res1728_Rus.asp)
Рекомендація Ради Європи №97 (20) «Про наклепницькі висловлювання», ухвалена Комітетом міністрів 30 жовтня 1997 р. // Стандарти Ради Європи у сфері медіа. Законодавчий бюлетень. – К.: IREX U-Media, 2005. – С. 47-49. – URL: http://www.archives.gov.ua/International/R_E_final.pdf

*Ланде Д. В., д.т.н., с.н.с.
НДІІП НАПрН України,
Ліненко Ю. О., студент
КПІ ім. Ігоря Сікорського*

ОБМЕЖЕННЯ ДОСТУПУ ДО ІНТЕРНЕТУ У СВІТІ: МЕРЕЖЕВА МОДЕЛЬ

На цей час у багатьох країнах світу існують обмеження доступу громадян до інтернет-ресурсів, зокрема соціальних мереж і месенджерів. Це явище підлягає всебічному дослідженню. Світова система обмежень доступу до інтернет-ресурсів може бути предметом вивчення у рамках правової науки та соціології. Для здійснення аналізу стану обмежень в Інтернеті до цього часу не вистачало інструментальних засобів, програмних модулів і методик, що надаються експертам.

Метою доповіді, що пропонується, є опис мережевої технології дослідження обмежень доступу користувачів до соціальних мереж і подібних сервісів – месенджерів, мікроблогів тощо. Це обумовлено тим, що подібні обмеження застосовуються досить широко, тому виникає потреба у спеціальному програмному забезпеченні, методах і засобах аналізу, візуалізації, формального рейтингування та класифікації подібних явищ, що й обумовлює актуальність цієї роботи.

Викладення основного матеріалу. Для побудови моделі вибрано у якості бази декілька країн та інтернет-ресурсів. До розгляду не попали країни типу Куби або Північної Кореї, де заборонено практично усі соціальні мережі. У даній роботі розглядаються можливості доступу 10 країн до 12 інтернет-ресурсів, перелік яких наведено у Таблиці. Крім того, не розглядаються такі мережеві ресурси як окремі веб-сайти, великі групи, доступ до яких на законних засадах заборонений навіть у Європейських країнах, де Інтернет-свобода є найвищою у світі. Дані, що розглядаються у цій роботі є актуальними, але ще далеко не повними. Вони використовуються скоріше як приклад, полігон для демонстрації методу. У даній роботі пропонується технологія дослідження питання щодо обмеження доступу до інтернет-ресурсів.

Таблиця. Обмеження доступу до інтернет-ресурсів

Інтернет-ресурс	Країни
Facebook	Китай, Іран, Єгипет, Туреччина, Пакистан, Саудівська Аравія
Twitter	Китай, Іран, Туркменістан, Єгипет, Туреччина
Wechat	Туркменістан, Іран, Росія
LinkedIn	Росія, Куба, Іран
Instagram	Китай, Туреччина, Туркменістан, Іран
ВКонтакте	Україна, Туркменістан, Іран
Однокласники	Україна, Китай
Telegram	Росія, Іран, Китай, Пакистан
Viber	Китай, Пакистан, Узбекистан
Whatsapp	Китай, Туркменістан, Пакистан
Skype	Китай, Росія, Узбекистан
Youtube	Іран, Пакистан, Китай, Єгипет, Туреччина, Саудівська Аравія

Розглянемо інформацію з Таблиці по країнам більш докладно.

Китай. Доступ до ряду іноземних сайтів з території КНР обмежується в рамках проекту «Золотий щит» (так званий Великий китайський фйрвол). Веб-сторінки фільтруються за ключовими словами, пов'язаними з державною безпекою, а також по «чорному списку» адрес сайтів. Фільтрації підлягають Facebook, Twitter, Instagram, Однокласники, Telegram та багато інших західних ресурсів.

Іран. В Ірані держава дуже жорстко обмежує неконтрольований доступ населення до Всесвітньої павутини. Під заборонаю знаходиться Youtube, Facebook, Twitter, Wechat, LinkedIn, Instagram, Вконтате й Telegram.

Египет. У Єгипті, незважаючи на проголошену свободу слова та думки, законодавство залишає для влади простір для блокування контенту: фільтруються Youtube, Facebook й Twitter.

Туреччина. У Туреччині громадянам заблокований доступ до Facebook, Twitter, Instagram і Youtube.

Пакистан. У Пакистані за рішенням суду був заблокований Youtube. Під фільтрацію також попадають Facebook, Viber, Telegram й Whatsapp.

Саудівська Аравія. У Саудівській Аравії встановлено низку правил й обмежень щодо розповсюдження інформації. У зв'язку з цим інтернет-фільтрація розповсюджується на такі ресурси як Facebook, Youtube та інші.

Туркменістан. У Туркменістані інтернет-фільтрація розповсюджується на Twitter, Wechat, Instagram, Вконтакте й Whatsapp.

Росія. На даний момент у Росії заблоковані Wechat, LinkedIn, Telegram й Skype.

Україна. 16 травня 2017 року Президентом України підписано указ [1], за яким введено в дію рішення РНБО про оновлення списку санкцій проти ряду російських компаній, серед яких соціальні мережі «ВКонтакте» і «Однокласники», електронний поштовий сервіс Mail.Ru тощо. Усім їм встановлено санкційний термін у три роки. Цей указ обумовлюється гібридною війною, яка ведеться проти нашої держави.

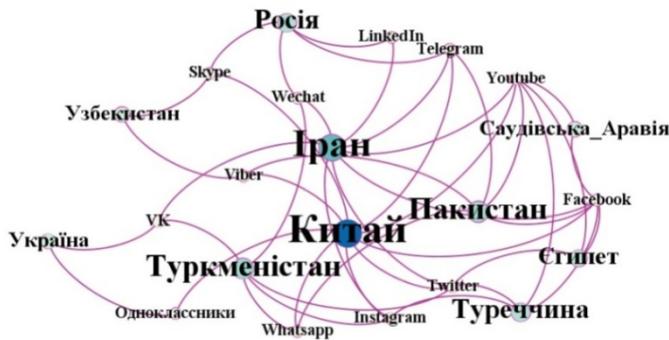
Узбекистан. Інтернет-фільтрація в Узбекистані розповсюджується на Viber й Skype.

З формальної точки зору наведену таблицю можна представити у вигляді біографу, один сегмент якої – інтернет-ресурси, інший – держави. Ці сегменти пов'язані між собою значенням «обмеження доступу». Відповідно пропонується сформувати матрицю цих зв'язків, яку можна зберігати на комп'ютерному носії у форматі csv.

Для візуалізації та подальшого аналізу сформованого біографу (мережі зв'язків «обмежень» між державами та інтернет-ресурсами) можна застосувати низку програмних систем, одна з яких – Gephi (<http://gephi.org>) [2]. Після завантаження сформованого csv-файлу буде отримано графічне відображення мережі (Мал. 1) і визначено основні її параметри: кількість вузлів: 22; кількість зв'язків: 44; щільність графу 0,095 тощо.

Як один із напрямків аналізу соціальних мереж можна розглядати ранжирування вузлів за різними критеріями, зокрема PageRank[3] і HITS [2].

Алгоритм HITS забезпечує вибір з інформаційного масиву кращих вузлів, на які введуть посилання («авторів», у нашому випадку країн) і «посередників» (вузлів, від яких йдуть посилання цитування, у нашому випадку – інтернет-ресурсів, доступ до яких обмежується).



Мал. 1. Мережа обмежень

Відповідно до алгоритму HITS, для кожного вузла мережі m_j рекурсивно вираховується його значимість як автора $a(m_j)$, при цьому підрахунок суми проводиться по всім вузлам, які посилаються на даний вузол, та посередника $h(m_j)$, де підрахунок суми проводиться по всім вузлам, на які посилаються у даному вузлі.

$$a(m_j) = \sum_{i \rightarrow j} h(m_i); \quad h(m_j) = \sum_{j \rightarrow i} a(m_i);$$

Рейтингування вузлів дає змогу виявляти країни з найбільшими обмеженнями доступу до інтернет-ресурсів, і інтернет-ресурси, що найбільше обмежуються.

Для мережі, що розглядається, результати ранжирування за цими критеріями наведено на Мал. 2. Слід відзначити, що ранжирування вузлів за критерієм HITS (Мал. 2 б) має більш велику розподільну здатність. Можна побачити, що тільки він дозволяє розділяти інтернет-ресурси за ступенем «обмеженості».

Label	PageRank
Китай	0.097906
Іран	0.08911
Туркменістан	0.069321
Росія	0.068442
Пакистан	0.064044
Україна	0.05305
Туреччина	0.051731
Узбекистан	0.048653
Єгипет	0.045135
Саудівськ...	0.039858
Facebook	0.031063
Youtube	0.031063
Twitter	0.031063
Instagram	0.031063
Telegram	0.031063
Whatsapp	0.031063
Viber	0.031063
Wechat	0.031063
VK	0.031063
Skype	0.031063
LinkedIn	0.031063
Однокласс...	0.031063

А

Label	Authority	Hub
Китай	0.549275	0.0
Іран	0.504343	0.0
Пакистан	0.338742	0.0
Туреччина	0.334866	0.0
Туркменістан	0.275962	0.0
Єгипет	0.264705	0.0
Саудівськ...	0.183387	0.0
Росія	0.167325	0.0
Узбекистан	0.073866	0.0
Україна	0.061206	0.0
Facebook	0.0	0.446615
Youtube	0.0	0.446615
Twitter	0.0	0.396074
Instagram	0.0	0.341728
Telegram	0.0	0.320219
Whatsapp	0.0	0.238977
Viber	0.0	0.197484
Wechat	0.0	0.194558
VK	0.0	0.172771
Skype	0.0	0.162291
LinkedIn	0.0	0.1379
Однокласс...	0.0	0.125338

Б

Мал. 2. Ранжирування вузлів мережі за критеріями PageRank (а) і HITS (б)

Висновки. У роботі представлено нову інформаційну мережеву технологію і методологію побудови та формального дослідження мережевих обмежень доступу до інтернет-ресурсів.

Представлена технологія дозволяє ранжирувати інтернет-ресурси та держави за рівнем обмеження перших іншими.

Мережева технологія також дозволяє виявляти кластери (класи) країн за рівнем обмеження доступу до інтернет-ресурсів, видаляти класи найбільш корельованих держав (на розглянутому прикладі, зокрема, Росія та Іран).

Змістовне пояснення обмеження доступу до соціальних мереж та інших інтернет-ресурсів у кожному випадку ґрунтується на нормативно-правових актах окремих країн.

Список використаних джерел:

1. Указ Президента України №133/2017 від 15 травня 2017 року. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)".

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

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

4. Kleinberg J.M. Authoritative Sources in a Hyperlinked Environment // Proceedings of the ACM-SIAM Symposium on Discrete Algorithms, 1998, and as IBM Research Report RJ 10076, May 1997.

*Свідло Т. М., к.ф.н., доцент
ФСП КІІ ім. Ігоря Сікорського*

ЗАХИСТ ВІД ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА, ЗАХИСТ ІНФОРМАЦІЙНИМ СУСПІЛЬСТВОМ

Сьогодні на передній план висувається така галузь суспільного виробництва як виробництво і розподіл знань, причому не поряд з іншими галузями, а як основна галузь виробництва.

У свій час американський економіст і соціолог Дж. Гелбрейт при дослідженні проблеми співвідношення сфери виробництва речей і виробництва знань прийшов до висновку, що потреби індустріальної системи повинні мати другорядне значення порівняно із задачами духовного розвитку людини. Вчений прогнозує, що в майбутньому освіта стане самоціллю, а не засобом для успішного обслуговування системи. Світ, що прагне і має жадобу до знань, не може задовольнитися лише виробництвом і споживанням товарів.

Виробництво знань стало важливою формою діяльності сучасного суспільства. Метою ж освіти є формування творчої особистості, що здатна генерувати нові ідеї. Творча ж особистість породжує новий світ, і цей світ має

ґрунтуватися на принципах гуманізму, людяності, справедливості, свободи, щастя. Проте справа полягає не лише проголошенні певних принципів, але і в їх практичній реалізації зі знанням справи, з коректуванням до певних умов і обставин. На жаль, на тлі підвищення тотального рівня освіти і освіченості, особливо у використанні сучасних інформаційних технологій, не зникають ниці риси людини, а, навпаки, приймають все більш викривлено-витончені обриси. І ґрунтуються вчинки такої «освіченості» на новітніх технічних досягненнях та знанні психології людини. Особливо жахливо, коли використовують злочинці ці технології і знання проти незахищених верств населення.

Всі ми родом із дитинства і рано чи пізно повертаємося туди, де ілюзія переважає над реальністю, де здобутий протягом життя досвід піднімає людину над буденністю спотвореного світу, а індивідуально-духовний рівень розвитку повертає тебе на круги своя, тобто, у дитинство, де знову широко відкритими очима з розкритими обіймами наївності людина вдивляється у вічний недосяжний горизонт. Більш за все переживає у достойних літах людина за здоров'я і добробут близьких і рідних людей, особливо дітей і внуків. І потурбовані зненацька, коли ніби рідна кровинка благає про допомогу, старенькі виносять все, що мають, і як правило те, що накопичували собі не на життя, на смерть. А вже потім, зрозумівши, що ошукані, омитими сльозами очима дивляться, не розуміючи, як таке могло статися. Сором'язливо стуляють вуста, щоб не повідати нікому про жорстоку образу, нанесену зухвалими нелюдами наприкінці земного шляху...

А що суспільство? Недосконалий світ, недосконале суспільство, недосконалі люди, недосконале законодавство... Тихесенько десь там хтось плаче, то й злочину нема?!

В засобах масової інформації, як правило, старенькі дивляться телевізор, а не «висять» у комп'ютері, ще інколи (не часто) почують оголошення в метро, де застерігають не попасти на гачок до шахраїв; на сайти банків, де пишуть про кардинг, фішинг, скимінг тощо, також не «ходять», бо не дуже потребують (кредитування обмежене певним віком). Залишаються соціальні служби, які повинні вести і роз'яснювальну роботу, індивідуальну, повсякденну, турботливу. Залишаються законотворці, які повинні і на цей аспект дивитися широко відкритими очима, тобто створювати відповідну законодавчу ініціативу (як правило, стареньким телефонують, то чи не можна, як тривожну кнопку, ввести тривожне словосполучення? – Сучасні технології дозволяють створити такі програми). Чи це не цікаво (поки не торкнулося твоїх батьків?).

Можливо, запропонувати щось зможуть молоді і творчі студенти-правники, інвестуючи знання і у своє майбутнє, коли скроні стануть срібними, а погляд наївно-спокійно-гарантовано-впевненим, тому що правозахищений.

СИСТЕМА ПРОТИДІЇ КОНКУРЕНТНІЙ РОЗВІДЦІ ЯК ТЕХНОЛОГІЯ

Система протидії конкурентній розвідці описана автором у достатній кількості робіт, однак як технологія визначається вперше і може бути використана тільки досить кваліфікованим персоналом.

Структурно технологія складається з трьох етапів:

1 етап - класифікація інформаційних ресурсів:

- за типом інформації;
- за видом доступу;
- за правом власності;
- за типом прав на інформацію;
- за сферами обігу;
- за типом нормативно-правового регулювання.

2 етап - грошова оцінка інформаційних ресурсів за трьома методиками:

- витратної;
- дохідної;
- аналогової або ринкової.

Кожна з методик включає в себе близько 15 різних методів оцінки інформаційних ресурсів.

3 етап - побудова системи захисту інформаційних ресурсів.

В основу методики покладена «цінність» інформаційних ресурсів та принципів відмінності між класичним і промисловим шпигунством, а також конкурентною розвідкою, які наведемо нижче.

Шпигунство - передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства.

Державна зрада - діяння, умисно вчинене громадянином України на шкоду суверенітету, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в умовах воєнного стану або в період збройного конфлікту, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України.

Державною таємницею визнається вид інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України і які визнані державною таємницею і підлягають охороні державою. Ці відомості мають гриф секретності.

Промислове шпигунство - це нелегітимне, протиправне отримання економічної інформації про конкурента для отримання економічних переваг.

Не слід плутати конкурентну розвідку з промисловим шпигунством. Першу відрізняє законність і використання тільки дозволених методів отримання відкритої інформації з офіційних джерел. Другий використовує незаконні методи (підкупу, шантажу і т.д.) отримання конфіденційної інформації. У цьому його принципова відмінність від конкурентної розвідки і бенчмаркінгу - запозичення передового досвіду.

Тобто, предметом контрконкурентної діяльності є безперервне забезпечення захисту інформації від нелегітимного, або протиправного заволодіння нею окремими організаціями, групами, або особами.

Метою протиконкурентної діяльності є виявлення, попередження та припинення нелегітимної, або протиправної діяльності з отримання значимої для підприємства інформації, заволодіння якої яку може призвести до значної матеріальної шкоди.

Більш просто: шпигунство і державна зрада спрямовані на заволодіння таємною інформацією, а промислове шпигунство - це незаконний метод заощадити час і кошти на винахід «велосипеда», на якому вже давно катається конкурент.

Тобто, коли протиправна діяльність «переступає» межі країни, говорять не тільки про економічну складову, а й про загрозу державній безпеці.

Виходячи з класичної структури діяльності у подальшому доцільно поетапно визначити мету протиконкурентної діяльності, систему її завдань, об'єкт діяльності, предмет діяльності та суб'єкти діяльності, види, форми, методи, сили та засоби які будуть використовуватися.

Виходячи з цього і будується система протиконкурентної діяльності організації.

Цінність технології визначається тим, що:

- є можливість докапіталізації підприємства за рахунок нематеріальних активів і впровадження системи їх якісного захисту від конкурентів;
- застосування продукту в повному обсязі захистить підприємство від втрати інформаційних ресурсів;
- технологія може бути адаптована під конкретний вид підприємств (наукові та навчальні заклади, підприємства ВПК і інші високотехнологічні виробництва).

Запропонована технологія дасть можливість:

- провести інвентаризацію і систематизувати інформаційні ресурси;
- провести їх грошову оцінку;
- побудувати систему захисту інформаційних ресурсів в залежності від їх вартості;
- використовувати споживачем технології, як продукту поетапно - як частково, так і в повному обсязі.

Головною перевагою технології над іншими є врахування реальної грошової вартості нематеріальних активів (інформаційні ресурси типу ноу-хау,

комерційна таємниця, об'єкти інтелектуальної власності тощо), які спочатку монетизуються і на цій основі будується система їх захисту від «агентурної» і технічної розвідок.

Якісне науково-практичне вирішення цієї проблеми під силу тільки висококваліфікованому науковому колективу, тому що, оціночною діяльністю в матеріальному секторі займаються суто практичні компанії з використанням єдиного існуючого методу на практиці - стандарту № 4.

Нами ж пропонується застосування 3-х методик оціночної діяльності, які знівелюють 30% похибку між методиками і визначають так звану - справедливу ціну нематеріальних активів. Відповідно від ціни ресурсів і буде будуватися система їх захисту.

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

Науковий керівник:

*Фурашев В. М., к.т.н., с.н.с., доцент
ФСП КПІ ім. Ігоря Сікорського*

МАНІПУЛЮВАННЯ У ХХІ СТОЛІТТІ

Наше сьогоднішнє, це стрімкий розвиток новітніх технологій в усіх сферах життя. В наш час вже відходять на другий план радіоприймачі, теле- та відео ролики, молодь все менше дивиться телебачення. Зараз все обертається навколо чи в Інтернеті. Використання Інтернету в наш час є не просто можливістю для пошуку інформації, а становить невід'ємну частину життя більшості користувачів. Із кожним роком Інтернет охоплює все більшу аудиторію користувачів, стаючи для них одним із основних джерел інформації.

Інтернет простір має багато переваг, це швидкий доступ до важливої інформації, пошук необхідних даних, зв'язок з людьми незалежно від місця знаходження та багато іншого, але поряд з тим є свої негативні сторони.

Це середовище віртуалізації суспільства, користувачі можуть там ховатись під маскою нової особистості, вони думають, що відчують себе захищеними та проявляться як того бажають. Вони перестають бути соціалізованими в реальному суспільстві, їх життя існує лише в інтернеті. Контент web-сайтів ніким не контролюється, вона може подаватись неправдивою, загрозливою, миролюбивою або агресивною.

Вагома аудиторія користувачів віртуального простору дає можливість проводити маніпуляційний вплив на свідомість людини без явного прояву. Інтернет користувачі піддаються маніпуляції навіть не помічаючи цього, наприклад через розміщені на сайтах разом з основною інформацією збоку з'являються невеликі інформаційні повідомлень або повідомлення з картинками, які можуть нести в собі недостовірну інформацію або чорного» піар тощо.

Найпоширеніший засіб маніпулювання свідомістю людини є ЗМІ та Інтернет.

Маніпуляція — вид психологічного впливу, який використовується для прихованого впровадження в психіку жертви цілей, бажань, намірів, відносин або установок маніпулятора, які не збігаються з актуально існуючими потребами жертви. Це приховане управління людьми та їх поведінкою. [1]

Брижко В. М., визначив поняття «маніпуляція» як набір способів прихованого управління, досить часто завдяки брехні, для досягнення односторонньої вигоди. Якщо узагальнити цей вираз, то можна виділити такі його головні ознаки :

-по-перше, це вид інформаційно-психологічної дії (не фізичне насильство, але може передбачати загрозу насильства). Мішенню дій маніпулятора є свідомість, психіка людини або колективу людей;

-по-друге, маніпуляція — це прихована дія, факт якої не повинен бути усвідомлений суб'єктом маніпуляції. Успіх гарантований тоді, коли той, хто піддається маніпуляції, вірить, що все те, що все відбувається, є дійсністю. Тому приховування інформації — обов'язкова ознака маніпуляції; [2]

Маніпулювання в інтернеті призводить до різних наслідків, вплив на формування нашого мислення світогляду, що впливає на нашу поведінку.

У звіті міжнародної правозахисної організації Freedom House зазначила, що за останній рік тактика маніпулювання та дезінформації зіграла важливу роль у виборах у щонайменше 17 інших країнах за останній рік, перешкодивши можливості громадян вибирати своїх лідерів на основі фактичних новин та справжніх дебатів.

Відповідно до ст. 40 Закону України «Про телекомунікації» відповідальності за інформацію, яка розміщена в мережі, Інтернет-провайдер не несе, а тому за розміщення неправдивої інформації практично ніхто не може бути покараним. У результаті цього відбувається поширення користувачів інформації, яка вигідна для тієї чи іншої групи [3].

Існує багато країн де рівень вільного доступу до інформації обмежений або частково обмежений, тобто контролюється владою, найпоширеніші:

Північна Корея є найбільш закритою країною світу. Доступ до соціальних мереж там заблоковано з моменту появи інтернету. Та й взагалі в країні є обмежений доступ до мережі. Логічно, що там не працюють Facebook, Twitter, YouTube, не кажучи вже про “Однокласники” чи “ВКонтакте”. У травні минулого року з'явилася північнокорейська версія соціальної мережі Facebook під назвою StarCon.net.kp, але через день вона зникла.

Китай дуже ревниво ставиться до соціальних мереж, розроблених іншими країнами. Ресурси Google, Flickr, Dropbox, Facebook, Twitter, YouTube, частково Вікіпедія – заблоковані в КНР, а жителі користуються китайськими аналогами. Доступ до низки іноземних сайтів з території Китаю обмежується в рамках

проекту “Золотий щит” (так званий Великий китайський файрвол), який працює з 2003 року.

Саудівська Аравія періодично бореться з Facebook і YouTube. Громадянам рекомендується активно розповідати про “аморальні” сайти, щоб їх могли заблокувати. У країні на час зникав доступ до “Вікіпедії” і навіть Google Translate. У 2012 році доступ до YouTube було повністю закрито. [4]

Нами маніпулюють завжди і скрізь але для формування своєї незалежної думки необхідно читати та аналізувати наданий матеріал, а не просто його «їсти». Перші кроки в цьому напрямку повинні включати державну освіту, спрямовану на навчання громадян, як виявляти фальшиві або маніпулятивні новини та коментарі. Державним органам необхідно контролювати контент який надається споживачу та притягати до відповідальності за порушення недостовірної або фейкової інформації.

Список використаних джерел:

1. Психологічна маніпуляція. URL:
https://uk.wikipedia.org/wiki/%D0%9F%D1%81%D0%B8%D1%85%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%87%D0%BD%D0%B0_%D0%BC%D0%B0%D0%BD%D1%96%D0%BF%D1%83%D0%BB%D1%8F%D1%86%D1%96%D1%8F
2. Брижко В.М. Маніпулювання свідомістю людини у проблемі упорядкування інформаційних відносин / В.М. Брижко // Правова інформатика. - 2015. - № 1. - С. 19-33. - Режим доступу:
http://nbuv.gov.ua/UJRN/Pinform_2015_1_6
3. Закон України «Про телекомунікації». URL:
<http://zakon.rada.gov.ua/laws/show/1280-15>
4. «Європи тут немає»: топ 10 країн, де забороняють соціальні мережі. URL:
<http://my.rv.ua/hotnews/yevropi-tut-nemaye-top-10-krayin-de-zaboronyayut-sotsialni-merezhi/>

Даценко А. Ю., аспірант Національного інституту стратегічних досліджень

СВОБОДА СЛОВА ТА ОБМЕЖУВАЛЬНІ ЗАХОДИ ЯК АЛЬТЕРНАТИВНІ СКЛАДОВІ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Засновуючись на аналізі контенту російських ЗМІ за останніх чотири роки, можна констатувати, що вони використовували такі пропагандистські «меседжи» щодо української цільової аудиторії: (а) в Україні шляхом державного заколоту владу захопили праві радикали; (б) в Україні панує фашистська ідеологія; (с) якби Крим та Донбас не вийшли з-під впливу України, їхнє населення стало би жертвою правих радикалів й було б винищене; (d) проєвропейські реформи в Україні провалились або рухаються вкрай повільно, а рівень корупції в Україні навіть вищий, ніж був за часів президентства Януковича; (е) Україна не потрібна Європі, її тільки використовують у своїх меркантильних інтересах Вашингтон та Брюссель; (f) Україна відповідальна за невиконання Мінських угод; прийняття нового закону про реінтеграцію Донбасу

перекреслює ці угоди; (g) Україна і Росія – один «братерський» народ; (h) на сході України йде «громадянська війна», а не війна з «російським агресором» [1].

Проблема полягає в тому, як протистояти російській агресивній пропаганді, дезінформаційним кампаніям та кібератакам як основним інструментам впливу на інформаційний простір України. Європейські експерти пропонують низку способів протидії, уникаючи контрпропаганди: (a) залежно від значимості проблеми, що вкидається в інформаційний простір, підвищувати масштаби її висвітлення, тим самим збільшуючи проінформованість цільової аудиторії щодо сутності проблеми та об'єктивності її подання; (b) гарантувати доступ до інформації й свободу слова; у цензурних обмеженнях не заходити надто далеко, навіть під час війни; (c) у процесі викриття дезінформації розкривати її методи та знайомити з ними реципієнтів інформації, щоб вони могли самостійно їх розпізнавати; (d) оприлюднювати свідчення викривачів-інсайдерів, які з різних причин покинули дану пропагандистську систему й можуть розповісти, які прийоми й методи використовує дана система; (e) використовувати новітні ІКТ для автоматизації «фактчекінгу» і ідентифікації «тролів», що діють у соцмережах Інтернету; (f) відслідковувати джерела фінансування пропагандистських кампаній (зазвичай той, хто їх фінансує, той і просуває свої меседжі); (g) розробляти та впроваджувати програми підвищення медіаграмотності населення й виховання критичного мислення тощо, бо «найбільшим ворогом пропаганди є інтелект»; (h) цензуру у всіх її формах й різновидах (штрафні санкції; блокування, тощо) використовувати тільки за гострої необхідності [2].

Під «цензурою» слід розуміти «свідоме чи несвідоме, державне чи позадержавне пригнічування інформаційної діяльності (діяльності мас-медіа зокрема), яка має такі вияви: обмежений доступ певних суб'єктів до певного кола джерел публічної інформації; повну або часткову заборону на діяльність деяких медіа; повний або частковий контроль над інформаційними потоками (включно з особистим листуванням) тощо [3].

Водночас пропаганда й цензура у своїх «м'яких», «білих» формах можуть бути корисними. Як зауважує Г. Почепцов, «пропаганда та цензура у своїх жорстких і м'яких проявах не стільки корегують, скільки створюють інформаційний простір. У своїх «гуманних» варіантах вони присутні в будь-якій, навіть самій демократичній державі, оскільки влада завжди намагається підсилити свої комунікації, щоб її почуло все населення. Будь-яка дія влади в умовах миру, а особливо в умовах війни, завжди буде вимагати підтримки громадян» [4].

Керування інформаційним простором базується на двох складових: з одного боку, слід максимально посилювати й доводити до цільових аудиторій власні меседжі, щоб охопити найбільшу кількість медіа з максимальною кількістю споживачів інформації, яким даний меседж адресований. Тобто, інформаційний простір слід максимально наповнювати власними меседжами, тоді як контрмеседжі слід відсувати на периферію уваги масової свідомості.

З іншого боку, враховуючи той факт, що цензура стоїть на заваді потраплянню контрмеседжів в інформаційний простір, в умовах війни слід оприлюднювати лише те,

що сприяє перемозі над ворогом, повністю або частково відповідає імперативам національної безпеки. З цього погляду виправданими є дії Української держави, яка розробила низку документів, що передбачають обмежувальні заходи, продиктовані міркуваннями національної безпеки:

1) Указ Президента України від 15 травня 2017 р. № 133/2017, яким введено в дію рішення РНБО України від 28 квітня 2017 р. "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", що передбачає введення санкцій проти низки фізичних та юридичних осіб, зокрема, проти ТОВ "Яндекс", російських соцмереж «ВКонтакте», «Однокласники», поштового сервісу Mail.ru. Також під санкції підпали низка інших російських медіа: "Наше Радіо", "Суспільне телебачення Росії", "Редакція телеканалу Ради Федерації", телеканали "Рен ТВ", "НТВ+", "ТНТ", ЗАТ "Національна медіа група", "Міжнародне інформагентство "Росія сьогодні".

2) Указ Президента України від 14 травня 2018 р. № 126/2018, яким введено в дію рішення РНБО України від 2 травня 2018 р. «Про застосування та скасування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», який серед іншого зобов'язує українських інтернет-провайдерів блокувати ще 192 сайти, у тому числі інтернет-сторінки Першого каналу, РТР-Планети, РІА та інших російських медіа.

3) законопроект № 6688 "Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері" (на теперішній час скерований на доопрацювання), яким передбачається ведення реєстру заборонених сайтів (на підставі чого 5 тисяч провайдерів і хостерів зобов'язані будуть закрити доступ до таких ресурсів), а також запропоновано дозволити Службі безпеки України блокувати сайти без рішення суду.

Але, як вважають правозахисники, відповідно до Європейської конвенції про права людини та Міжнародної конвенції про громадянські та політичні права, інтернет-свобода, як і решта свобод, може бути обмежена тільки за дотримання трьох критеріїв: по-перше, таке обмеження має бути передбачене законом, по-друге, воно має слугувати законним інтересам людей і, по-третє, воно є необхідним у демократичному суспільстві. Згідно зі ст. 39 Закону України «Про телекомунікації», інтернет-провайдери зобов'язані обмежувати доступ користувачів лише до сайтів з дитячою порнографією, у разі, якщо є судові рішення.

У законопроекті № 6688 правозахисників непокоїть, що ініціатори цього документа не передбачили механізм контролю за трафіком, а віддали право на його створення Кабінету Міністрів України, який має видати на цей рахунок спеціальне розпорядження або постанову. Але в такому разі цілком можливо, що Кабмін «пропише» у цих документах механізм контролю, який передбачатиме тотальний контроль СБУ не лише за джерелами інформації (метаінформацією), але й за змістом трафіку (контентом). Більше того, - стверджують правозахисники, - українська влада хоче здійснити усі ці обмеження за рахунок провайдерів, зобов'язавши їх встановлювати відповідне обладнання (будь-яке порушення вимог їм загрожуватиме

штрафом у розмірі одного відсотка річного доходу). На думку правозахисників такі неконтрольовані повноваження для СБУ можуть призвести до тиску на суб'єктів інтернет-спільноти. Окрім того, у законопроекті відсутні механізми формування санкційного списку і шляхи реалізації цієї санкції [5].

На думку представників ряду громадських організацій («Лабораторія цифрової безпеки», «Платформа прав людини», коаліція «За вільний Інтернет») [6, 7]:

- питання безпеки країни вищезазначені документи зачіпають «дуже поверхнево»;

- можливість влади мати в руках непідконтрольний громадськості інструмент блокування сотень сайтів створюють небезпечні передумови для безконтрольної інтернет-цензури;

- блокування інтернет-джерел не відповідає ustalеним стандартам свободи вираження поглядів, зокрема суперечать принципам законності та пропорційності обмежень;

- за певного тлумачення законопроект № 6688 може створити можливість повного блокування будь-якого сайту через будь-який негативний коментар, залишений сторонньою особою;

- під приводом боротьби з пропагандою та дезінформацією представники влади, керуючись не державними, а приватними інтересами, закриватимуть чи блокуватимуть небажані ЗМІ та економічні інтернет-ресурси, підриваючи тим самим довіру до медіа та журналістів у цілому, що зашкодить свободі слова.

З критикою дій української влади виступила також організація «Human Rights Watch», яка закликала український уряд скасувати дану заборону як таку, що порушує право людини на свободу слова та інформації [8]. Такою ж за характером була критика зазначеного законопроекту Гарлемом Дезіром (Harlem Desir), представником ОБСЄ з питань свободи медіа (OSCE Representative on Freedom of the Media) [9].

Водночас НАТО підтримала позицію Українського уряду стосовно блокування інтернет-ресурсів Росії, мотивуючи це тим, що в умовах загострення кіберзлочинності та кібервійни питання національної безпеки є важливішими за питання свободи слова.

Таким чином, правове регулювання інформаційного простору в умовах іноземної агресії потребує дуже виваженої державної інформаційної політики з урахуванням питань захисту вітчизняного інформаційного простору, але з дотриманням базових гарантій свободи слова.

Навіть у рішеннях ЄСПЛ йдеться, що «законодавче регулювання інтернету – це обов'язок держави. Проте мають дотримуватися ті гарантії, які стосуються свободи слова». Для цього потрібно ще до ухвалення будь-яких законодавчих ініціатив із регулювання проводити консультації з представниками громадських організацій, які знаються на правах людини і можуть вказати на можливі негативні моменти.

Наступними кроками у напрямі вдосконалення законопроекту № 6688 має бути напрацювання обґрунтованих підходів до вирішення проблемного питання інтернет-цензури з врахуванням думки усіх зацікавлених суб'єктів, і лише потім перейти до розроблення законопроекту або у вигляді окремого закону для інтернет-медіа, або ж у

вигляді об'єднання вже існуючих актів у єдиний великий закон, який регулював би питання щодо всіх видів інтернет-ЗМІ та ЗМІ загалом.

У законопроекті № 6688 обов'язково мають бути визначені чіткі і прозорі правила Інтернет-регулювання і суб'єкти такого регулювання, а саме: які державні інституції є суб'єктами інтернет-регулювання та на підставі чого вони мають ухвалювати відповідні рішення. Ці правила мають розроблятися відкрито, за участі представників громадськості та медіа-індустрії. Вони повинні бути чіткими і зрозумілими, зафіксованими в нормативно-правових документах та не мінятися «ad hoc».

Список використаних джерел:

1. Журналістика vs міфотворчість: хто і що формує імідж України в Європі.- URL: <https://mind.ua/openmind/20172752-zhurnalistika-vs-mifotvorchist-hto-i-shcho-formue-imidzh-ukrayini-v-evropi> (дата звернення 9.10.2018).
2. 25 способів противодействия прокремлевской дезинформации без использования контрпропаганды.- URL:<http://fakeoff.org/propaganda/25-sposobov-protivodeystvovat-propagande-ne-zanimayas-kontpropagandoy> (дата звернення 9.10.2018).
3. Ожеван М.А. Свобода слова та її обмеження в умовах війни: американський досвід та його проєкції на Україну // Міжнародні відносини. Серія «Політичні науки». 2015. №5. –URL:http://journals.iir.kiev.ua/index.php/pol_n/article/view/2513/2243 (дата звернення 9.10.2018).
4. ПочепцовГ.Г. Пропаганда и цензура: два крыла одного механизма. - URL: https://ms.detector.media/trends/1411978127/propaganda_i_tsenzura_dva_kryla_odnogo_mekhanizma/ (дата звернення 9.10.2018).
5. Законопроектom про блокування сайтів влада хоче запровадити цензуру. - URL:https://humanrights.org.ua/material/zakonoprojektom_pro_blokuvannjia_sajtiv_vlada_khoche_legalizuvati_cenzuru (дата звернення 9.10.2018).
6. Свобода в інтернеті чи нацбезпека: як знайти баланс в умовах війни? - URL:https://humanrights.org.ua/material/svoboda_proti_zaboron_jiak_v_ukrajini_namagajutsjia_kontroljuvati_internet_ (дата звернення 9.10.2018).
7. Китайська хвороба України. Як наша влада хоче зарегулювати інтернет. - URL:<https://detector.media/infospace/article/137394/2018-05-11-kitajska-khvoroba-ukraini-yak-nasha-vlada-khoche-zaregulyuvati-internet/> (дата звернення 9.10.2018).
8. Ukraine: Failing Its Human Commitments. - URL:<https://www.hrw.org/news/2018/01/18/ukraine-failing-its-human-rights-commitments> (дата звернення 9.10.2018).
9. OSCE Representative raises concerns regarding Ukrainian draft law to counter threats to national security in the information sphere. - URL:<https://www.osce.org/representative-on-freedom-of-media/387053> (дата звернення 9.10.2018).

ВПЛИВ ІНФОРМАЦІЙНОЇ ДІЇ ЗМІ НА ФОРМУВАННЯ ГРОМАДСЬКОЇ ДУМКИ: ФІЛОСОФСЬКО-ПРАВОВИЙ АСПЕКТ

Громадська думка відображає реальний стан суспільної свідомості, визначає настрої та інтереси більшості людей, актуальні проблеми суспільного життя. Громадська думка формується тоді, коли виноситься на обговорення важлива проблема, яка стосується інтересів більшості людей, та має практичне значення. Враховується при цьому вже існуючий досвід, який можна використовувати у політичному, культурному, духовному житті суспільства.

Найчастіше громадська думка піднімає питання, пов'язані з політикою, правом, мораллю, культурою, сферами наших інтересів, де часто ми стикаємося з багато чим незрозумілим та суперечливим. Предметом обговорення громадськості найчастіше виступають ті питання, на які можна отримати різні відповіді, при цьому відмінності в оцінках, судженнях, спонукають до конструктивного діалогу, дискусії.

Засоби масової інформації виступають одним із головних інструментів формування громадської думки. Це, перш за все, телебачення, періодичний друк, система комп'ютерних мереж, що забезпечують обробку і передачу інформації аудиторії. Засоби масової інформації систематично поширюють інформацію, впливаючи на формування духовних цінностей та створюючи культурний, суспільний простір.

Громадська думка не повинна залежати від політичних організацій чи соціальних інститутів, але дуже часто відбувається маніпулювання суспільною свідомістю. При цьому громадська думка яка формується в інтересах соціального або політичного замовника не репрезентує більшість аудиторії, але здатна впливати на сформовану систему цінностей, установки, мораль.

Мораль як сукупність норм, правил поведінки людей у суспільстві не закріплена у юридичних законах, на відміну від правових норм, а регулюється у суспільстві саме силою громадської думки.

У правовій державі повинна формуватися незалежна від соціального замовника громадська думка, а право, закріплене в офіційних документах держави, повинно встановлювати загальну форму відносин, визначати міру свободи людей, їх об'єднань, державних органів у взаємовідносинах між ними і гарантувати свободу і захист кожного.

Засоби масової інформації повинні сприяти розвитку демократії, бути незалежними від політичних організацій, та політичних лідерів. Вони повинні поширювати інформованість у суспільстві, говорити відкрито про діяльність влади, а влада не повинна тиснути на свободу слова.

У правовій державі «засоби масової комунікації повинні володіти публіцистичною різноманітністю, тобто давати можливість «повідати світу» різні

точки зору і думки» [1, с.13].

Впливаючи на одержувачів інформації засоби масової інформації повинні затверджувати духовні цінності, норми моралі та права.

Список використаних джерел:

1. Ноэль-Нойман Э. Общественное мнение. Открытие спирали молчания. — М.: Прогресс-Академия, 1996. — 393с.

*Самчинська О. А., студент
ФСП КПІ ім. Ігоря Сікорського*

Науковий керівник:

*Фурашев В. М., к.т.н., с.н.с., доцент
ФСП КПІ ім. Ігоря Сікорського*

СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ПОЛІТИЧНИХ МАНІПУЛЯЦІЙ

Ми живемо в епоху інформаційного суспільства. Коли стан розвитку технологій відкриває неосяжне поле можливостей. Не виходячи з дому можна навчатися, працювати, платити за комунальні послуги, здійснювати покупки та навіть подорожувати і це далеко невичерпний перелік досягнень інформаційного суспільства.

Однак, напевно кожен з нас задумувався, що ж ще «подарувала» нам епоха інформаційних технологій?

Сьогодні, невід’ємною частиною життя практично кожного є соціальні мережі. Вікове різноманіття користувачів інтернету просто неймовірне, починаючи з дітей дошкільного віку до пенсіонерів. Винайдення інтернету та меседжерів є значним «проривом» в історії людства, який значно розширив можливості та сприяв до інтеграції. Дані соціологічних досліджень свідчать, що саме за допомогою інтернету та соціальних мереж поширюється значна частина інформації і саме такий спосіб обміну та отримання інформації на сьогодні практично витіснив живе спілкування.

Прийнято вважати, що соціальні мережі – це простір, де кожен може висловити свою думку, виявити волю та бути незалежним.

Однак, чи можна бути впевненим, що інтернет – це лише свобода?

На жаль, епоха високих технологій та глобальної інформації як і будь-яке інше явище має свої плюси та мінуси. Одним з головних негативних аспектів є те, що інформація сьогодні стала не просто всезагальним благом, а й потужним інструментом впливу та маніпулювання свідомістю громадян.

Безперечно основною метою створення соціальних мереж перш за все була інтеграція світової спільноти, адже вони давали людям, які знаходяться у різних частинах планети можливість обмінюватись інформацією. Це був великий прорив в розвитку людства тому і не дивно, що вони дуже швидко набули великої популярності. Попит у спілкуванні та обміні інформацією збільшувався, тому

виникла потреба у винайденні все нових та нових соціальних мереж, які давали все більші можливості.

Звичайно така популярність соціальних мереж не могла не зацікавити, тому стало зрозуміло, що це може стати найпотужнішою зброєю для досягнення стратегічних завдань у політичній сфері.

Першими, хто почав використовувати соціальні мережі як засіб маніпулювання суспільною свідомістю були Росія та Китай і зовсім скоро це набуло поширення і в інших країнах світу. Так, за статистикою світової правової організації FreedomHouse, маніпуляції в соціальних мережах на сьогодні вплинули на результати виборів близько в 17 державах світу. Одним із найяскравіших прикладів цьому можуть слугувати вибори Президента США. Так для залучення більшої підтримки кандидата Трампа використовувався Твітер, який був його центром виборчої компанії, там працювали десятки тисячі ботів, завданням яких було створення ілюзії популярності кандидата. Такий прийом називається «виборчий консенсус». Його суть полягає в тому, що так звана ілюзія онлайн-підтримки кандидата спрямована на стимулювання реальної підтримки через ефект перемоги.

Як ж було створено цей ефект популярності?

Відповідь на це питання досить проста, на сьогодні боти є основним способом поширення інформації в соціальних мережах, яка є фундаментом для маніпулювання людською свідомістю.

Що ж являють собою боти? Це прості програми, які виконують одноманітні завдання, на які їх запрограмовано. Саме боти здійснюють так звану «модельовану пропаганду», тобто поширюють інформацію, яка не відображає дійсності, вводять людей в оману та не дозволяє реально сприймати ті чи інші явища. Так, зазвичай робота бота полягає у дублюванні неправдивої новини в соціальній мережі та поширенні її серед якнайбільшої аудиторії.

Саме за допомогою використання ботів думку однієї особи можна висвітлити як думку великої кількості громадян або придушити критику інакодумців.

Саме модельована пропаганда є одним із найпоширеніших способів використання ботів для маніпуляції суспільною думкою. Вона проходить наступним чином: першим етапом є публікування неправдивої інформації на відомому сайті чи особистому блозі, що здійснюється за допомогою корупції досить просто. Далі вступають в процес боти, вони поширюють таку інформацію серед користувачів інтернету і зазвичай цього достатньо, щоб привернути увагу провідних засобів масової інформації. ЗМІ свою чергу поширюють цю інформацію серед широкого кола населення, видаючи її за правду і в результаті отримуємо ефект сприйняття фейку за реальність, що відкриває великі можливості для маніпуляції населенням.

Яскравим прикладом цього може існувати ситуація, пов'язана з ураженням у 2014 р. літака рейсу MH17 авіакомпанії Malaysia Airlines. Так однією із теорій

літак був збитий українським винищувачем. Ця теорія виникла з Twitter - повідомлення іспанського авіадиспетчера Карлоса (@spainbusca), якого насправді не існує. Допис @spainbusca поширили інші користувачі соціальної мережі, а за ними засоби масової інформації, зокрема, телекомпанія RT, а також інші російські новинні агентства.

Як наслідок, у громадян Російської Федерації склалося неправильне уявлення про події, що в світлі стану сучасних відносин між нашими державами сприяло загостренню негативного ставлення до українців.

На жаль, це лише маленька частина в просторі глобальної маніпуляції. І сьогодні, в умовах постійної боротьби держав за вплив одна на одну, маніпуляції давно перестали бути чимось надзвичайним і стали повноцінною частиною повсякденного життя. Саме тому дуже важливо розвивати свою інформаційну культуру, вміти вчасно розпізнавати маніпулятивний вплив та твердо йому протидіяти.

Список використаних джерел:

1. Костюк Богдана «Соціальні мережі –місце маніпуляцій суспільною свідомістю» –URL:<https://www.radiosvoboda.org/a/28856229.html>
2. Лісовський П.М. «Феномен інтернету як засіб маніпуляції свідомістю в українському сучасному соціумі». –URL:http://novyn.kpi.ua/2005-3-1/04_Lisovskii.pdf

*Співак І. В., ст. викладач
ФСП КПІ ім. Ігоря Сікорського*

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ПРАВО ГРОМАДЯН НА ПРИВАТНІСТЬ

Глобальна інформатизація соціально-правових відносин сприяла лібералізації державної інформаційної політики.

Основними принципами європейської інформаційної політики є:

- захист і здійснення ідеалів загальноєвропейської спадщини, насамперед, визнання свободи слова та інформації одним з найважливіших принципів демократичного суспільства і необхідною умовою прогресу та розвитку кожної особистості;
- забезпечення вільного руху інформації та ідей, захист плюралізму і рівності можливостей для всіх демократичних груп і політичних партій, створення умов для вільного формування поглядів і переконань;
- забезпечення подальшого розвитку інформаційно-комунікаційних технологій;
- підтримка реалізації права вираження, пошуку, одержання і передачі інформації та ідей, незалежно від їх джерела;
- визнання необхідності узгодження меж регулювання аудіовізуального сектора в різних європейських країнах тощо [1].

У резолюції 59 (1) Генеральної Асамблеї ООН зазначається, що свобода інформації є основним правом людини і критерієм усіх інших свобод.

Одним з найважливіших прав людини є право на повагу до приватного життя (ст. 8 Конвенції про захист прав і основних свобод людини) та право на свободу виявлення поглядів (ст. 10 Конвенції).

Глобальна інформатизація ще більш актуалізувала необхідність забезпечити захист інформації про особу та права на повагу до приватного життя, що є важливим не тільки для самоствердження, а й для безпеки індивіда[2].

Оприлюднення в березні 2017 року міжнародною організацією WikiLeaks документів про можливе отримання Центральним розвідувальним управлінням США інформації через камери та мікрофони мобільних пристроїв з системами IOS та Android, комп'ютери з операційними системами Microsoft та Linux[3] свідчить про те, що Уряд (і не тільки) може збирати дані про телефонні розмови, інтернет-пошук тощо. А Тімоті Бернерс-Лі окреслив важливу проблему Інтернету: втрату контролю над особистими даними (веб-сайти не забезпечують можливості прямого контролю за персональними даними особи і не дозволяють відслідковувати про передачу персональних даних третім особам).

А в лютому 2016 р. Національна комісія з обробки даних та громадянських свобод Франції, яка здійснює нагляд за дотриманням законодавства про захист персональних даних, звинуватила соціальну мережу Facebook у зберіганні даних про віросповідання, політичні погляди, сексуальну орієнтацію користувачів, що є порушенням права людей на таємницю приватного життя.

Для забезпечення захисту персональних даних 14 квітня 2016 р. Європейським парламентом були ратифіковані GeneralDataProtectionRegulation (Загальні положення про захист даних), якими передбачають: право на стирання інформації; право на скаргу (згідно з яким особа може не погоджуватись на обробку своїх персональних даних); право на перенесення даних; а також передбачено штрафи за порушення конфіденційності даних [4].

Зазначений акт посів важливе місце серед багатьох інших, покликаних забезпечити захист права на приватне життя та захист персональних даних. Так, у ст. 17 Міжнародного пакту про громадянські та політичні права 1966 р. зазначено, що “ніхто не повинен зазнати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканість його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію”[5]. У ст. 8 Європейської конвенції про захист прав людини і основоположних свобод зазначено, що “кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції”[6], а у ст. 10 Конвенції зазначено, “1. Кожен має право на свободу висловлення своєї думки. Це право включає свободу дотримуватись своєї думки, отримувати і розповсюджувати інформацію та ідеї без втручання з боку державних органів і незалежно від державних кордонів. 2. Здійснення цих свобод, яке накладає обов'язки та відповідальність, може бути пов'язано із формальностями, умовами,

обмеженнями і штрафними санкціями, які передбачені законом та необхідні у демократичному суспільстві в інтересах національної безпеки, територіальної цілісності чи громадського порядку, з метою запобігання заворушенням та злочинам, захисту здоров'я і моральності, захисту репутації чи прав інших осіб, запобігання розголошенню інформації, отриманої конфіденційно, чи забезпечення авторитету та неупередженості правосуддя”.

Практика Європейського суду з прав людини конкретизує положення статті 10 Конвенції, зокрема, “вираження поглядів “поширюється на подання інформації в будь-якій формі (документи, спічі, зображення, дії, що виражають певну позицію чи подають відповідну інформацію), а також за допомогою будь-яких засобів (друковані та електронні ЗМІ, тощо). З огляду на зазначене, захист поширюється не тільки на саме вираження поглядів, але й на відповідні засоби вираження.

Слід зважати на те, що Суд при винесенні рішень керується не тільки положеннями статті 10, а й статей 8, 9, знаходячи баланс між положеннями статті 8, якою гарантовано право на недоторканість приватного життя (особливо актуальним є після загибелі в Парижі принцеси Діани), і статті 10, якою гарантовано право на вільне отримання та розповсюдження інформації.

Важливими для захисту права на приватність є Керівні принципи регулювання комп'ютерних файлів, які містять персональні дані, прийняті резолюцією № 95 Генеральної Асамблеї ООН [7].

Важливою також є Директива №95/46/ЄС Європейського парламенту та Ради ЄС “Про захист осіб у зв'язку з обробкою персональних даних та вільне переміщення таких даних ” від 24 жовтня 1995 р.[8].

Відповідно до ст.32 Конституції України ніхто не може зазнавати втручання в його особисте життя, а також не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законодавством [9].

Важливим етапом у забезпеченні захисту в Україні права на приватність є прийняття 01.06.2010р. Закону України ‘Про захист персональних даних’[10], а також затвердження у 2014 році Типового порядку обробки персональних даних; Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних; Порядку повідомлення Уповноваженого Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних та деяких інших.

Список використаних джерел:

1. Гнатюк С. Нормативно-правове регулювання діяльності аудіовізуальних ЗМІ в Європейському Союзі і в Україні: порівняльний аналіз. - URL:[http:// old. Niss. Gov. Ua/ Monitor/ fpril08/19htm](http://old.Niss.Gov.Ua/Monitor/fpril08/19htm).
2. Горпинюк О.П. Кримінально-правова охорона інформаційного аспекту приватності в Україні: автореф. дис. на здобуття наук. ступеня к.ю.н./ЛьвДУВС . – Львів, 2011. – С. 4.

3. Vault 7: CIA Hacking Tools Revealed. - URL: <http://wikileaks.org/ciav7p1/index.htm>
4. Data Protection Regulation.- URL: [http:// www. Eugdpr.org.html](http://www.Eugdpr.org.html)
5. Міжнародний пакт про громадянські та політичні права від 16.12.1966р.//36. Нормативних актів з питань правозахисної діяльності/упорядник С.Ф. Гончаренко. – Київ: Юрінком Інтер, 1995. – С.38-44.
6. Огляд практики Європейського суду з прав людини: Норми та стандарти Конвенції про захист прав і основних свобод людини/ Міністерство юстиції України. – К.: Видавничий Дім “ Ін Юре “, 2001. –64 с.
7. Резолюція Генеральної Асамблеї ООН №95 (XLV) : A/45/PV.68/Организация Объединенных Наций. – Официальный сайт ООН.
8. Директива №95/46/ЄС Європейського парламенту та Ради ЄС “Про захист осіб у зв’язку з обробкою персональних даних та вільне переміщення таких даних” від 24 жовтня 1995р.//Європейський Союз. - URL: <http://zakon4.rada.gov.ua/laws/show/994242>
9. Конституція України: чинне законодавство зі змінами та допов. станом на 18 серпня 2011 р.: (Офіційний текст).- К.: Паливода А.В., 2011. – 56 с.
10. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI//Верховна Рада України. – Офіційний вісник України від 09.07.2010р.- Офіц. вид.- 2010. - № 49. – С. 199. –Ст. 1604

Головатый А. А., студент

ФСП КПИ им. Игоря Сикорского

ЛИЧНАЯ ИНФОРМАЦИЯ И ЕЁ ОБОРОТ В ИНТЕРНЕТЕ

Информация всегда была важнейшим винтиком истории. Благодаря ей выигрывали войны, создавали всё новые и новые чуда технического прогресса, да что там говорить – само развитие человека стало возможным лишь потому, что он передаёт информацию лучше прочих живых существ. Именно появление, генерация, открытие новой для нас информации привело к небывалому развитию общества, в котором мы сейчас живём.

С каждым годом на планете Земля всё труднее найти место, где бы не было Интернета или же сотовой связи. Если раньше основной объем информации был достоянием немногих, то сейчас всё совершенно иначе – практически вся она теперь есть в открытом доступе в сети Интернет. Если раньше нужно было годами коптеть над пыльными книгами не самых известных авторов и учёных, то сейчас достаточно несколько раз нажать на клавиатуру, и вы получите желанную информацию. Казалось бы, вот оно – теперь люди станут гораздо умнее, а развитие человечества умчится вперёд со скоростью света. Так, возможно, думали его создатели ещё десять-двадцать лет назад, однако реальная жизнь показала нечто иное...

На сегодняшний день в интернете преобладает то, что хотелось бы назвать «информационным шумом» по аналогии с радио. Что вы видите первым, открывая ту или иную страницу в сети Интернет? Ожидаемый текст? Интересное видео?

Нет! Вы видите рекламу, хотите того или нет. Информация, зачастую вам неинтересная, по сути – тот же мусор, и сейчас в Интернете преобладает именно она. Легче всего это увидеть на примере бесплатных приложений, в особенности – социальных сетей. Ни для кого не секрет, что любая информация, будь то слово, видео- или аудиозапись, попадая в Интернет, остаются там навсегда. И если для большинства людей это тот же «информационный шум», который они скорее всего просто проигнорируют, то для некоторых – это способ незаконного заработка невероятных размеров прибыли. Почему незаконного? Для ответа на этот вопрос нужно вспомнить о таком явлении как «таргетинговая реклама». Рассмотрим её на примере одного из самых популярных Интернет-браузеров под названием “GoogleChrome”. Выглядит всё очень просто – такое-себе окошко, в котором размещена рекламная вывеска (таких всегда много на более-менее популярных сайтах). Размер окошка совсем небольшой, и на популярных сайтах их может быть даже больше десятка. Вот только реклама, размещенная в них, сгенерирована вовсе не случайно. Если, к примеру, вчера вы искали новую клавиатуру, то сегодня у вас появится куча рекламы со все той же клавиатурой. Как? На деле очень даже просто – путем анализа ваших запросов в интернете. В социальных сетях анализируются группы, на которые вы подписаны, загруженные вами приложения и прочее, и прочее, и прочее. Если присмотреться, подробным образом на сегодня работают практически все популярные приложения. Реклама уже давно стала одним из наиболее прибыльных сфер деятельности, но то, как она действует, становится всё более и более «грязным». Приведенные выше примеры – безобидны и даже полезны, но ведь это совсем не отражает того объема информации, которой они могут воспользоваться прямо сейчас. Если уже сегодня такие компании не боятся использовать данные из вашей личной жизни для собственного заработка, то что они сделают завтра? И наиболее важный вопрос: это вообще законно? Если вы обратили внимание, прежде, чем установить ту или иную программу, на экран всегда всплывает окно с пользовательским соглашением, без подтверждения которого программа установлена не будет. Возможно, в нем и содержатся пункты, соответственно которым вы прямо или косвенно соглашаетесь на использование ваших данных. Однако этот договор, если он противоречит правам человека, просто не может иметь юридического значения. Следовательно, из всего этого можно сделать два вывода. Первый – эти документы оформлены настолько качественно, что формально не нарушают прав человека, но тогда появляется вопрос: как вообще может быть юридически удовлетворительным то, что де-факто нарушает права человека? Второй – такие документы прямо противоречат правам человека, а это значит, что любая подобная деятельность незаконна.

Это лишь малая часть того, как можно использовать личную информацию пользователей, и считать, что эти способы никогда не будут задействованы – самообман. Пока что данные процессы никак не регулируются, в первую очередь из-за отсутствия механизма, способного на такое. Так или иначе, механизм

регулювання оборота личної інформації життєво необхідним для здорового існування людського суспільства, а інакше воно просто утоне в власній бруді. А поки оборот інформації користувачів дозволяє використовувати їх для вигоди тих, у кого немає моральних принципів, не говорячи вже про повагу до прав людини і законів.

Розділ 3 *РОЛЬ ТА МІСЦЕ ІНФОРМАЦІЙНОГО ПРАВА В СИСТЕМІ ПРАВА ТА ОСВІТИ*

Баранов О. А., д.ю.н., с.н.с, завідувач наукового відділу правового забезпечення у сфері інформаційних технологій НДІІП НАПрН України

МІСЦЯ, МЕТА І РОЛЬ ІНФОРМАЦІЙНОГО ПРАВА

В останні десятиріччя практично у всіх країнах відбувається дискусія щодо реформування системи освіти, зокрема і юридичної. Висуваються різні ідеї, пропонуються оновлені підходи, оприлюднюються різноманітні концепції та програми з вдосконалення вищої школи у сфері права. Зазвичай необхідність реформування обґрунтовується певними гаслами, наприклад: наявність змін, що відбулися в суспільстві (для країн колишнього СРСР (є справедливим і для України) – це відхід від соціалістичної ідеї, для інших – це трансформація економіки виробництва та споживання); докорінні зміни ринку та умов праці, що відбуваються під впливом впровадження нових технологій, зокрема завдяки досягненням 3-ї технологічної революції тощо.

Водночас майже без критичного аналізу сприймаються традиційні місця, мета і роль системи права, що сформувалися протягом останніх сторіч, але які, на наш погляд, потребують вивчення на відповідність сучасним умовам розвитку суспільства.

Беззаперечно, мета системи права (правового регулювання) повинна підпорядковуватися меті системи соціального регулювання, важливою складовою якої вона є, та гармонізуватися. За такої умови зміст соціальних правил поведінки, система соціального регулювання визначаються цілями та задачами розвитку суспільства або його конкретної сфери [1].

Автори, які досліджували теоретичні засади системи права, по-різному визначали мету системи соціального регулювання, а саме: визначення процесу, що обумовлює соціальний порядок в частині стабілізації та упорядкування соціальних відносин [1]; встановлення різноманітних соціальних норм (зокрема, норм права – авт.), які переслідують такі цілі й завдання – упорядкування та вдосконалення суспільного життя, внесення в нього організаційних засад, розвиток та збагачення особистості, захист прав людини, утвердження ідеалів

гуманізму, справедливості [2]; мета встановлення соціальних (авт.) правил поведінки в суспільстві – це досягнення його благополуччя [3]; соціальне регулювання забезпечує досягнення необхідного або бажаного стану суспільства [4]; задоволення потреби в узгоджених діях між людьми, спрямованих на досягнення конкретного, усвідомленого результату у процесі розвитку соціального середовища [5].

Підсумовуючи та узагальнюючи наведене вище, можна зробити висновок, що мета системи соціального регулювання – це забезпечення високої ефективності людської діяльності для досягнення конкретної цілі окремим індивідумом, групою індивідумів, певною соціальною групою та суспільством шляхом створення відповідних соціальних умов поведінки суб'єктів суспільних відносин. Всі інші редакції, які було напрацьовано багатьма дослідниками, вбачаються такими, які несуперечать цьому визначенню і віддзеркалюють певні окремі аспекти та грані процесу соціального регулювання.

Однією з основних умов забезпечення високої ефективності будь-якої людської діяльності є мінімізація транзакційних витрат. Транзакційні витрати – це непродуктивні витрати грошових, часових, організаційних, інтелектуальних, матеріально-технічних та інших ресурсів в процесі здійснення будь-якої діяльності між суб'єктами суспільних відносин.

З урахуванням положень теорії економіки права, які базуються на теоремі Р. Коуза (Нобелівській лауреат, 1991 р.), були запропоновані загальні рекомендації до формування правової системи [6]: закон (правові норми) повинен сприяти зниженню транзакційних витрат (витрати, які супроводжують взаємодію суб'єктів права один з одним), зокрема, усуваючи штучні бар'єри на шляху добровільного обміну та забезпечуючи виконання укладених контрактів.

Отже, надаємо наступне визначення: *місія та базова мета правової норми* – це створення правових умов для:

- забезпечення прав та задоволення інтересів суб'єктів суспільних відносин;
- врахування при цьому прав та інтересів третьої сторони (інших суб'єктів);
- мінімізації транзакційних (непродуктивних) витрат при реалізації суспільних відносин.

Таким чином, пропонується висновок про те, що *місія та базова мета системи (галузі, інституту) права* – це створення правових умов для забезпечення високої ефективності людської діяльності в будь-яких сферах або сегментах суспільної активності.

З іншої сторони, широко відомо, що *місія та базова мета застосування інформаційно-комп'ютерних технологій (ІКТ)* – це створення технологічних умов для забезпечення високої ефективності людської діяльності в будь-яких сферах або сегментах суспільної активності.

Оскільки майбутнє цивілізації залежить від рівня ефективності людської діяльності в будь-яких сферах суспільної активності, то, відтак, воно залежить і від наявності широкого та якісного застосування інформаційних комп'ютерних технологій та системи права.

Традиційно система права формувалась після встановлення усталеної практики утворення певних суспільних відносин, тобто після ретроспективного аналізу змісту, умов та соціальних правил створення суспільних відносин. Відомо, що раніше на такий ретроспективний аналіз потребувалося від декількох років до сотні. Але на початку XXI сторіччя виникає нагальна потреба у правовому регулюванні нових видів суспільних відносин, які:

- тільки-тільки почали з'являтися;
- будуть з'являтися у майбутньому.

Тому, вочевидь, у сучасних умовах потрібна зміна парадигми формування як окремих правових норм, так і загалом системи права, тобто потрібен перехід від ретроспективного аналізу вже сформованих суспільних відносин до побудови прогностичних моделей розвитку суспільства та правових моделей регулювання майбутніх суспільних відносин.

Сучасний стан розвитку суспільства характеризується [7]:

1) відбувається широке впровадження технологій Інтернету речей (ІКТ) на основі використання штучного інтелекту, робототехніки, різноманітних сенсорів, технологій блокчейн, «хмарних» технологій, «великих даних», технологій передачі даних (мережі Інтернет) тощо;

2) загальносвітовим визнанням того, що широке впровадження технологій Інтернету речей є генеральною умовою соціального розвитку та прогресу;

3) різким збільшенням кількості горизонтальних суспільних зв'язків типу реер-to-реер (P2P), що обумовлює зменшення різноманітних бар'єрів (валютних, транспортних, фінансових, адміністративних, митних тощо), завдяки чому мінімізуються транзакційні витрати.

Одночасно, слід зазначити, що багато країн вже обрали стратегію розвитку, побудовану на повсюдному використанні технологій Інтернету речей:

1. США: національна стратегія Інтернету речей – 2016 р.; законопроект «Розвиток інновацій и сприяння Інтернету речей» – січень 2017 р.;
2. Велика Британія: «Цифрова стратегія Великої Британії 2017»;
3. Південна Корея: генеральний план створення IoT -2014 р.;
4. Японія: «Стратегії роста Японії – 2016» (Індустрія 4.0, розвиток IoT, великих даних, робототехніки);
5. Китай: \$127,5 млрд. на державну програму з розвитку Інтернет речей до 2020 року; створення 500 розумних міст - 2017 р.;
6. ОАЕ – в уряді введено посаду міністра з питань штучного інтелекту.

За прогнозами багатьох експертів через 50-60 років очікується технологічний стрибок завдяки застосуванню досягнень технологій Інтернету речей, штучного інтелекту, нано- і біо- технологій, генетики, робототехніки тощо.

Наслідком цього буде стрибкоподібний технологічний прогрес, який призведе до такого феномену, як сингулярність, яка унеможливило сьгодні точне уявлення того, що буде відбуватись з людством через 50-60 років, тобто нівелює прогнозування релевантної моделі суспільства 80-х років 21 століття. Тому вбачається, що наразі також є неможливим спрогнозувати майбутній розвиток правової системи.

Водночас сьгодні можна впевнено стверджувати, що протягом наступних 50-60 років у всіх сферах суспільної активності відбудуться безпрецедентні технологічні зміни, які будуть обов'язково базуватись на використанні ІКТ. Тому використання ІКТ стане технологічною основою здійснення всіх суспільних відносин, які будуть потребувати правового регулювання.

Таким чином, правове забезпечення правовідносин буде обов'язково включати норми інформаційного права. Відповідно, протягом наступних 50-60 років інформаційне право стане необхідною та важливою складовою правового забезпечення будь-якої суспільної діяльності, тому розвиток теорії інформаційного права повинен базуватися на прогностичному підході з урахуванням можливих сценаріїв технологічного розвитку суспільства. Але за такої умови з'являється правова невизначеність через застосування технологій Інтернету речей: штучного інтелекту, роботів, робомобілей, технологій блокчейн, «хмарних» технологій, «великих даних» та багато іншого. Перед науковцями постане питання, яке треба застосовувати інформаційне законодавство у таких умовах: традиційне, модернізоване або зовсім нове.

З огляду на зазначене, вважаємо, що в якості пріоритетів потрібно визначити засади, напрями та проведення реформування правової системи держави, системи юридичної освіти та юридичної науки, а в рамках останньої забезпечити адекватний майбутнім вимогам розвиток системи інформаційного права.

Слід зауважити, що обґрунтування практично всіх робочих груп, творчих колективів і окремих експертів щодо необхідності проведення реформи юридичної освіти та юридичної науки базуються на такій основній тезі: зміст юридичної освіти не відповідає сучасним потребам ринку праці. Звичайно, це твердження є справедливим уже декілька десятків років, але ця поширена теза потребує поправки, яка, ми вважаємо, має стратегічне значення для майбутнього розвитку окремих людей, суспільства і держави. Уточнення полягає в наступному: сьгоднішній стан системи юридичної освіти, пропоновані стратегії, концепції та програми її реформування не відповідають не лише сьгоденним вимогам ринку праці, а й майбутнім потребам суспільства.

Юридична освіта повинна бути зорієнтована на надання майбутнім юристам таких знань, навичок та умінь, які стануть актуальними за декілька років.

Горизонт планування змісту системи юридичної освіти не повинен обмежуватися вимогами сьогодення, потрібно планувати на 5-10 років наперед.

На наше переконання, у найближчий час юрист має:

- знати та розуміти на системному рівні тенденції та закономірності розвитку предметної сфери, у якій він буде працювати за фахом;
- бути ініціатором у формуванні креативних та інноваційних юридичних пропозицій, які стануть базовими для вироблення будь-яких стратегій розвитку;
- вивчати різноманітні технології та перспективи їх розвитку з таким ступенем деталізації, який можна вважати достатнім для з'ясування їх впливу на виникнення особливостей здійснення суспільних відносин та їх правового регулювання;
- збільшити швидкість та якість реакції на соціальні запити та виклики;
- прагнути до оволодіння комплексною правовою спеціалізацією в умовах широкого застосування технологій штучного інтелекту, завдяки чому він буде позбавлений рутинної нетворчої роботи;
- впроваджувати новітехнологічно орієнтовані форми просування юридичних послуг та клієнт-орієнтований юридичний сервіс.

Список використаної літератури:

1. Теория государства и права: учебник. Отв. ред. - В. Д. Первалов. — 3-е изд., перераб. и доп. — М.: Норма, 2008. — 484 с.
2. Теория государства и права: курс лекций. Под ред. Н. И. Матузова и А.В. Малько. – 2-е изд., перераб. и доп. – М.: Юристъ, 2001. –776 с.
3. Шершеневич Г.Ф. Общая теория права: Философия права. Часть теоретическая Т. 1: Вып. 1-4 /– М.: Бр. Башмаковы, 1910. – 839 с.
4. Венгеров А.Б. Теория государства и права: Учебник для юридических вузов. 3-е изд. – М.: Юриспруденция, 2000. – .528 с.
5. Загальна теорія права: підручник. За заг. ред. М.І. Козюбри. – К.: Ваїте, 2015. – 392 с.
6. Р. Капелюшников, «Новая институциональная теория». - URL: <<http://www.libertarium.ru/10625>>
7. Баранов О.А. Интернет речей: теоретико-методологічні основи правового регулювання. Т.1:Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія. – К.: Видавничий дім «АртЕк». – 2018.–344 с.

Фурашев В. М., к.т.н., с.н.с., доцент
ФСП КПІ ім. Ігоря Сікорського

ПРАВО ТА ПРАВОВА ОСВІТА У СУЧАСНОСТІ

Сучасність, точніше, сучасний науково-технічний прогрес, а ще точніше, його результати та їх наслідки, суттєво, а у багатьох сферах життєдіяльності людства, можемо сказати, докорінним чином змінюють середовище існування, світове суспільство, суспільні відносини на всіх рівнях. Змінюють звичні

людські, національні та міжнаціональні орієнтири, звичні системи цінностей та ін.

Право, як основний регулятор суспільних відносин на національному та міжнаціональному рівнях, об'єктивно не може бути осторонь цих процесів.

Право, як сукупність правової науки, правотворення, правозастосування, правоохоронення та системи підготовки кадрів, за своїм призначенням, повинно бути в середині, центрі цих процесів.

Україна, не зважаючи на всі “негаразди”, які її переслідують майже всі роки з моменту отримання державної незалежності, також не може бути поза межами цих процесів. В Україні також, як у будь якій країні світу, діють об'єктивні закони взаємозв'язку розвитку національного суспільства зі світовим. Як відоме, дію об'єктивних законів не можливо відмінити – їх можна лише призупинити, пригальмувати.

Коли світ змінюється, то змінюються і складові забезпечення життєдіяльності суспільства, в тому числі і правового забезпечення цій життєдіяльності.

Колись та, поки ще і наразі, основною функцією права було і є встановлення правовідносин на основі відносин які вже склалися у суспільстві, міждержавних відносин. У таких умовах, **право є констатуючою, обслуговуючою складовою** забезпечення життєдіяльності суспільства, тим більше, що часу для встановлення подібним чином правовідносин було значно більше.

У 21-ому сторіччі ситуація кардинально змінилася у зв'язку з надто високими темпами науково-технічного процесу та впровадження його результатів у реальне життя, масштабами та глибиною наукових досліджень, непередбачливістю наслідків результатів деяких досліджень та ін. Цілком зрозуміло, що все це впливає на визначення акцентів у системі забезпечення життєдіяльності суспільства. Те що вчора було головним, наразі вже другорядне та навпаки.

Спрямованість та темпи науково-технічного прогресу, а також, саме головне, темпи впровадження його результатів об'єктивно становлять право в один ряд зі всіма фундаментальними науками, які визначають цей прогрес.

Право, особливо правова наука, правотворчість та правозастосування, у сучасності повинно бути не **констатуючим**, а **формулюючим**.

Право повинно не просто встановлювати правовідносини, а формувати суспільні відносини через інститут випереджаючого встановлення правовідносин на основі інструментаріїв інформаційного та соціально-правового моделювання і прогнозування наслідків для суспільних відносин результатів науково-технічного прогресу.

Але це потребує досить суттєвої трансформації поглядів на роль і місце права в системі забезпечення життєдіяльності суспільства, ролі і місця галузей права в системі права. Це обов'язково потребує визначеної трансформації

інституцій правозастосування, правоохоронення та, саме головне, в системі підготовки кадрового забезпечення системи права, яка відповідатимуть викликам сучасності.

Це дуже складне завдання, але це – об'єктивна вимога сучасності. Нехтування цим буде мати дуже негативні наслідки як для держави та суспільства в цілому, так і для кожної людини у частості.

Завдяки цьому, може до кінця не усвідомлюючи наведене вище але відчуючи це на професійно-інтуїтивному рівні, у грудні 2011 року Науково-дослідний центр правової інформатики (с 03.10.2012 р. – Науково-дослідний інститут інформатики і права) Національної академії правових наук України звернувся (вих. № 10 від 16.01.2012 р.) до Національного технічного університету України «Київській політехнічний інститут» з пропозицією щодо розгляду можливих напрямів спільної наукової, науково-навчальної співпраці з метою концентрації та координації зусиль представників різних суміжних наук при вирішенні сучасних проблем в інформаційній сфері у зв'язку з новими викликами та загрозами, які викликали наслідки результатів науково-технічного прогресу. Дана пропозиція була розглянута та підтримана шляхом підписання 06 вересня 2012 року відповідного Договору про співробітництво (далі – Договір). Основною метою Договору є концентрація та координація зусиль представників різних галузей науки для вирішення проблем розробки правових основ і належного правового регулювання інформаційної діяльності людини, суспільства і держави, а також суспільних інформаційних відносин, що виникають в гуманітарній, економічній, фінансовій, телекомунікаційній та інших сферах в сучасних умовах стрімкого розвитку інформаційних технологій, становлення інформаційного суспільства та входження України у світовий інформаційний простір.

Договіром, крім інших його цілей та завдань, передбачалося також участь НДПП НАПрН України у науково-педагогічній діяльності НТУУ «КПІ», підготовка та впровадження у навчальний процес підручників, навчальних і навчально-методичних посібників та інших видань з питань інформаційних технологій і права та спільна організація і проведення конференцій, симпозіумів, семінарів, круглих столів та експертних зустрічей, у тому числі міжнародних, з питань розвитку інформаційних технологій і права.

З метою об'єднання ресурсів, потенціалу і досвіду Сторін для реалізації спільних проєктів, що становлять предмет цього Договору, було передбачено створення на базі НТУУ «КПІ», за безпосередньої участі Факультету соціології і права та Фізико-технічного інституту НТУУ «КПІ», спільного навчально-наукового підрозділу.

За результатами підготовчої роботи по втіленню у життя основних положень зазначеного Договору 1-го липня 2013 року Вчена рада НТУУ «КПІ» (протокол №8) схвалила створення спільного Навчально-наукового центру інформаційного права та правових питань інформаційних технологій у складі Факультету соціології і права НТУУ «КПІ», а також «Положення про Навчально-

науковий центр інформаційного права та правових питань інформаційних технологій».

18 жовтня 2013 року, тобто рівно 5 років тому, було підписане ректором НТУУ «КПІ» М.З. Згуровським наказ № 1-270, погоджений з директором НДІП НАПрН України В.Г. Пилипчуком, *«Про створення Навчально-наукового центру інформаційного права та правових питань інформаційних технологій»*.

У наказі ректора НТУУ «КПІ» вказане, що Центр створюється «відповідно до законів України «Про вищу освіту», «Про наукову і науково-технічну діяльність», статуту Національного технічного університету України «Київський політехнічний інститут», Договору про співробітництво між НТУУ «КПІ» та НДІП НАПрН України і рішення Вченої ради НТУУ «КПІ» від 01 липня 2013 року (протокол №8), з метою сприяння та координації у здійсненні міждисциплінарних наукових досліджень та у підготовці фахівців освітньо-кваліфікаційних рівнів «бакалавр», «спеціаліст» і «магістр» у сфері інформаційного права та правових питань інформаційних технологій.

Відповідно до наказу № 1-270 від 18.10.2013 р. визначається, що «Науково-методичне забезпечення і координація наукової діяльності Центру покладається на Науково-дослідний інститут інформатики і права Національної академії правових наук України».

Таким чином, у під час роботи даної конференції відзначається й **п'ятарічниця** спільного Навчально-наукового центру інформаційного права та правових питань інформаційних технологій.

До основних досягнень Центру за цей період слід віднести:

1. Започаткування та становлення процесу кадрового забезпечення інформаційного права, інформаційної безпеки вимогам не лише сьогодення, а й майбутнього, маючого основні наступні основні компетенції:

– свідоме розуміння об'єктивної необхідності впровадження, у майбутньої діяльності, принципів, методів та механізмів формуючого права;

– свідомого розуміння, що в умовах політичної та соціально-економічної нестабільності внутрішніх та міждержавних відносин, їх «гібридності», право є суттєвою зброєю захисту державного суверенітету, національних інтересів, національної безпеки, прав та свобод людини;

– розуміння природи, явищ та процесів, які здійснюють вплив на формування та трансформацію суспільних відносин;

– аналітичного мислення, знання структури обраної галузі права та основних законодавчих положень даної галузі права, вміння роботи з джерелами правової інформації, орієнтуватися у суті правовій проблемі, яка виникла та швидко знаходити законодавче вирішення даної проблеми.

2. З метою практичної реалізації наведених вище компетенцій професорсько-викладацьким складом було розроблено та впроваджено у навчальний процес **15 навчальних дисциплін** з відповідними навчально-методичними матеріалами, які щорічно оновлюються, вплоть до повноно

перегляду, зокрема: «Основи інформаційного права», «Інформаційне право» та «Проблеми інформаційного права» (Баранов О.А., Фурашев В.М.), «Міжнародне інформаційне право» (Золотар О.О., Довгань О.Д.), «Інформаційне суспільство і право» (Золотар О.О.), «Інформаційні ресурси» (Золотар О.О.), «Основи інформаційної безпеки» та «Правові аспекти інформаційної безпеки» (Фурашев В.М., Петряєв С.Ю.), «Правова інформатика» (Ланде Д.В., Юдкова К.В.), «Сучасні методи інформаційного та соціально-правового моделювання» (Ланде Д.В.) та ін.

Також були розроблені навчально-методичні матеріали з дисципліни «Правові основи інформаційної безпеки» (Фурашев В.М.) для опанування студентами інших спеціальностей, які готуються в КПП ім. Ігоря Сікорського, базовими знаннями правового вирішення питань у сфері забезпечення інформаційної безпеки.

3. Спільна робота Центру та кафедри інформаційного права і права інтелектуальної власності ФСП КПП ім. Ігоря Сікорського упродовж минулих 4-ох навчальних років дозволила визначити базову структуру дисциплін навчального циклу інформаційного права та правових питань інформаційних технологій.

4. За 4-і повних навчальних років дисципліни з навчальних курсів у сфері інформаційного права та інформаційної безпеки прослухало понад 420 студентів різної форми навчання зі спеціальності 081 «Право», а також понад 260 студентів денної форми навчання інших факультетів та інститутів КПП ім. Ігоря Сікорського прослухали навчальну дисципліну «Правові основи інформаційної безпеки». На даний час слухають дані дисципліни біля 85 та 210 студентів відповідно.

Крім того необхідно відмітити, що за ці роки під науковим керівництвом співробітників Центру було підготовлено та успішно захищені 20 дипломних робіт на здобуття спеціальності «спеціаліст з спеціальності 081 «Право» за тематикою інформаційного права та інформаційної безпеки, а також – 7 магістерських дисертацій.

Цілком зрозуміло, що наведене всього лише початок практичної підготовки нової формації працівників правової сфери до роботи у зовсім інших умовах, переосмислення ролі та місця права у сучасності.

*Корж І. Ф., д.ю.н., с.н.с.,
завідувач науковою лабораторією
НДІІП НАПрН України*

ІНФОРМАЦІЙНЕ ПРАВО У ЖИТТІ СЧАСНОЇ ЛЮДИНИ **Добрий день, шановні колеги!**

Хочу ще раз привітати усіх з ювілейною датою нашої Академії та побажати усім співробітникам високих звершень і здобутків на науковій ниві, особистого щастя і здоров'я.

У цей день не можу пару слів сказати про Академію. Перекоаний, що створення та функціонування Національної академії правових наук – непересічне явище у житті нашої держави, адже його можна назвати своєрідним логічним кроком після досягнення багатоміліардної мрії українського народу – здобуття незалежності Україною. Як і будь-яка держава, Україна створює відповідні інституції, що обумовлюється необхідністю регулювання суспільних відносин. І саме Національна академія правових наук, яка, як зазначає її Почесний Президент Василь Якович Тацій, акумулює творчий потенціал провідних наукових установ та навчальних юридичних закладів України, приймає активну участь у процесі реформування вітчизняної правової системи, сприяє законодавчому забезпеченню, розвитку необхідних для ідеології державного будівництва соціально орієнтованих ринкових відносин, захисту прав людини та основних свобод, рівності кожного перед законом, утвердженню верховенства права, реалізації правового захисту, взаємної відповідальності держави та громадянина.

Академія та її установи беруть безпосередню участь у розробці та реалізації цілої низки найважливіших загальнодержавних програм правового забезпечення інноваційного розвитку, інвестиційної діяльності, розвитку місцевого самоврядування, адаптації законодавства України до законодавства Європейського Союзу тощо.

Одним із важливих напрямків функціонування Академії є подальший розвиток інформаційного права, і це є пріоритетним завданням академічного інституту інформатики і права. Я перекоаний, що кожен розуміє надзвичайну важливість таких напрямів інформаційного права, як гарантії прав і свобод людини в інформаційній сфері (своєрідний базис інформаційного права), забезпечення реалізації зазначених прав і свобод; забезпечення інформаційної безпеки; регулювання правових режимів інформації та інформаційних ресурсів.

У діяльності будь-якої держави, суспільства і кожної людини важливу роль відіграє таке явище, як право – в цілому, так інформаційне право – зокрема. Без нього жодне суспільство не змогло б існувати мирно і упорядковано, і жодна держава не змогла б розвиватися. Ця система правил висловлює індивідуальні та загальні інтереси всіх громадян держави.

Що ж до інформації та інформаційного права, то сьогоднішні події навколо України (гібридна війна і гібридні спецоперації Росії проти України) свідчать про

напрочуд високу важливість інформації у повсякденному житті не лише українського суспільства. Інформація майже завжди займала вагоме місце в житті людини. Еволюція людства, формування нашого суспільства та виникнення державних інституцій завжди були пов'язані з накопиченням, поширенням та обробкою відповідної інформації. Тому важко собі уявити повноцінну людську спільноту без інформаційних процесів.

Необхідно зазначити, що п'ята інформаційна революція асоціюється з винаходом електронно-обчислювальної техніки, появою персонального комп'ютера, створенням комп'ютерних мереж та комунікацій. Шосту інформаційну революцію пов'язують з формуванням та розвитком трансграничних глобальних інформаційно-телекомунікаційних мереж (кін. ХХ – поч. ХХІ ст.), що сьогодні охоплюють усі континенти та держави, проникають у кожний дім і в кожную оселю, впливають на кожную людину та суспільство в цілому.

Інформаційно-телекомунікаційні мережі на даний момент інтегрують у єдиному інформаційному просторі всіх суб'єктів інформаційної діяльності (фізичні та юридичні особи, органи державної влади та місцевого самоврядування) та засоби інформаційної діяльності (засоби зв'язку та телекомунікації, програмно-технічні засоби). В існуванні інформаційно-телекомунікаційних мереж зацікавлені всі користувачі, оскільки у них з'являються унікальні можливості здобути або передати потрібну інформацію, значно полегшити свою роботу чи виконання завдання, зайнятися новими видами діяльності у мережах тощо.

Інформація у різних її формах набуває все більш важливого значення, стає потужним ресурсом, товаром, що стоїть на «вітринах» поряд з іншими матеріальними благами. Само суспільство у зв'язку із вищезазначеним кардинально змінюється, стає більш інформаційним. Інформаційне суспільство являє собою різновид постіндустріального суспільства, що пов'язаний зі становленням та домінуванням «четвертого сектору» економіки – інформаційного, який гармонійно співіснує разом з трьома відомими секторами (сільське господарство, промисловість та сфера послуг). Водночас слід зазначити таку невід'ємну ознаку інформаційного суспільства, як наявність демократичного режиму та орієнтації на побудову правової держави, оскільки інтереси отримання повної, достовірної інформації не стикуються із обмеженням прав людини, цензурою та іншими негативними явищами, що характерні для недемократичного ладу. Такий міжнародно-правовий документ як Окінавська хартія глобального інформаційного суспільства (Окінава, 22 липня 2000 року) присвячений, головним чином, питанням ефективного використання можливостей цифрових технологій, ліквідації електронно-цифрового розриву в області інформації та знань всередині держав і між ними.

За таких умов значно зростають можливості громадян у реалізації свого конституційного права на інформацію. Гарантії прав і свобод людини щодо інформаційної сфери належать до найважливіших засад формування правової

держави та громадянського суспільства. Такі права передбачені і в дієвому механізмі державного управління в демократичному суспільстві. Це робить забезпечення захисту прав і свобод людини в інформаційній сфері однією з найважливіших цілей інформаційної безпеки, а саму людину – найголовнішим її об'єктом.

Одним із напрямків наукових досліджень нашого інституту є напрацювання правових механізмів для забезпечення гарантії прав і свобод людини в інформаційній сфері. Так, метою дослідження є розробка науково-методичних, інформаційно-аналітичних та правових засад, пропозицій і рекомендацій щодо принципів, концептуальних, методологічних, доктринальних положень, а також удосконалення законодавства з метою формування інформаційно-комунікаційних та організаційних складових національної інтегрованої системи нормативно-правових актів в умовах децентралізації влади в Україні.

Зазначене планується досягти шляхом вивчення та аналізу актуальних правових проблем децентралізації влади в Україні в частині перерозподілу повноважень, функцій та фінансів з центрального на місцевий рівень управління; дослідженням проблем формування і функціонування інформаційних правових відносин в умовах здійснення децентралізації влади в Україні та відповідних змін у сфері інформаційних потоків у законотворчій та законодавчій роботі; напрацюванням пріоритетних, науково-обґрунтованих методів і правових механізмів інформаційно-комунікаційного та організаційного забезпечення формування та функціонування національної інтегрованої системи нормативно-правових актів в Україні; сприянням розвитку складових електронного парламенту, формування електронних баз даних нормативно-правових актів в галузі держави і права, як основи створення національної інтегрованої системи нормативно-правових актів в Україні; дослідженням питання інтеграції національної системи нормативно-правових актів в Україні до відповідних електронних баз даних Європейського Союзу.

Це дозволить забезпечити органи державної влади та місцевого самоврядування повною і достовірною нормативно-правовою інформацією в галузі держави і права, сприятиме підвищенню рівня їхньої нормотворчої та правозастосовної роботи. Буде також започатковано процес підтримки нормотворчої діяльності державних службовців та службовців органів місцевого самоврядування, науковців та громадськості за допомогою інтегрованої бази даних нормативно-правових актів.

Створення теоретико-правової бази системної інформатизації нормотворчої діяльності на усіх рівнях надасть можливість:

– унормувати застосування засобів системної інформатизації для розбудови національного інформаційного простору в складі інформаційно-аналітичних систем і баз даних нормативно-правових актів парламенту, уряду, міністерств та відомств, регіональних органів місцевого самоврядування;

– розробити єдині вимоги та правила формування електронних інформаційних ресурсів;

– забезпечити інформаційну відкритість та інформаційну взаємодію між парламентом, органами державної влади, регіональними органами місцевого самоврядування та громадянами; ведення, доступ, зберігання та обмін інформацією. Тим самим, зазначене буде відповідним вкладом у розвиток демократичних засад нашої Вітчизни та інформаційного права.

Переконаний, що дослідники інституту, докладаючи зусиль у вирішенні поставлених завдань, зможуть досягти належних результатів у своїх наукових пошуках, зробивши відповідний вклад у справу побудови інформаційного суспільства в Україні.

*Заярний О. А., д.ю.н., доцент
Київського національного
університету імені Тараса Шевченка,
Член Науково-консультативної ради при
Верховному Суді України*

ВИЗНАЧЕННЯ ПРЕДМЕТА ГАЛУЗІ ІНФОРМАЦІЙНОГО ПРАВА В ПРАКТИЦІ ВЕРХОВНОГО СУДУ УКРАЇНИ: ДЕЯКІ ТЕОРЕТИКО-ПРИКЛАДНІ АСПЕКТИ

Однією із змістоутворюючих ознак будь-якої галузі права, що визначає її сутність, обумовлює місце в системі права є предмет правового регулювання [1, с. 97].

Щодо інформаційного права, ця галузева ознака піддавалася глибоким науковим дослідженням, результатом яких стало вироблення різних доктринальних підходів до визначення інформаційних правовідносин у відповідному значенні [2, с. 118; 3, с. 32].

Серед дослідників, чії наукові праці зробили значний внесок у формування предмета галузі інформаційного права необхідно відзначити: І. В. Арістову, О. А. Баранова, І. Л. Бачило, К. Є. Белякова, О. Д. Довганя, Р. А. Калюжного, О. В. Кохановську, П. У. Кузнецова, І. В. Панову, В. Г. Пилипчука та інших.

У той же час, істотне зростання кількості справ про порушення норм інформаційного законодавства, переданих на розгляд за останні роки до Верховного Суду України, (далі – ВСУ), предметна розпорошеність таких спорів по різних судовим юрисдикціям поряд з відсутністю однозначної позиції ВСУ щодо визначення сутності інформаційних правовідносин обумовлює перед юридичною наукою формування важливого інституційного завдання. Його сутність полягає у необхідності виявлення методологічних зв'язків між правовими позиціями ВСУ щодо визначення елементів інформаційних правовідносин та сучасним станом доктринальної розробки поняття «предмет галузі інформаційного права», виявлення на цій основі основних розбіжностей у

теоретичних і правозастосовчих підходах до розуміння змісту відповідних категорій. Саме реалізація цих завдань і зумовлює мету даної роботи.

Предметом роботи є правові позиції ВСУ, в яких розкриваються елементи предмета галузі інформаційного права, узагальнюються їх окремі властивості.

Визначаючи правила підвідомчості справ про порушення інформаційних прав особи судам загальної юрисдикції, норми процесуального законодавства України не використовують поняття «інформаційні відносини», так само, як і не передбачають уніфікованого підходу до визначення сутності їх окремих елементів. Така побудова предметної юрисдикції відповідної категорії справ певною мірою ускладнює юридичну можливість виокремлення процесуальної складової при визначенні предмета галузі інформаційного права.

У той же час, аналіз змісту окремих постанов ВСУ, винесених за результатами розгляду різних категорій інформаційних спорів [4;5], дозволяє виокремити ряд безпосередніх властивостей інформаційних відносин, акцентуючи увагу на яких найвищий орган в системі судів загальної юрисдикції фактично формує процесуальне підґрунтя для визначення предмета галузі інформаційного права. Йдеться передусім про суб'єктів спірних правовідносин, їх об'єкт, об'єкт судового захисту, тобто зміст порушених інформаційних прав, свобод та інтересів сторін інформаційного спору, нормативні підстави відкриття провадження у відповідному касаційному суді у складі ВСУ тощо.

Так, зокрема, згідно з мотивувальною частиною постанови ВСУ від 19.09.2018 р. у зразковій справі N 806/3265/17 (Пз/9901/2/18) за позовом ОСОБА_2 до Коростенського районного відділу Управління Державної міграційної служби України в Житомирській області, Управління Державної міграційної служби України в Житомирській області про визнання протиправною бездіяльності та зобов'язання вчинити певні дії: «... Велика Палата Верховного Суду вважає за доцільне зазначити, що реалізація державних функцій має здійснюватися без примушення людини до надання згоди на обробку персональних даних, їх обробка повинна здійснюватися, як і раніше, в межах і на підставі тих законів і нормативно-правових актів України, на підставі яких виникають правовідносини між громадянином та державою. При цьому, згадані технології не повинні бути безальтернативними і примусовими. Особи, які відмовилися від обробки їх персональних даних, повинні мати альтернативу - використання традиційних методів ідентифікації особи» [4].

Аналіз наведеного висновку ВСУ показує, що наголошуючи на інформаційно-правовій сутності, суб'єктного складу, об'єкта, предмета та змісту спірних правовідносин, ВСУ водночас, уникає прямого визнання таких правовідносин інформаційними, а нормативних підстав їх виникнення актами інформаційного законодавства. Такий правозастосовчий підхід вбачається дискусійним та таким, що веде до ігнорування особливостей спірних правовідносин, які складаються у сфері обігу персональних даних.

Разом з тим, постановка основного акценту на необхідності відновлення права на невтручання в особисте, сімейне життя при виконанні державою покладених на неї функцій, межах, цілях, суб'єктах та способах обробки персональних даних, дає підстави вважати, що саме через встановлення інформаційно-правової сутності окремих елементів, ВСУ в такий спосіб визначає належність спірних правовідносин до категорії інформаційних. В цьому зв'язку, проблема визначення предмета галузі інформаційного права одержує своє вирішення через процесуальне доведення юридичного зв'язку конкретних елементів спірних правовідносин з інформаційною діяльністю, в результаті здійснення якої і формується предмет відповідної галузі права.

Поряд з оцінкою елементів спірних правовідносин, що складають предмет галузі інформаційного права, ВСУ допускає застосування у своїй практиці також і інших критеріїв, в яких розкривається їх прямиий зв'язок з інформаційною діяльністю.

З огляду на зміст мотивувальної частини постанови Касаційного адміністративного Суду України у складі ВСУ від 26.06.2018 р. у адміністративній справі №826/2810/17 за позовом фізичної особи-підприємця ОСОБА_2 до Виконавчого органу Київської міської ради (Київської міської державної адміністрації), третя особа без самостійних вимог на предмет спору - Департамент містобудування та архітектури виконавчого органу Київської міської ради (Київської міської державної адміністрації) про зобов'язання вчинити дії за касаційною скаргою Виконавчого органу Київської міської ради (Київської міської державної адміністрації): «Колегія суддів також враховує, що дотримання всіх вимог до розміщення зовнішньої реклами у м. Києві становить значний суспільний інтерес, оскільки столичний статус міста покладає на органи місцевого самоврядування та органи виконавчої влади додаткові обов'язки та гарантує цим органам надання з боку держави додаткових прав, зокрема, у сфері здійснення заходів щодо збереження та відновлення пам'яток історії, культури, релігії, архітектури та містобудування, заповідних та природних зон і ландшафтів, що мають національне значення (частина п'ята статті 1, пункт 5 частини першої статті 4 Закону України «Про столицю України - місто-герой Київ»)).

Пов'язуючи правомірність дій суб'єктів рекламних правовідносин з категорією «суспільного інтересу», Касаційний адміністративний суд України у складі Верховного Суду тим самим встановив безпосередній зв'язок між результатами реалізації інформаційних правовідносин та суспільним інтересом щодо задоволення інформаційних потреб жителів територіальної громади.

Узагальнення змісту наведених постанов вказує на те, що ВСУ здійснює практичний вплив на формування предмета галузі інформаційного права шляхом визнання інформаційно-правової сутності за окремими елементами спірних правовідносин, встановлення юридичного зв'язку між суспільним інтересом, наявним в інформаційній сфері та результатами інформаційної діяльності. У той же час, в практиці ВСУ залишається відкритим питання про вироблення

універсальних критеріїв виокремлення із категорій спірних публічних та приватних правовідносин тих, які мають інформаційно-правову сутність. Саме такі процесуальні критерії могли б не лише сприяти законодавчому оформленню категорії «інформаційних спорів» в окрему складову предметної юрисдикції ВСУ, а й інституалізації спірних інформаційних правовідносин, як окремого наукового поняття з відповідним матеріальним та процесуальним наповненням. Таким чином, на сьогоднішній день вплив практики діяльності ВСУ на формування предмета галузі інформаційного права відбувається лише шляхом процесуального встановлення належності окремих елементів спірних правовідносин до категорії інформаційних з подальшим їх охопленням предметом відповідної галузі права.

Список використаних джерел:

1. Загальна теорія права: підручник / за заг. ред. М. І. Козюбри. – К.: Ваіте, 2015. – 392 с.

2. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: [монографія]./О. А. Баранов. – К.–Едельвейс.– 2014.–434 с.

3. Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія / О.А. Заярний. – Херсон: Видавничий дім «Гельветика», 2017. – 700 с.

4. Постанова Великої палати Верховного Суду України від 19.09.2018 р. у зразковій справі N 806/3265/17 (Пз/9901/2/18) за позовом ОСОБА_2 до Коростенського районного відділу Управління Державної міграційної служби України в Житомирській області, Управління Державної міграційної служби України в Житомирській області про визнання протиправною бездіяльності та зобов'язання вчинити певні дії / [електронний ресурс]: <https://verdictum.ligazakon.net/document/76822787>.

5. Постанова колегії суддів Касаційного адміністративного Суду України у складі Верховного суду від 26.06.2018 р. №826/2810/17 за позовом фізичної особи-підприємця ОСОБА_2 до Виконавчого органу Київської міської ради (Київської міської державної адміністрації) про зобов'язання вчинити певні дії. - URL: <http://advocat-cons.info/index.php?newsid=51404>

*Гордієнко С. Г., д.ю.н., доцент
ФСП КПІ ім. Ігоря Сікорського*

ОСНОВНІ ПОНЯТТЯ СФЕР ІНФОРМАЦІЙНОГО ПРАВА, ІННОВАЦІЙНОЇ ДІЯЛЬНОСТІ ТА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ЯК СИСТЕМОУТВОРЮЮЧІ АСПЕКТИ ЇХ РЕГУЛЮВАННЯ

Починаючи розмову про понятійно-категоріальний апарат, слід визначити **основні правила його формування**: визначення повинно бути ясним; поняття як система знання – це сукупність відомих нам як основних, так і похідних ознак, що мисляться у понятті предметів, а також знання про те, у яких конкретних формах існують у дійсності ці предмети, що узагальнюються в понятті; одним з найважливіших правил утворення понять також є «закон тотожності» – не називай ту саму річ двома різними іменами і не називай дві різні речі тим самим ім'ям; у

визначенні не повинно бути кола – термін, що зустрічається у визначальній частині, не повинен визначатися через обумовлений термін; предмет є таким, що лише ця форма діяльності свідомості йому відповідає, що лише за допомогою цього способу може бути відтворений, відображений у свідомості (у мисленні); зрозуміти явище – це означає з'ясувати його місце і роль у конкретній системі явищ, що взаємодіють, у якій воно з необхідністю здійснюється, і з'ясувати саме ті особливості, завдяки яким це явище може грати визначену роль у складі цілого; зрозуміти явище – означає з'ясувати спосіб його виникнення, «правило», за яким це виникнення відбувається з необхідністю, закладеною в конкретній сукупності умов, проаналізувати самі умови виникнення явища; визначення повинно бути співрозмірним – визначальна частина повинна виділяти саме той клас предметів, що представляє те, що визначається.

Існування великої кількості визначень **інформації** зумовлено складністю, специфічністю і різноманіттям підходів до тлумачення сутності цієї категорії. Відомі три найбільш поширені концепції інформації, кожна з яких по-своєму пояснює її сутність. Вони не існують незалежно одна від одної, а доповнюють одна одну, висвітлюють різні сторони філософської категорії «інформація», але не дають однозначної відповіді стосовно її суті внаслідок крайньої її багатозначності, що є результатом змішання повсякденних, наукових і технічних значень.

Нами **інформація** визначається як відомості, отримані людиною в процесі діяльності з пізнання інформації. Це осмислені людиною відомості про навколишній світ і процеси, що відбуваються в ньому. Інформація існує незалежно від пізнання її людиною, і лише пізнана інформація стає відомостями.

Наступним є поняття **знання** – це перевірений практичною діяльністю людини результат пізнання відомостей про навколишній світ.

Вивчення **інновації** як соціального феномена дозволяє зробити висновок про те, що інноваційний розвиток сучасного суспільства має негативну, тривожну тенденцію: здійснюється масштабно, але стихійно.

Терміни «нове», «новація», «інновація», «нововведення» широко використовуються у повсякденній практиці і нерідко ототожнюються, хоча дещо різняться за своєю сутністю. Їх об'єднує те, що вони відображають розвиток шляхом оновлення.

Загалом **інновацію описують як: процес, сукупність** технічних, виробничих і комерційних **заходів**, що спричиняють появу на ринку нових товарів, промислових процесів та устаткування; **результат**, який дістав втілення у вигляді нового або удосконаленого продукту; **новий продукт** або послугу; **оригінальне рішення**, що володіє **світовою новизною** і одержало втілення в доступних споживачам продуктах; **нові або вдосконалені** конкурентоздатні **технології**.

Основними ознаками інноваційної діяльності є: впровадження, використання та комерціалізація результатів наукових досліджень й розробок у виробництво і соціальну сферу; нематеріальні блага – результати інтелектуальної

діяльності (результати наукових досліджень і розробок), які доводяться до стану інноваційного продукту та впроваджуються як інновації; довгостроковий характер; високий ступінь непередбачуваності наслідків та результатів, тобто ризиковий характер; супроводжується інвестуванням коштів у нематеріальні об'єкти – результати наукових досліджень і розробок – з метою їх впровадження та/або використання; позитивні соціально-економічні зрушення; підвищення конкурентоздатності суб'єктів господарювання та продукції, що ними випускається на базі реалізації інновацій.

На наш погляд, **інновація** – це якісно нове знання, яке може бути комерціалізованим.

На нашу думку, нова інформація чи **нове знання народжується в духовній, науковій, науково-технічній й «нетрадиційній» сферах**. До цього слід додати, що духовні досягнення чи надбання можуть бути класифіковані як загально- так і конкретно людські; наукові узагальнення можуть здійснюватися як суто теоретичного характеру, так і прикладного, технічні досягнення можуть мати загальнолюдський, загальнодержавний рівні тощо.

Поділяючи точку зору В.В. Копейчикова у визначенні терміну **«право»** як найбільш адаптованого до вимог, що пред'являються до визначень, пропонуємо вдосконалене його трактування як системи норм, які встановлені державою, мають офіційний формально-визначений характер, виражають права й обов'язки учасників правовідносин, направлені на регулювання найбільш важливих суспільних відносин, є загальнообов'язковими для всього населення та охороняються державою.

Поняття **власність** у визначеннях, як правило, характеризується як власність будь-якого виду; майно будь-якого типу; активи будь-якого роду; гроші та всі види рухомого чи нерухомого майна; суспільні відносини; суспільна форма привласнення матеріальних благ; будь-яке майно, будь-яка власність.

Виходячи з аналізу наведених вище понять ми робимо висновок, що **власність** – це будь-яка матеріальна чи нематеріальна субстанція, яка належить юридичній або фізичній особі.

При визначенні **інтелектуальної власності** використовують такі категорії та поняття, як розум, винахід, творчість, наукова й науково-технічна діяльність, мислення, розумова діяльність, нові знання, використання нових знань, здатність до мислення, раціонального пізнання, розумова діяльність, раціональне пізнання, духовність, здатність до мислення та розуміння, свідомість, виключні права, юридичний термін, продукт розумової праці, що охороняється законом, пошукова діяльність людини, результатом якої є щось якісно нове, цілеспрямована пошукова діяльність людини, наукове, нове досягнення, нове технічне вирішення завдання, результат науково-дослідної й (або) дослідно-конструкторської розробки, інтелектуальний продукт тощо.

Викладене дає підстави стверджувати, що термін «інтелектуальна власність» набагато складніший за «власність», хоча б тому, що описати таку

категорію, як розум, надто складно. Однак, головним у розумінні інтелектуальної діяльності є створення якісно нових знань і їх нормативно-правове закріплення.

Отже, **інтелектуальна власність** – це матеріалізовані або нематеріальні якісно нові знання, які належать юридичній чи фізичній особі.

Тепер зупинимося на **визначенні права власності** і визначимо його як систему правових норм, що закріплюють, охороняють та регулюють суспільні відносини з належності й використання нематеріальної чи матеріалізованої субстанції, яка належить фізичній або юридичній особі.

Тож **право інтелектуальної власності** - це система правових норм, що закріплюють, охороняють та регулюють суспільні відносини з належності й використання нематеріальних чи матеріалізованих якісно нових знань, що належать фізичній або юридичній особі.

Інтелектуальна творчість як процес (родове явище), а не конкретне науково-обґрунтоване визначення, **поділяється на такі види:** духовна (художня, літературна) творчість; наукова творчість; науково-технічна творчість; інша (нетрадиційна) творчість.

Виходячи з того, що будь-яке надбання людства, у тому числі й віднесене до творчого, має свого конкретного автора (суб'єкта творчого результату), породжується певне право автора на цей результат, тому воно завжди існує в усіх проявах (родах, видах, формах та ін.) творчості, з якої виникає право володіння ідеєю, її виконанням чи втіленням та використанням. Кожен вид інтелектуальної власності (до речі, як і форма) виражається її змістом і підрозділяється на конкретні об'єкти права інтелектуальної власності, що можуть створювати правовий інститут.

Структуру категорії **діяльність** описують її мета, завдання, об'єкт, предмет, суб'єкт, засоби, форми й методи діяльності та її результат.

Поняття охорона, захист та оборона співвідносяться лише як різні етапи, чи стадії забезпечення схоронності інформації з будь-якими грифами обмеження у доступі, починаючи від державної таємниці, закінчуючи медичною та адвокатською таємницями.

Викладене вище дає підстави зробити наступні висновки:

Інноваційна діяльність є підставою створення нового знання та інтелектуальних продуктів визнаних на державному, регіональному та світовому рівнях, на які у подальшому поширюється право власності.

Тобто, це формулювання вводить до науково-практичного обігу методіку утворення інновацій і закріплення їх нормами права:

- спочатку просто існує інформація як певна непізнана, чи пізнана характеристика матерії та енергії;
- в результаті специфічної розумової людської діяльності з пізнання інформації з'являються відомості;
- останні мають бути класифіковані і створювати інформаційні масиви;

- інноваційна діяльність з інформаційними масивами створює якісно нові знання;
- інформаційні масиви з якісно нових знань є ресурсами;
- інформаційні ресурси мають свою вартість і їх ціна повинна виражатися в грошовому еквіваленті;
- від цінності інформаційних ресурсів залежить система їх захисту;
- інформаційні ресурси повинні бути комерціалізованими;
- комерціалізації без власника практично приречена на невдачу;
- інформаційні ресурси при набутті власника стають об'єктами інтелектуальної власності;
- об'єкти інтелектуальної власності підлягають як неюрисдикційному захисту, так і юрисдикційному у повному обсязі.

Запропоноване сприятиме структурному формуванню платформи для вивчення навчально-наукового предмету «Право на інтелектуальну власність»: інформація – право на інформацію – створення якісно нового знання і його комерціалізація (інноваційна діяльність) – право на інтелектуальну власність (патент... тощо) – комерціалізація інтелектуальної власності – захист інтелектуальної власності.

*Голосніченко Д. І., д.ю.н., доцент,
професор ФСП КПП ім. Ігоря Сікорського,
Маслова Є. В., аспірант
ФСП КПП ім. Ігоря Сікорського*

ІНФОРМАЦІЯ ЯК ОБ'ЄКТ АДМІНІСТРАТИВНОГО ПРАВОПОРУШЕННЯ

Важливою складовою розвитку будь – якого суспільства є відкритість та прозорість державної влади, яка забезпечується шляхом надання та оприлюднення інформації. Поінформованість громадян є однією з найголовніших ознак розвитку та становлення демократичного суспільства. На конституційному рівні гарантовано і передбачено право кожного на доступ до інформації. А саме, стаття 34 Конституції України визначає, що кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [1].

Щодо визначення терміну «інформація», то він закріплений в Законі України «Про інформацію» № 2657 – XII від 02.10.1992 року. Даний Закон встановлює, що кожен має право на вільне одержання, використання, поширення,

зберігання та захист інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Під інформацією слід розуміти будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2].

Відповідно до статті 27 Закону України «Про інформацію» порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України [2].

З 06.05.2003 року компетентні органи та посадові особи за заявою фізичних та юридичних осіб мають право притягти посадових осіб, які порушують їх гарантоване право на інформацію, до адміністративної відповідальності.

Стосовно інформації як об'єкту адміністративної відповідальності, то відповідальність за порушення права в сфері інформації чітко закріплене в Кодексі України про адміністративні правопорушення, а саме в статті 212³ даного Кодексу.

Як нам відомо, що основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте життя [2], як наслідок підставами для притягнення посадових осіб до адміністративної відповідальності слід вважати:

- Неправомірну відмову в наданні інформації;*
- Несвоєчасне або неповне надання інформації;*
- Надання інформації, що не відповідає дійсності;*
- Обмеження доступу до інформації;*
- Неоприлюднення інформації [4].*

Під неправомірною відмовою в наданні інформації слід розуміти відмову, оформлену в письмовому вигляді із зазначенням прізвища, ім'я, по батькові та посаду особи (розпорядника інформації), мотивовану підставу відмови, порядок оскарження відмови, дата відмови та підпис. Якщо розпорядник інформації не володіє запитуваною інформацією, то він має надіслати даний запит іншому розпоряднику, повідомивши про це запитувача. У цьому разі строк розгляду запиту на інформацію починається з того дня, коли його отримує належний розпорядник [3].

Несвоєчасне або неповне надання інформації означає, що запит на інформацію був незадоволений протягом п'яти робочих днів, а якщо запит стосується великого обсягу інформації, то розпорядник може подовжити цей термін до двадцяти робочих днів. Якщо запит стосується життя чи свободи особи, стану довкілля, якості харчових продуктів, надзвичайних подій, що

сталися чи можуть статися, то розпорядник інформації має надати відповідь протягом 48 годин з дня отримання запиту [3].

Надання інформації, що не відповідає дійсності, мається на увазі будь – яке перекручування або надання неправдивої інформації.

Обмеження доступу до інформації. Слід зазначити, що в Законі України «Про доступ до публічної інформації» прописаний один з найважливіших міжнародних стандартів доступу до публічної інформації, відповідно до якого доступ можна обмежити до інформації, а не до документа. Тобто, якщо до документа застосовано гриф обмеження доступу, то він поширюється не на всю інформацію, яка в ньому міститься, а тільки на інформацію з обмеженим доступом. Та інформація, яка не обмежена в доступі й надається на запит та оприлюднюється [3].

Неоприлюднення інформації. Як нам відомо, однією з важливих властивостей інформації є її своєчасність та актуальність. Розпорядник інформації має систематично та оперативно оприлюднювати інформацію в офіційних друкованих виданнях, на офіційних веб – сайтах в мережі Інтернет, на єдиному державному веб – порталі відкритих даних, на інформаційних стендах, в будь – який інший спосіб. Стаття 15 Закону України «Про доступ до публічної інформації» чітко визначає, яку інформацію розпорядник має оприлюднювати. Якщо особа винна в неоприлюдненні інформації відповідно до статті 15 Закону України «Про доступ до публічної інформації», вона несе відповідальність за порушення законодавства про доступ до публічної інформації [3].

Підсумовуючи вищезазначене, слід зауважити, що інформація не може бути об'єктом речових прав, а отже держава отримуючи від народу чи створюючи нову інформацію не стає її власником. Держава має лише виконувати певні та надані їй законодавчими актами повноваження, а не розпоряджатись інформацією на власний розсуд, щоб зберегти та забезпечити гарантованість кожної особи на відкритість та доступність до інформації, що становить суспільний інтерес.

Список використаних джерел:

1. Конституція України [Електронний ресурс]: Закон України від 28.06.1996 № 254к/96-ВР // Верховна Рада України. - - URL: <http://zakon2.rada.gov.ua/Laws/show/254к/96-вр>.
2. Закон України «Про інформацію» [Електронний ресурс]: Закон України від 02.10.1992 № 2657 – XII // Верховна Рада України. - URL: <http://zakon.rada.gov.ua/laws/show/2657-12>.
3. Закон України «Про доступ до публічної інформації» [Електронний ресурс]: Закон України від від 13.01.2011 № 2939-VI // Верховна Рада України. – URL.: <http://zakon.rada.gov.ua/laws/show/2939-17>.
4. Кодекс України про адміністративні правопорушення [Електронний ресурс]: Закон України від 07.12.1984 року № 8074 – 10 // Відомості Верховної Ради Української РСР. - URL: <http://zakon.rada.gov.ua/laws/show/80731-10/ed20180927>.

ЗАСТОСУВАННЯ ПРИНЦИПУ «ЦИФРОВЕ ЗА ЗАМОВЧУВАННЯМ»: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

У переважній більшості зарубіжних країн спостерігається прискіплива увага до запровадження нових технологій й інструментів електронного урядування та електронної демократії. Вже не просто говорять про розвиток електронного урядування, а намагаються попереджати та уникати різноманітні перешкоди на цьому шляху. Саме цим пояснюється, що навіть в країнах, які є лідерами з розвитку електронного урядування, розробляються стратегії та напрацьовуються відповідні нормативно-правові акти, які мають прискорити процеси запровадження різноманітних технологій та інструментів електронного урядування, наблизити громадян до влади, а владу до громадян, зробити прозорим регулювання бізнесу і створити умови для їх гармонійного розвитку.

Тому, не випадково в Стратегії «Європа 2020» [1] ставилося за мету: «досягнення високого рівня зайнятості, продуктивності та соціальної згуртованості, що має бути втілено у конкретних діях на рівні ЄС та держав-членів». Серед семи головних напрямів (ініціатив), які були виокремлені для реалізації стратегії, саме в «Цифровому порядку денному для Європи» [2] акцентується увага на використанні ІКТ для досягнення амбітних цілей Стратегії «Європа 2020». Це стане можливим завдяки максимізації соціального і економічного потенціалу ІКТ, насамперед, мережі інтернет, як посередника в економічній і соціальній діяльності: для бізнесу, роботи та отримання електронних (цифрових) послуг.

В цьому контексті особлива увага приділяється сумісності, під якою розуміється здатність організацій (публічних адміністрацій або їх об'єднань) взаємодіяти задля досягнення спільних і узгоджених цілей, включаючи обмін інформацією та знаннями між цими організаціями, через бізнес-процеси, завдяки обміну даними між їх ІКТ системами [3].

У березні 2017 року була затверджена Європейська рамкова програма із забезпечення сумісності «European interoperability framework» (EIF) [3] - рекомендації стосовно взаємодії, обміну та співпраці між європейськими державними адміністраціями для надання європейських суспільних послуг через національні кордони та сектори. Також прийнято «План дій з сумісності» на період з 2017 по 2020 рр., в якому надаються конкретні вказівки щодо створення сумісних електронних (цифрових) публічних послуг. Передбачається, що реалізація цих дій сприятиме вирішенню проблем поліпшення якості послуг, більшого включення громадян в процеси прийняття управлінських рішень, спрощення різноманітних процедур для бізнесу, тощо. Крім того, це має призвести і до економії коштів, які витрачаються органами влади та місцевого

самоврядування для впровадження електронного урядування. Проте, потрібно підкреслити, що ІКТ – це лише засіб, а не мета для досягнення поставлених завдань в Стратегії «Європа 2020».

В Концепції розвитку електронного урядування в Україні, яка була затверджена в 2017 році, серед основних принципів, також, зазначається одноразове введення інформації та сумісність за замовчуванням. Під сумісністю розглядається: «необхідність здійснення проектування та функціонування інформаційно-телекомунікаційних систем в органах влади відповідно до єдиних відкритих вимог та стандартів для забезпечення їх подальшої сумісності та електронної взаємодії та повторного використання». [4]

Забезпечення сумісності є надзвичайно важливе, тому що без цього не можливо надавати якісні електронні послуги, налагодити електронну взаємодію, діалог між громадянами, владою та бізнесом. Проте, замість того, щоб дослідити найкращі зарубіжні практики, зокрема практику розробки програмного забезпечення з відкритим кодом і зробити його доступним для всіх зацікавлених сторін, як це запроваджується в Європейському Союзі, в Україні, принцип «сумісність за замовчуванням» починає перетворюватися на принцип «цифрове за замовчуванням». Так, в оприлюдненому проекті постанови Кабінету Міністрів України «Деякі питання цифрового розвитку» [5], на веб-сторінці Державного агентства з розвитку електронного урядування, зазначається, що принцип «цифровий за замовчуванням» означає переведення у цифровий формат тих аналогових систем, розвиток та підтримка яких є очевидно не вигідна та неефективна. Тобто, цифровий стан стає звичайним станом функціонування та розвитку багатьох систем, сфер, організацій, індустрій та економік. Тому запропоновано «використовувати критерії цифрової реалізації під час підготування нових або внесення змін до чинних законодавчих актів і реалізації владних повноважень органами державної влади та органами місцевого самоврядування, а також запровадження в органах державної влади й органах місцевого самоврядування цифрової експертизи проектів нормативно-правових актів та організаційно-розпорядчих документів, висновок про проведення якої визначається обов'язковим додатком до проекту відповідного акту» [5]. Цей Проект Постанови розроблений на виконання п. 6 Плану заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр., затвердженого розпорядженням КМУ від 17 січня 2018 р. № 67-р. [6].

При детальному ознайомленні з цими документами, можна зробити висновок, що хоча розробники й брали за основу «Цифровий порядок денний для Європи» (Digital Agenda for Europe), «Єдиний цифровий простір» (Digital Single Market), Програми Європейського Союзу щодо рішень сумісності європейських публічних адміністрацій (Interoperability Solutions for European Public Administrations 2), проекти e-CODEX, e-Invoicing, а також ініціативи Single Digital Gateway, спостерігається ігнорування особливостей сучасного розвитку України, а саме її внутрішньої і зовнішньої вразливості в умовах мережевої війни. Хоча у

Пояснювальній записці до цього проекту, відзначається, що розробники керувались такими вимогами, як : «працювати з людьми й іншими органами під час розроблення електронних послуг; користуватися можливостями нових цифрових технологій та готувати людей до змін, які ці технології несуть нашому суспільству й економіці; забезпечувати кращий доступ до даних, одночасно гарантуючи захист конфіденційної та іншої чутливої інформації; підтримувати людей, які не мають доступу до цифрового світу; інвестувати бюджетні кошти розумно». Залишається відкритим питанням, яким чином можна запобігти, під час форс-мажорних обставин (військові дії, зникнення електропостачання, стихійні явища, тощо), припиненню он-лайн доступу до публічної інформації, наданню якісних електронних послуг, використанню інструментів електронної демократії? Чому перебуває поза увагою, необхідність забезпечення гарантованого отримання життєве необхідних послуг, не зважаючи на зовнішні обставини?

Список використаних джерел:

1. COM (2010) 2020 final Communication from the Commission: EUROPE 2020 A strategy for smart, sustainable and inclusive growth, Brussels, 3.3.2010. - URL: <http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf>
2. Цифровий порядок денний для Європи. URL: <file:///C:/Users/sofis/Downloads/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D0%BA%20%D0%B4%D0%B5%D0%BD%D0%BD%D0%B8%D0%B9%20%D0%B4%D0%BB%D1%8F%20%D0%84%D0%B2%D1%80%D0%BE%D0%BF%D0%B8.pdf>
3. COM (2017) 134 final ANNEX 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Region: European Interoperability Framework — Implementation Strategy, Brussels, 23.3.2017. URL:http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF
4. Концепція електронного урядування в Україні від 20.09.2017.URL: <http://zakon.rada.gov.ua/laws/show/649-2017-%D1%80>
5. Проект постанови Кабінету Міністрів України «Деякі питання цифрового розвитку».URL: <https://www.e.gov.ua/content/proekt-postanovy-kabinetu-ministriv-ukrayiny-deyaki-pytannya-cyrovogo-rozvytku>
6. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки.URL:<http://zakon.rada.gov.ua/laws/show/67-2018-%D1%80>

ОСВІТНЬО-ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДИТИНИ В УКРАЇНІ

Підвищення ролі інформації у житті сучасного суспільства, активний розвиток інформаційних і комунікаційних технологій та їх активне використання призводять до збільшення загроз для дитини в інформаційній сфері.

Рівень інформаційних загроз для дитини підвищується відповідно до ступеня її залучення до інформаційних та комунікаційних процесів. Організація охорони здоров'я Великобританії (PHE) визнала, що нині діти і підлітки піддаються психологічному тиску в мережі Інтернет сильніше, ніж коли-небудь раніше (кожен 5 молодий британець був жертвою інформаційно-психологічного переслідування).

Відповідно до статистичних даних Національної поліції України за 2016 рік третина злочинів (32 %), скоєних з використанням соціальних мереж, пов'язані з ввезенням, виготовленням, збутом і розповсюдженням порнографічних предметів, тобто правопорушень, передбачених статтею 301 КК України. 59 % із них – це примушування неповнолітніх до участі у створенні творів, зображень, кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру. Тобто, рівень небезпеки для дитини в сучасному інформаційному суспільстві є вищим ніж для дорослого.

Особливу небезпеку нині становлять спеціальні інформаційно-психологічні операції проти держави, об'єктом яких є свідомість дитини. Прикладом подібних дій є створення та популяризація різних груп серед молоді, у тому числі «групи смерті», у соціальних мережах. На кінець 2017 року кіберполіцією України було заблоковано більше 1000 «груп смерті» у соціальних мережах. Станом на квітень 2017 року відкрито 35 кримінальних проваджень і встановлено 4 факти самогубства, попереджено 10 спроб покінчити життя самогубством.

Забезпечення інформаційної безпеки дитини слід розглядати, виходячи із факторів ризику, які відрізняють її від інших суб'єктів інформаційних відносин, зокрема:

- психофізичні особливості вікового онтогенезу;
- соціального статусу дитини та її основної суспільної функції;
- невизначеність правового статусу дитини в інформаційній сфері;
- спрямованість спеціальних інформаційних операцій на дитину в інформаційному протиборстві.

Психофізичні вікові особливості сприйняття інформації дитячою свідомістю, слабо розвинені когнітивні та аналітичні здібності дитини за відсутності вибіркової у споживанні нею інформаційного продукту, а також безвідповідальне ставлення до захисту персональних даних призводять до

підвищення безпеки від реалізації загроз в інформаційній сфері. Тому для дитини, як суб'єкта інформаційних відносин необхідно передбачити низку особливих попереджувальних заходів і механізмів захисту, які передували би виникненню інформаційної безпеки. Особливе місце у превенції інформаційних загроз слід відвести системі освітньо-правових заходів з метою підвищення інформаційної грамотності та культури дитини.

Соціальний статус дитини, як об'єкта соціалізуючого виховного впливу, передбачає використання щодо неї позитивного інформаційно-психологічного соціального впливу інститутів соціалізації, зокрема, навчальних і виховних закладів, батьків. Сучасний навчально-виховний процес створює підвищене інформаційне навантаження на свідомість дитини. Перенасичення інформаційного простору знижує внутрішній інформаційний спротив і підвищує рівень виникнення безпеки для дитини в інформаційній сфері, на що вказують дослідження у сфері психології та інформаційно-психологічної безпеки [1; 2; 3]. Тому, забезпечуючи навчально-виховний процес, слід ретельно дотримуватись принципу обмеження доступу дитини до шкідливої інформації та недопущення дії негативного інформаційно-психологічного впливу на її свідомість при одночасній реалізації природнього права дитини на доступ до інформації, необхідної для навчання і розвитку, що гарантує національне законодавство та норми міжнародного права.

Тобто, інформаційну безпеку дитини потрібно розглядати з трьох позицій:

1. законодавчо закріпленого суб'єктивного права дитини на інформацію, яка відповідає її духовному та інтелектуальному розвитку, сприяє її індивідуальному та суспільному становленню;
2. права на захист від інформації, яка може завдати шкоди морально-психологічному здоров'ю дитини чи завадити її повноцінному та гармонійному розвитку;
3. права на охорону та захист персональних даних дитини і непоширення інформації про неї.

Особливим фактором ризику, що значно впливає на стан інформаційної безпеки дитини є спеціальні інформаційно-психологічні операції проти держави, об'єктом яких є свідомість дитини. Метою таких операцій є не лише нанесення шкоди життю та здоров'ю дитини, але й поширення певних патернів серед молодіжної аудиторії, нав'язування визначених поглядів та маніпулювання свідомістю з метою запровадження у суспільстві керованого хаосу. Важливим елементом у системі протидії таким інформаційним загрозам поряд з політико-правовим та охоронними заходами повинна стати інформаційно-освітня складова загальної системи забезпечення.

Аналіз міжнародного досвіду у питаннях забезпечення інформаційної безпеки дитини свідчить про підвищення ролі навчально-освітніх програм у системі захисту від інформаційних загроз. Наприклад, організацією охорони здоров'я Великобританії (PHE) разом із Міністерством освіти країни розроблена

учбова програма для дітей 11-16 років, яка навчає їх протидіяти переслідуванню у соціальних мережах та адекватно реагувати на прояви агресії в Інтернеті. Подібна програма діє у США, запущена приватною компанією Nearpod, що спеціалізується на запровадженні мобільних технологій в учбовий процес.

В Австралії з 4-х років навчатимуть дітей основам кібербезпеки. Основна мета – попередження появи жертв сексуальних інтернет-злочинців серед дітей.

У школах Ізраїлю введено предмет «Кібербезпека» через занепокоєння медиків та батьків стосовно кіберзалежності дітей. Уроки складаються з теоретичної та практичної частин, на яких школярів вчать як поводитись у соціальних мережах, як правильно спілкуватись. Окремим важливим питанням у вказаному курсі є боротьба із залежністю від комп'ютерних ігор та Інтернет-залежністю. Розроблено відповідні освітні методики для їх подолання.

Розглядаючи правовий статус дитини в інформаційній сфері, було виявлено правову колізію. З одного боку, дитина є особливим суб'єктом суспільних відносин відповідно до положень національного та міжнародного права (*Конституції України, Конвенції ООН про права дитини*) [4; 5]. Дитина потребує особливого захисту та піклування з боку держави та основних її інститутів, на які покладено функції по забезпеченню найкращих інтересів, направлених на задоволення 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»*) [6]. Реалізація природнього права дитини на захист в інформаційній сфері покладається на батьків або осіб, що їх замінюють, і державу та відповідні її інститути, на які, згідно із законодавством України, покладено функції щодо охорони дитини (*ст. 12 Закону України «Про охорону дитинства», ст. 14, 152 Сімейного кодексу України*) [6; 7].

Однак, Закон України «Про основи національної безпеки України» [8] не поділяє об'єкти захисту від небезпек, у тому числі і в інформаційній сфері, за віком та відносить дитину до загальних об'єктів захисту.

Зважаючи на підвищення рівня загроз інформаційній безпеці та особливості дитини як суб'єкта інформаційних відносин, доцільним є перегляд її правового статусу та визначення дитини як особливого суб'єкта інформаційних відносин аналогічно до визнання її особливим суб'єктом суспільних відносин.

Підсумовуючи вище наведене слід відзначити, що навчально-освітня складова у системі забезпечення інформаційної безпеки дитини є важливим компонентом і потребує подальшого розвитку. Підвищення рівня інформаційної грамотності та інформаційної культури у суспільстві дозволить збільшити обізнаність дитини щодо загроз в інформаційній сфері, навчить її безпечно поводитись в мережі Інтернет та мережесі спілнотах, а також створювати навколо себе безпечний інформаційний простір.

Для удосконалення правових засад забезпечення інформаційної безпеки дитини в Україні, серед іншого, доцільним є:

- розроблення та запровадження Концепції інформаційної безпеки дитини в Україні;

- розроблення Державної соціальної програми «Національний план дій щодо реалізації Конвенції ООН про права дитини» на період до 2021 року з врахуванням питань подолання цифрової та когнітивної нерівності серед дітей і підвищення їх інформаційної грамотності та культури в контексті пріоритетів Стратегії Ради Європи з прав дитини (2016 – 2021);

- оновлення ряду нормативно-правових актів у сфері освіти, зокрема Положення про кабінет інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів, затверджене Постановою Кабінету Міністрів України від 20.05.2004 № 407 та в рамках пріоритетів, визначених Законом України «Про освіту»;

Успішність реалізації системи заходів по забезпеченню інформаційної безпеки дитини у освітньо-правовому аспекті, на наш погляд, залежить від:

- 1) створення максимально безпечного інформаційного простору для навчання з мінімізацією ризиків в процесі самореалізації дитини;

- 2) поступового зменшення заборон для дитини в інформаційному просторі по мірі її дорослішання;

- 3) коригування мотиваційної сфери дитини з урахуванням її інформаційної безпеки методом м'якої виховної дії, переорієнтація її бажань у більш безпечних напрямках через ознайомлення з небезпеками в інформаційному просторі, наслідками, до яких призводять ці небезпеки, та способами їх уникнення чи протидії.

Список використаних джерел:

1. Петрунько О. В. Діти і медіа: соціалізація в агресивному медіа середовищі: монографія. 2-ге вид. Ніжин: ТОВ «Видавництво «Аспект-Поліграф», 2011. 480 с.

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

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

4. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. // База даних Законодавство України / ВР України. - URL: <http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

5. Конвенція про права дитини: Конвенція ООН від 20.11.1989. // База даних Законодавство України / ВР України. - URL: http://zakon3.rada.gov.ua/laws/show/995_021

6. Про охорону дитинства: Закон України від 26.04.2001 № 2402-III. // База даних Законодавство України / ВР України. - URL: <http://zakon5.rada.gov.ua/laws/show/2402-14>

7. Сімейний кодекс України: Закон України від 10.01.2002 № 2947-III. // База даних Законодавство України / ВР України. - URL: <http://zakon3.rada.gov.ua/laws/show/2947-14>

8. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-IV. // База даних Законодавство України / ВР України. - URL: <http://zakon2.rada.gov.ua/laws/show/964-15>

*Соснін О. В., д.п.н., професор,
заслужений діяч науки і техніки України,
Інститут держави і права
ім. В. М. Корецького НАУ України,
Гордієнко С. Г., д.ю.н., доцент
ФСП КПП ім. Ігоря Сікорського*

РОЛЬ ЮРИДИЧНОЇ НАУКИ В ПРОЦЕСІ ВИХОВАННЯ ІНЖЕНЕРНО-ТЕХНІЧНИХ КАДРІВ

Глобалізація, що подібно до цунамі накриває нас, та яка її творцями (ідеологами і провідниками) взагалі вбачалася як багаторівнева система, верхній шар якої являє собою мережу компактних територій мегаполісів, транспортних і фінансових центрів, центрів освіти, науки, комунікаційних вузлів, об'єднаних новітніми інформаційно-комунікаційними технологіями (ІКТ), які розподіляють інформаційні і матеріальні потоки, фокусуючи політичний і економічний вплив провідних країн на регіони світу.

Саме тому предметність глобального інформаційно-комунікативного простору і ролі національних центрів розподілу і зберігання інформаційних ресурсів дедалі більше стає предметом спеціальних наукових досліджень. Огляд робіт, присвячених цій темі, дозволяє бачити закономірності, відмінності і суттєві особливості процесів, пов'язаних з природою процесів, які відбуваються у вітчизняному інформаційно-комунікативному просторі.

Сам феномен комунікації трактується по-різному, однак, головним чином, як «широкосмугова» соціально-культурна взаємодія. У практичному плані глобальний інформаційно-комунікативний простір віддзеркалюється в диспозиціях різних каналів сучасної комунікації, технічних засобах генерування і поширення інформаційних повідомлень.

Комунікація, безумовно, є констатуюючим процесом, оскільки є засобом людського існування, а в сучасному світі навіть основним соціальним процесом, в якому людина взаємодіє з іншими людьми, створюючи соціальні реальні і віртуальні світи і простори. Огляду засобів комунікації, як феномену інформаційно-змістовної взаємодії, теж присвячено сьогодні багато досліджень. Переважно, увага звертається на соціальну природу комунікації. Це пов'язано із розширенням концептуальних і предметних меж розгляду цього феномена.

Сьогодні, в умовах, коли світове співтовариство переживає справжню інформаційно-комунікаційну революцію, яку генерують комп'ютер і новітні ІКТ,

в суспільстві з'являються нові соціально-економічні й культурні структури, фактично виникає новий світ, який Г. М. Маклюен назвав «новою галактикою». В історії людства він виділяв чотири такі галактики-епохи:

1. Епоха дописемного варварства².
2. Епоха фонетичного письма³.
3. Друкарства епоха Гутенберга⁴.
4. Епоха Марконі⁵.

Останню епоху порівнюють з такими подіями в житті людства, як винахід нових знарядь праці і методів використання енергії пари та електрики у виробничих процесах. Взагалі, поява кожного принципово нового засобу комунікації завжди приводила до інформаційно-комунікаційних «вибухів» і змін в пануючих конфігураціях комунікацій. Ідеологами підходу про вирішальну роль у культурі сучасних комунікаційних технологій, ще в середині ХХ століття виступили Г. А. Інніс⁶ і Г. М. Маклюен⁷. Вони вважали, що домінуючі засоби комунікації визначають своєрідний, відмінний від інших, вигляд культури, задають певний спосіб кодування й декодування реальності й активізують діяльність тих або інших органів влади і почуття людини.

Процеси, які пов'язано з інформатизацією і інфраструктурними проектами, сьогодні стають ареною зухвалих і непримиренних «баталій», між компаніями і державами за вплив на всі або окремі сфери та регіони. Все частіше суспільна свідомість потрапляє в націлені на результат та вміло інтегровані глобальні мережі. Ситуація вимагає терміново змінювати систему підготовки інженерно-технічних кадрів, юристів, лікарів і всіх інших спеціалістів, підпорядкувати її ідеям формування в них засад нової інформаційно-комунікаційної культури на засадах інноваційної. Взагалі інформаційно-комунікаційна парадигма сучасності напряму пов'язана із процесами глобалізації і широкої майже тотальної інформатизації суспільства. Вона стрімко і бурхливо вибудовується на тлі пізнання реального світу, надаючи йому низку нових якостей, рис, тенденцій, які активізують і мотивують необхідність процесів філософського осмислення

² Епоха дописемного варварства, щасливий період єдності слова й справи, коли зберігався безпосередній контакт із природою й з одноплемінниками. У цей період панує «оральна» – усна комунікація, у сенсорному балансі лідирує слух.

³ ФОНЕТИЧНЕ ПИСЬМО — ВИД ПИСЬМА В ЯКОМУ ГРАФІЧНИЙ ЗНАК (ГРАФЕМА) ПРИВ'ЯЗАНИЙ ДО ПЕВНОГО ЗВУЧАННЯ.

⁴Йоганн Генсфляйш цур Ляден цум Гутенберг (нім.*Johannes Gensfleisch zur Laden zum Gutenberg*; *1397–1400, Майнц, Німеччина — 3 лютого 1468) — німецький ювелір і винахідник. Прецизійний механік шляхетного роду. У середині 1440-х років створив європейський спосіб друкарства рухливими літерами, що поширився усім світом та зробив величезний вплив не лише на європейську культуру, але і на всесвітню історію.

⁵ Гульєльмо Марконі (ІТАЛ.*GUGLIELMO MARCONI*; 25 квітня 1874 — 19 липня 1937) — ІТАЛІЙСЬКИЙ ВЧЕНИЙ І ВИНАХІДНИК («БАТЬКО РАДІО»); НОБЕЛІВСЬКИЙ ЛАУРЕАТ У ГАЛУЗІ ФІЗИКИ (1909) ЗА РОБОТИ З БЕЗДРОВОЇ ТЕЛЕГРАФІЇ.

⁶ Гарольд Адамс Інніс (АНГЛ.*HAROLD ADAMS INNIS*, 5 листопада 1894, Гампльтон — 8 листопада 1952, Торонто) — КАНАДСЬКИЙ ЕКОНОМІСТ І СОЦІОЛОГ, «БАТЬКО КАНАДСЬКОЇ ЕКОНОМІЧНОЇ ТЕОРІЇ», ДОСЛІДНИК КУЛЬТУРИ І МАСОВИХ КОМУНІКАЦІЙ.

⁷ ГЕРБЕРТ МАРШАЛЛ МАКЛЮЕН (АНГЛ.*HERBERT MARSHALL MCLUHAN*, 21 липня 1911 — 31 грудня 1980) — КАНАДСЬКИЙ ФІЛОСОФ, ФІЛОЛОГ, ЛІТЕРАТУРНИЙ КРИТИК, ДОСЛІДНИК ВПЛИВУ МЕДІА, ЯК ЗАСОБІВ КОМУНІКАЦІЇ НА АУДИТОРІЮ.

ситуації. Зрозуміти сенс і місце інформації в якості резерву розвитку суспільства стає завданням рівня проблеми національної безпеки.

За таких умов найважливішою проблемою сучасної вищої освіти стає вивчення понять і ціннісноговиміру змістовної інформації.⁸ Вирішення проблеми має два головних виміри: перший – це орієнтація на нову соціально-політичну і економічну кон'юнктуру, яка пов'язана, скажімо, з необхідністю підготовки фахівців за новими спеціальностями; другий – це вимоги до орієнтації процесу навчання і виховання на наявні духовні національні традиції, скажімо, на вміння працювати в колективі. Все це сходить до джерел вітчизняної гуманістичної педагогіки і організації вищої освіти і сьогодні вона повинна стати центром інтелектуального й духовного відтворення (так званий культуро-центризм) української держави.

На тлі нових викликів особливо розуміння вимагає необхідність організації вивчення політико-правових дисциплін захисту інформації, зокрема, інтелектуальної власності. Вивчення методів формування нових диференційованих регулятивних механізмів в праві – від самоцензури до визначення правил модерування текстів і способів самовираження стає турботою технічних університетів. Все це супроводжується вибудовою складних інтелектуальних моделей поведінки в інформаційно-комунікаційному просторі навіть при оцінці етичності передачі тих або інших повідомлень (інформації) при виконанні державою інформаційно-комунікаційної функції. Її організація і методи виконання набувають особливої ваги, оскільки основною характеристикою глобалізації можна вважати те, що вона із принципово новими доленосними наслідками вводить наше мислення дедалі глибше у віртуальні процеси інженерної правової, наукової, освітньої, а, головне, інноваційної діяльності людства в будь-якій сфері. Саме вона, головним чином, підвищуючи роль інформаційного обміну на глобальному рівні, вирішує питання рівності громадян і стимулює процеси захисту інтелектуальної власності і інформації взагалі.

Постійно продукуючи інноваційні промислові і управлінські інформаційно-комунікаційні технології, глобалізація підвищує не тільки значення науково-промислових центрів і технічних університетів. За таких умов при плануванні навчально-виховного процесу в технічному університеті пропонується виходити з наступних тез:

- спочатку просто існує наукова інформація, яка описує певну характеристику матерії й енергії;
- в результаті специфічної розумової інженерно-технічної діяльності з'являються технології її використання;
- останні мають бути класифіковані і створювати певні інформаційні масиви, які використовуються інженерно-технічними фахівцями в інноваційній

⁸ СОСНІН О.В. ПРОБЛЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ НАЦІОНАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ З НАУКОВОГО ПОТЕНЦІАЛУ УКРАЇНИ: МОНОГРАФІЯ / О.В. СОСНІН – К.: ІНСТИТУТ ДЕРЖАВИ І ПРАВА ІМ. В.М. КОРЕЦЬКОГО НАН УКРАЇНИ, 2003. – 572 с.

діяльності, створюючи якісно нові знання та технології, які стають інформаційним ресурсом розвитку країни;

- інформаційні ресурси мають свою вартість і їх ціна завжди має грошовий еквівалент;
- від цінності інформаційних ресурсів залежить система їх захисту.

Важливою функцією сучасної вищої школи є інвентаризація та комерціалізація існуючих інформаційних ресурсів.

Запропоновані напрями діяльності вищої школи повинні структурно формувати платформу для вивчення нових навчально-наукових предметів, які дозволяють реалізацію права на інтелектуальну власність. Його основою є вивчення (оволодіння) знань про інформацію – право на інформацію – про процеси створення якісно нових знань і їх комерціалізацію (інноваційна діяльність) – про право на інтелектуальну власність і її захист.

Тобто, наукова та навчальна частини дисциплін, які мають вивчати сьогодні студенти технічних університетів має складатися з:

1. Інформаційного блоку:

Наука – Інформаціологія.

Навчальна дисципліна – Інформаційне право.

2. Інноваційного блоку:

Наука – Інноватика (галузь знань, що включає методологію й організацію інноваційної діяльності).

Навчальна дисципліна – Інноваційна діяльність – Право інноваційної діяльності.

3. Блоку інтелектуальної власності:

Наука – Інтелектуальна власність.

Навчальна дисципліна – Право на інтелектуальну власність.

Зазначені блоки є основою формування знань, умінь та навичок за рівнем пізнання у бакалаврів, магістрів та докторів філософії.

Відзначимо, що освітні стандарти і «втомленість» або невідповідність вимогам часу викладачів утворюють так звану раціональнускладову інформаційно-комунікативного просторуучбового закладу (аксіосферу), що стає просто сукупністю ідей, образів і символів, що означають зміст/сене, мету, критерії оцінного відношення людини як до світу речей і явищ, так і віртуальної реальності. Культурна парадигма часто характеризується відсутністю глибини та мутацією фундаментальних поглядів на предметний реальний світ. Дедалі частіше він, на жаль, стає набором текстів або симуляцією активної діяльності. Ірраціональне в цьому транслюється повсякденністю, повсякденним досвідом, засобами масової комунікації (ЗМК) і засобами масової інформації (ЗМІ), насамперед, – телебаченням і глобальними інформаційно-комунікаційними мережами, а вони багато в чому і визначають аксіосферу закладів вищої освіти.

*Доронін І. М., к.ю.н., доцент
завідувач лабораторії НДШІП
НАПрН України*

КООРДИНАЦІЯ У СФЕРАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ: ІНФОРМАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Значне оновлення чинного вітчизняного законодавства, що відбулось за останній рік, зумовило і уточнення підходів до предмету та меж правового регулювання суспільних відносин у сфері національної безпеки та оборони. У першу чергу мова йде про правові новели, що встановлені Законом України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. Встановлена цим законодавчим актом зміна підходів у розумінні суті національної безпеки від широкого (та найширшого), що були визначені Законом України «Про основи національної безпеки України» від 19.06.2003 в різних редакціях, до більш вузького стосується і компетенції державних органів у сфері національної безпеки і оборони.

Конституційною основою для Закону України «Про національну безпеку України» є прямі приписи статей 1, 2, 17, 18 і 92 Основного Закону, а метою (що впливає з преамбули):

- визначення та розмежування повноважень державних органів у сферах національної безпеки і оборони;
- створення основи для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони;
- визначення системи командування, контролю та координації операцій сил безпеки і сил оборони,
- запровадження всеосяжного підходу до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони.

Отже, преамбулою Закону визначено як мету правового регулювання встановлення, визначення та розмежування повноважень певних органів держави.

Суб'єктний склад сектору безпеки і оборони регламентовано ч. 2 ст. 12 Закону і до нього входять: «Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління

державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику».

По суті, суб'єктний склад, що визначено зазначеним законодавчим актом, є традиційним для державної політики у сфері забезпечення національної безпеки і оборони. Водночас, Законом серед суб'єктів сектору безпеки і оборони вперше самостійно визначено Апарат Ради національної безпеки і оборони України.

Питання координації у сферах національної безпеки і оборони регламентовано ст. 14 Закону України «Про національну безпеку України» і єдиним суб'єктом здійснення координації є Рада національної безпеки і оборони України, особливий «координуючий» статус якої випливає із приписів статті 107 Конституції України. Водночас, її Апарат згідно з п. 1 Положення про Апарат Ради національної безпеки і оборони України, затвердженого Указом Президента України від 14.10.2005 № 1446, є державним органом, що здійснює поточне інформаційно-аналітичне та організаційне забезпечення діяльності Ради національної безпеки і оборони України. В науковій літературі пропонується розглядати систему РНБО як єдине явище, до складу якої входить Апарат РНБО, як її невід'ємна частина [1, с. 92]. Водночас, фактичний правовий статус Апарату РНБО є явно допоміжним, що зумовлює низку правових проблем характерних для всіх так званих «допоміжних органів» при Президентові України [2, с. 17-18]. Зазначений аспект проблеми нібито є суто організаційним, проте не слід забувати і про визначення суті координації в її правовому розумінні.

Взагалі в теорії управління сутність координації розуміється як процес узгодження (налагодження залежностей) від різних форм активності [3]. У державному управлінні координацію зазвичай розглядають на протигагу субординації, як діяльність «рівних» суб'єктів. Методологічно в адміністративному праві в основі координації розглядається «необхідність узгодження управлінських дій між кількома органами одного структурного рівня для досягнення загальної мети» [4, с.188]. За деяких умов координація застосовується із використанням форм притаманних субординації на що зверталась увага в літературі [5, с. 261; 6].

Законодавчо питання забезпечення координації у сферах національної безпеки і оборони на сьогодні врегульовані вкрай схематично. Зокрема, ст. 14 Закону України «Про національну безпеку України» встановлено, що «в умовах воєнного або надзвичайного стану, в особливий період, а також у разі виникнення кризових ситуацій, що загрожують національній безпеці України, Рада національної безпеки і оборони України координує діяльність органів виконавчої влади, розглядає пропозиції щодо застосування відповідно до закону спеціальних економічних та інших обмежувальних заходів». У даному випадку сутність повноважень з «координації» законодавчо не визначено, хоча реалізація повноважень Ради і пов'язана із її компетенцією щодо застосування санкцій

(спеціальних економічних та інших обмежувальних заходів). Таким чином, належна правова регламентація компетенції та порядку здійснення координації у сфері національної безпеки є завданням перспективного законодавства. Що стосується сфери оборони, то координуючі повноваження визначені Законом України «Про національну безпеку» і в мирний час покладені на РНБО. Водночас, відповідно до ч. 3 ст. 14 Закону «у випадках, передбачених законом, Рада національної безпеки і оборони України подає на розгляд Президентові України пропозиції щодо утворення вищого колегіального стратегічного органу воєнного керівництва обороною держави в особливий період. Пропозиції про утворення цього органу та його персональний склад затверджуються рішенням Ради національної безпеки і оборони України та вводяться в дію Указом Президента України. Положення про вищий колегіальний стратегічний орган воєнного керівництва обороною держави в особливий період затверджує Президент України».

На сьогоднішній день, в умовах «гібридної війни» та особливостей її інформаційної складової, питання належної координації у сфері національної безпеки стосовно забезпечення інформаційної безпеки набувають особливої ваги, що зумовлено специфічністю загроз у цій сфері. Певне реагування відбулось, у першу чергу, в сфері кібербезпеки, враховуючи підвищену небезпечність таких загроз, що детально аналізувалось у науковій літературі останнього часу [7-9]. Засобом такого реагування є створення координуючих органів – Національного координативного центру кібербезпеки як робочого органу РНБО України відповідно до Указу Президента України від 07.06.2016 № 242. Водночас, у питанні забезпечення інформаційної безпеки та забезпечення національної безпеки в інформаційній сфері координація перебуває на початковому етапі, що зумовлено низкою проблем організаційного та правового характеру.

Таким чином, на нашу думку, координація у сферах національної безпеки і оборони, правова регламентація якої започаткована законодавчо останнім часом, потребує подальшого організаційно-правового вдосконалення.

Список використаних джерел:

1. Цоклан В.І. Структура Ради національної безпеки і оборони України як важливий елемент її конституційно-правового статусу/ В. І. Цоклан// Часопис Київського університету права. - 2011. - № 2. - С. 90-92;
2. Коваль Н.В., Пухтинський М.О. Забезпечення впорядкування допоміжних структур при Президентові України на законодавчому рівні// Н.В.Коваль, М.О.Пухтинський// Вісник НАДУ при Президентові України (Серія «Державне управління»).- 2017.- № 4. – С. 10-19;
3. Kral J. Introduction to Coordination Concept/ J.Kral// Human Resources Management and Ergonomics. 2007. Vol.2.- URL: https://frcatel.fri.uniza.sk/hrme/files/2007/2007_2_06.pdf
4. Криволапчук В.О. Сучасний погляд на методи адміністративного права/ В. О. Криволапчук// Науковий вісник Львівського державного університету внутрішніх справ.- 2014. - № 4. – С. 184-192;

5. Иващук А.В. Координация правоохранительной деятельности как научная категория/ А. В. Иващук// Вестник Нижегородской академии МВД России. – 2015. - № 1. – С. 259-261;

6. Фрідман-Козаченко М.М., Рафальський В.П. Роль прокуратури в координації взаємодії правоохоронних органів України щодо виявлення кримінальних правопорушень/М. М. Фрідман-Козаченко, В. П. Рафальський// Міжнародний юридичний вісник. - 2016.- Вип. 1(3). – С. 79-84;

7. Петров В.В. Щодо формування національної системи кібербезпеки України/В.Петров//Стратегічні пріоритети. – 2013. - № 4(29) – С. 127-130;

8. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції/Р.Лук'янчук//Вісник НАДУ – 2015. - № 3. – С. 110-116

9. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту. Монографія.- К.: АртЕК, 2017. – 107 с.

*Огороднік Ж. А., к.ю.н.,
ФСП КПП ім. Ігоря Сікорського*

КОНФІДЕНЦІЙНІСТЬ КОРПОРАТИВНОГО ДОГОВОРУ

У статті 7 нещодавно прийнятого Закону України «Про товариства з обмеженою та додатковою відповідальністю» (надалі – Закон), який набув чинності 17.06.2018 р.[1], визначено, що договір, за яким учасники товариства зобов'язуються реалізовувати свої права та повноваження певним чином або утримуватися від їх реалізації (далі – корпоративний договір), є безвідплатним і вчиняється в письмовій формі. Корпоративний договір, який не відповідає цим вимогам, є нікчемним. Поява «корпоративного договору» є новелою в законодавстві України і відповідно потребує часу для його практичного втілення.

Корпоративний договір укладається учасниками товариства, тобто він може бути укладений після реєстрації товариства або до реєстрації товариства з визначенням того, що датою набуття чинності цього договору є дата реєстрації товариства. Також корпоративний договір може бути укладений учасниками товариств, які були створені до набуття чинності Закону. Строк дії корпоративного договору визначається сторонами в договорі. Відповідно строк є істотною умовою корпоративного договору, і цей строк може залежати від настання тих цілей, які учасники мали на меті досягнути при укладенні договору або може бути встановлений на весь строк існування сторін договору як учасників товариства.

Водночас, укладення корпоративного договору не є обов'язковим, це є правом, а не обов'язком учасників товариства. Відносно змісту корпоративного договору законодавець не дає детального визначення, обмежуючись загальним «за яким учасники товариства зобов'язуються реалізовувати свої права та повноваження певним чином або утримуватися від їх реалізації». А також в п.п.3,

4 ст.7 Закону зазначається, що корпоративний договір може передбачати умови або порядок визначення умов, на яких учасник має право або зобов'язаний купити або продати частку у статутному капіталі (її частину), а також визначати випадки, коли таке право або обов'язок виникає. Корпоративний договір, яким встановлюється обов'язок учасників забезпечити голосування згідно з вказівками органів управління товариства, є нікчемним.

З огляду на вищезазначене, учасники товариства можуть врегулювати в корпоративному договорі будь-які питання своїх прав та повноважень в товаристві, водночас, ці положення договору не повинні суперечити Закону та Статуту товариства.

П.п.3, 4 ст.7 Закону встановлює, що зміст корпоративного договору не підлягає розкриттю і є конфіденційним, якщо інше не встановлено законом або договором.

Згідно загальновідомого визначення конфіденційність (англ. *confidentiality*) - властивість, яка не підлягає розголосі; довірливість, секретність, суто приватність [2]. Виникає питання, чому законодавець встановив, що корпоративний договір, за загальним правилом, є конфіденційним? На мій погляд, така позиція зумовлена тим, що відносини, які можуть бути врегульовані корпоративним договором між учасниками товариства, носять суто приватний характер, і такий договір має на меті врегулювати відносини між учасниками, щоб запобігти непорозумінню, неузгодженостей між учасниками, водночас, вирішити і спірні ситуації. Наприклад, встановлення порядку відчуження часток учасників у статутному капіталі, регламентування детальної процедури такого відчуження. Також має можливість встановити, як саме будуть вирішуватись спірні питання: можливі переговори, застосування процедури медіації, третейський суд тощо. Тому встановлення конфіденційності корпоративного договору цілком виправдано, оскільки вся публічна інформація щодо створення та діяльності товариства міститься в його установчому документі – статуті, і цієї інформації, яка в ньому міститься, достатньо, щоб мати уявлення про товариство, його учасників, їх права та обов'язки, органи управління тощо. Корпоративний договір не повинен бути дублікатом статуту товариства, а повинен передбачати саме конфіденційні умови домовленостей між учасниками з приводу реалізації ними своїх прав та повноважень, і такі домовленості виносяться на публічний розгляд, крім випадків, коли інше не буде встановлено сторонами договору, про що буде прямо зазначено в договорі.

Водночас, Закон містить виключення із загального правила, зокрема, корпоративний договір, стороною якого є держава, територіальна громада, державне або комунальне підприємство чи юридична особа, у статутному капіталі якої 25 і більше відсотків прямо або опосередковано належить державі або територіальній громаді, оприлюднюється протягом 10 днів з моменту його укладення шляхом розміщення на сайті відповідного органу державної влади, органу місцевого самоврядування.

В таких випадках вимога розголошення умов корпоративного договору цілком зрозуміла, оскільки йде мова саме про діяльність товариств, заснованих на державній та/або комунальній власності, та відповідно діяльність таких товариств повинна бути прозорою і контрольованою.

Корпоративний договір обов'язково укладається в письмовій формі, нотаріальне посвідчення такого договору можливе на вимогу сторін. Таким чином, при укладанні договору в простій письмовій формі, дотримання конфіденційності змісту договору покладається на самі сторони договору, від них залежить те, як вони дотримуються приватності при підготовці договору, його укладанні, при подальшому його зберіганні. У випадку нотаріального посвідчення корпоративного договору, конфіденційність договору також буде захищена ще й нотаріальною таємницею (ст. 8 Закону України «Про нотаріат»: нотаріальна таємниця - сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо) [3].

Вважаю, що сьогодні в Україні ще не склалася практика щодо укладення корпоративних договорів, тому слід враховувати і застосовувати досвід інших країн, які вже тривалий час і досить плідно використовують цей юридичний інструмент при визначенні відносин між учасниками товариств.

Список використаних джерел:

1. Про товариства з обмеженою та додатковою відповідальністю: Закон від 06.02.2018 № 2275-VIII.- URL: <http://zakon.rada.gov.ua/laws/show/2275-19>
2. URL: <https://uk.wikipedia.org/wiki/Конфіденційність>
3. Про нотаріат: Закон від 02.09.1993 № 3425-XII. -URL: [http:// zakon.rada.gov.ua/laws/show/3425-12](http://zakon.rada.gov.ua/laws/show/3425-12)

*Бежвець А. М., ст. викладач
ФСП КПІ ім. Ігоря Сікорського*

КІБЕРПРОСТІР ЯК НЕОБХІДНА СКЛАДОВА КІБЕРБЕЗПЕКИ СУСПІЛЬСТВА

Розвиток сучасних інформаційних технологій спричиняє сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, що, в свою чергу, зумовлює формування окремої сфери суспільних відносин – інформаційних (цифрових) правовідносин.

Безпека держави залежить від того, як вона використовує можливості та вирішує проблеми в інформаційному просторі та забезпечує кібербезпеку суспільства. З метою забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів у цій сфері 05.10.2017 було прийнято Закон України «Про основні засади забезпечення кібербезпеки України».

Цей закон має на меті створення національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами шляхом комплексного підходу у тісній взаємодії державного і приватного секторів та громадянського суспільства.

Підставно зауважити, що прийняття цього закону є актуальним та необхідним кроком на сучасному етапі розвитку України. В положеннях закону знайшли своє відображення основні науково-практичні тенденції щодо визначення понятійно-категоріального апарату, організаційних, правових, інженерно-технічних заходів регулювання кіберпростору.

Проте, зазначений закон має ряд зауважень (критики) щодо застосованого законодавчого підходу, який не відповідає вимогам щодо якості законів в контексті верховенства права, гарантованого статтею 8 Конституції України, зокрема його елементу «юридична визначеність», який вимагає, щоб норми були чіткими і точними та спрямованими на забезпечення того, щоб ситуації та правовідносини залишалися передбачуваними, оскільки закон має декларативні положення, принципи і наміри.

Не зважаючи на категоричні заперечення деяких науковців, зазначеним законом введено поняття кіберпростору як середовища (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

На нашу думку, закріплене в законі визначення кіберпростору є не досить вдалим і надто складним для сприйняття і розуміння, оскільки його формулювання здійснюється за допомогою слів, виразів та термінів, значення яких є не більш зрозумілим чи відомим, аніж саме значення кіберпростору.

Враховуючи значний досвід в цій сфері інших країн, доцільно порівняти визначення кіберпростору згідно українського законодавства із аналогічним поняттям за законодавством та судовою практикою цих країн.

Наприклад, згідно з рішенням Верховного Суду США (JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al., APPELLANTS v. AMERICAN CIVIL LIBERTIES UNION et al.), під кіберпростором розуміється унікальне середовище, що не розташоване в географічному просторі, але доступне кожному в будь-якій точці світу, за допомогою доступу до мережі Інтернет.

«Інтернет» Верховний Суд США визначає як глобальне об'єднання комп'ютерних мереж і інформаційних ресурсів, що не має чітко визначеного власника і служить для інтерактивної комунікації фізичних і юридичних осіб.

На наш погляд, визначення, наведене в рішенні Верховного Суду США, найбільш повно відображає співвідношення інформаційного простору та кіберпростору як загального до конкретного, та розкриває природу кіберпростору.

Таким чином, визначення кіберпростору, яке міститься в національному законодавстві, не є досконалим та потребує наступного доопрацювання з урахуванням норм міжнародного права, наукової думки та практики застосування.

Розділ 5 *ІННОВАЦІЇ У РОЗВИТКУ ПРАВОВОЇ НАУКИ ТА ОСВІТИ В ІНФОРМАЦІЙНІЙ СФЕРІ*

*Мельниченко А. А., к. ф. н., доцент,
декан ФСП КПІ ім. Ігоря Сікорського*

ІНФОРМАЦІЙНЕ ПРАВО В СТРУКТУРІ ПІДГОТОВКИ ФАХІВЦІВ З ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

Становлення інформаційного права як окремої галузі правничих наук пов'язане з бурхливим розвитком інформаційно-комунікаційних технологій, трансформацією інформаційної культури населення, утвердженням головних рис поставання інформаційного суспільства та появою нових викликів і загроз функціонуванню як людини, так і держави. Сучасна людина суттєво занурена в систему інформаційних відносин та зв'язків, які повинні належним чином урегулюватися на засадах справедливості, законності та гуманності.

Вимоги, які вже сьогодні необхідні сучасним фахівцям у різних сферах діяльності, суттєво відрізняються від тих, що були ще 20 років тому. В свою чергу, майбутні фахівці потраплять у значно відмінне робоче середовище, ніж їхні колеги у минулому, а це означає, що вони повинні розуміти зміни, які несе у собі цифровізація та інформатизація.

Окремою проблемою постає питання підготовки фахівців саме у галузі публічного управління та адміністрування. Добре усвідомлюючи закономірності співвідношення суспільного буття і суспільної свідомості, все ж таки вкажемо, що у рамках конкретного історичного періоду розвитку суспільства або державного утворення роль особистості (у нашому випадку – публічного управлінця) та її активного впливу на суспільні процеси, важко перебільшити. Під публічними управлінцями у цьому контексті ми розуміємо всю «армію чиновників», тобто осіб, уповноважених на виконання функцій держави або місцевого самоврядування. Ми переконані, що майбутні державні чиновники повинні володіти комплексом компетентностей, які дозволять ефективно управляти суспільними процесами на мікро-, мезо- та макрорівнях, якісно надавати адміністративні послуги населенню, забезпечувати реалізацію принципів сталого розвитку держави, регіону або громади. Донедавна фахова освіта для публічних (державних) управлінців обмежувалася магістерською підготовкою, яка здійснювалася в основному через Національну академію управління при Президентіві України або її філії. Курикулум, зазвичай, передбачав наявність

правничої підготовки, але першочергово був пов'язаний з формуванням компетентностей з конституційного, адміністративного та фінансового права. Сьогодні, а тим паче у ближчому майбутньому, правнича підготовка фахівців у галузі публічного управління та адміністрування поряд зі знаннями з вказаних галузей права, першочергово потребуватиме знань з інформаційного права. Така необхідність викликана появою нових форм взаємодії громадян та держави, появою нових електронних сервісів, бурхливого розвитку електронного урядування. Зазначимо, що правове регулювання інформаційних відносин має комплексний характер, адже сам феномен інформації однаковою мірою є об'єктом методів як публічного, так і приватного права. Враховуючи те, що фахівці з публічного управління та адміністрування репрезентують розпорядників публічної інформації або інформації з обмеженим доступом адекватна інформаційно-правова поведінка цих суб'єктів управлінської діяльності є критично важливою для забезпечення національних інтересів держави. Вони часто потрапляють в ситуацію амбівалентності коли постає проблема співвідношення забезпечення свободи інформації та права на інформацію. Більше того, сучасному публічному управлінцю все частіше доводиться стикатися з ситуаціями, пов'язаними із взаємодією з засобами масової інформації, що в умовах гібридної агресії набуває серйозного значення, а відтак потребує необхідної правової підготовки. Більше того, часто особи, уповноваженні на виконання функцій держави або органів самоврядування, самі стають об'єктами збору інформації не тільки щодо їх публічної професійної діяльності, а також стосовно їх приватного життя. Відтак, компетентності пов'язані з умінням захисту права на недоторканність приватного життя є важливою компетентністю для сучасних державних службовців.

Нестримний розвиток глобальних інформаційних мереж, вимагає від державних службовців належного поведіння з персональними даними громадян і в цьому контексті, одним з головних завдань інформаційного права – захист цих даних. Незважаючи на те, що захист персональних даних в розвинених країнах вже давно є одним з пріоритетів взаємодії держави і громадянина, в Україні ще десять років тому цією проблемою в органах державної влади серйозно ніхто не переймався. Сьогодні ж ми ведемо мову про необхідність формування відповідної правової культури державних службовців у питанні поведіння з персональними даними громадян.

Враховуючи той факт, що вітчизняне законодавство, не дивлячись на наявність певної кількості базових законів, ще зовсім недосконало визначає вихідні засади регулювання інформаційних відносин, нинішнім державним службовцям варто у своїй діяльності враховувати напрацювання наукового співтовариства в галузі правових наук, які ближчим часом можуть лягти в основу відповідних нормативно-правових актів.

Варто відзначити, що окремі освітні програми з підготовки фахівців за спеціальністю «Публічне управління та адміністрування» вже в структурі своїх

навчальних планів мають дисципліни спрямовані на формування компетентностей з інформаційного права. Зокрема, хорошим прикладом цього є освітні програми, які пропонує КПІ імені Ігоря Сікорського.

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

ІНФОРМАЦІЙНА МОДЕЛЬ МЕХАНІЗМУ ДОРОЖНЬО-ТРАНСПОРТНОГО ЗЛОЧИНУ

Застосування заходів кримінально-правового впливу щодо винних у злочинному порушенні правил безпеки дорожнього руху та експлуатації транспорту вимагає встановлення механізму вказаних діянь. Складність цього завдання полягає у тому, що дорожньо-транспортні пригоди (далі – ДТП) відбуваються протягом лічених секунд. Зокрема, перебіг події, коли водій на швидкості 80 км/год вчинює наїзд на нерухому перешкоду, внаслідок чого гинуть водій і пасажери, триває всього 0,15 секунди [1, с. 81].

Отже, перед органами розслідування при встановленні механізму ДТП постають складнощі відтворення його обставин через виявлення, фіксацію, перевірку та оцінку доказів. Такими доказами є інформація, на підставі якої у визначеному законом порядку орган досудового розслідування і суд встановлюють наявність або відсутність суспільно небезпечного діяння, винність особи, яка вчинила це діяння, та інші обставини, що мають значення для вирішення кримінального провадження. Така інформація встановлюється показаннями (свідка, потерпілого, підозрюваного, обвинуваченого, підсудного), висновками експертів, речовими доказами, протоколами слідчих і судових дій, схемами місця ДТП тощо. Таким чином, від достовірного встановлення інформації щодо обставин ДТП залежить вирішення завдань кримінального судочинства, а відтак дотримання законності, прав і свобод людини.

Саме цим обумовлюється проблема застосування сучасних інформаційних технологій при розслідуванні ДТП. За відповідною методикою на місці пригоди з'ясовують інформацію про розташування транспортних засобів (далі – ТЗ), слідів гальмування, бокового заносу, знаходження уламків скла, металу та інших об'єктів, що вказують на місце зіткнення, наїзду тощо. Шляхом вимірів отримується інформація щодо ділянки дороги, смуг руху, тротуарів, узбіч, геометричних параметрів перехресть та інших елементів дорожньої обстановки.

Необхідну інформацію отримують при огляді і перевірці технічного стану транспортних засобів, органів їх керування, зокрема рульового керування, положення і справності робочого й стоянкового гальм, важеля коробки передач, зовнішніх світлових приборів, зчеплення причепа, кріплення вантажу та багатьох інших.

За показами свідків, потерпілих, підозрюваного, обвинуваченого з'ясовується інформація щодо обставин виникнення аварійної ситуації, яка вивчається, аналізується та оцінюється з метою встановлення інформаційної моделі механізму пригоди. Разом з цим стрімкий перебіг ДТП показує, що безпосередній розвиток її механізму (небезпечно-аварійної обстановки) у середньому триває від 3 до 5 секунд. Тому очевидно, що покази учасників ДТП про вказаний механізм переважно мають орієнтовний характер. Зокрема, аналіз кримінальних проваджень показує, що при визначенні свідками швидкості ТЗ, їх покази мають розбіжність від 10 до 30 км/год, а нерідко й більше. Розрахунки швидкості ТЗ за слідами гальмування дозволяють отримати більш точну інформацію, проте й тут часто виникають складнощі, коли частина кінетичної енергії ТЗ згасає за рахунок їх зіткнення, наїзду на перешкоду, перекидання тощо. Крім того, інформація про стан дорожнього полотна, коефіцієнт ковзання та інші параметри, що слугують складовими при визначенні швидкості ТЗ перед аварією, внаслідок відсутності надійних методик та відповідного інструментарію також часто мають лише вірогідний характер.

Зокрема, використання при проведенні судової автотехнічної експертизи інформації щодо вихідних даних з розбіжностями нижчого і вищого показників швидкості ТЗ (наприклад, 60 – 80 км/год), не усунуті під час розслідування, часто створюють ситуацію, при якій висновок експерта дає підстави для альтернативних рішень, що впливає на кримінально-правову оцінку діяння, пов'язану з безпідставним звільненням або, навпаки, притягненням особи до кримінальної відповідальності та покарання.

Визначення відповідних даних під час експериментальних дій при відтворенні механізму ДТП також не завжди забезпечує отримання точної інформації щодо показників швидкості ТЗ, встановлення факту функціонування світлових приборів тощо. Більш того практика показує, що нерідко протиріччя щодо такої інформації у показах свідків, потерпілих чи підозрюваних взагалі не вдається усунути.

Засобами подолання цих вад є використання спеціальних пристроїв та технологій, необхідних для отримання відповідної доказової інформації. Так, сьогодні ТЗ облаштовуються бортовими комп'ютерами, що діагностують його параметри у процесі руху. Також існує можливість використання з цією метою так званої «чорної скриньки», що застосовується для реєстрації робочих параметрів основних систем ТЗ. Успішні розробки таких приладів здійснено в Італії, Канаді, Росії, США, ФРН, Японії та інших країнах світу. За повідомленнями засобів масової інформації «чорні ящики» використовуються при розкритті злочинних порушень правил безпеки дорожнього руху. Так, в м. Монреаль Г., керуючи автомобілем «Pontiac Sunfire», вчинив зіткнення з машиною під керуванням 19-літнього З., який загинув. У аварії Г. звинуватив загиблого водія, стверджуючи, що той рухався на червоний сигнал світлофора. Свідків зіткнення не було – ДТП відбулася вночі. Суд в якості доказу використовував дані вмонтованої в

автомобіль «чорної скриньки». Г. не знав, що в машині був цей прилад, який зберіг запис останніх 5 секунд до наїзду. Поліція з'ясувала, що машина Г. рухалася зі швидкістю 160 км/год, тобто тричі вище припустимої, і перед зіткненням водій не гальмував. Канадський суд засудив Г. за «необережне керування автомобілем, що привело до смерті людини».

У ФРН розроблено автомобільну «чорну скриньку» або датчик аварійних даних, основу якого складає запам'ятовуючий пристрій, а дані постійно оновлюються і «заморожуються» лише у момент аварії. В результаті зберігається об'єктивна інформація про стан і поведінку автомобіля та водія в останні 30-40 секунд до аварії. Національна асоціація аварійних служб (США) ще у 2001 році представила створену компанією Veridian автомобільну «чорну скриньку» з системою глобального позиціонування, запису швидкості руху автомобіля, його координат і параметрів ушкодження під час аварії та передачі інформації в аварійну службу, що дозволяє визначити як відбулася аварія, характер механізму аварії автомобіля та його положення в даний момент часу. Останнім часом з'явилися подібні запатентовані вітчизняні розробки [2].

Значні складнощі для органів розслідування виникають у ситуаціях, що виникають при зіткненні ТЗ, особливо при їх маневруванні, проїзді перехресть, коли виникає питання щодо порушень водіями правил користування зовнішніми світловими приборами, особливо в умовах недостатньої видимості. Незавжди уявити, що використання цих даних є вагомою, об'єктивною інформацією для органів розслідування та суду.

Останнім часом отримують резонансний характер факти ДТП з особливо тяжкими наслідками, пов'язані із травмуванням та загибеллю багатьох людей, що привертає підвищену увагу громадян до таких злочинів. При цьому, засоби масової інформації ретельно відстежують судові процеси у таких справах і часто висвітлюють недоліки, протиріччя і прогалини, що, насамперед, стосуються інформаційних характеристик тих чи інших доказів, зокрема пов'язаних з показниками швидкості руху ТЗ. А відтак результати розслідування та судового розгляду таких проваджень сприймаються як недостовірні та необ'єктивні.

Натомість надійними параметрами, що мають доказовий характер, зафіксованими «чорною скринькою», можуть бути: положення, технічний стан і функціонування рульового керування; технічний стан і функціонування робочої гальмової системи (величина вільного ходу педалі, тиск у гальмовій системі); технічний стан і функціонування стоянкового гальма та положення його приводу; швидкість руху ТЗ; положення педалі газу і важелю коробки передач; технічний стан тягово-зчіпного пристрою; положення передніх коліс відносно ТЗ; технічний стан зовнішніх світлових приладів ТЗ, причепу (фари, покажчики поворотів, передні і задні габаритні ліхтарі, стоп-сигнали); наявність і стан ременів безпеки, вага ТЗ та інші. Важливим є використання Web-камер у ТЗ з максимальним кутом огляду, з фіксацією зображення, дати і часу. Камери дозволяють фіксувати все, що відбувається в ТЗ і біля нього. Йдеться про інформацію щодо поведінки водія за

кермом, сприймання тих чи інших обставин перед пригодою (рух ТЗ і пішоходів, перешкоди на шляху, видимість дорожніх знаків, світлофорів тощо).

Обов'язкове обладнання ТЗ «чорними скриньками» для фіксації вищезазначених параметрів дозволить будувати інформаційну модель ДТП не на вірогідних даних, що враховують методично обґрунтовані допустимі припущення, а на точних інформаційних показниках, отриманих за допомогою сучасних технологій, що також сприятиме запобіганню аварійності.

Список використаних джерел:

1. Жерондо К. Безопасность движения: прошлое, настоящее, будущее: Пер. с франц. / Под ред. В. И. Жулева. – М.: Юрид. лит., 1983. – 224 с.

2. База патентів України // Автомобільна чорна скринька (“black motor-car box”). URL: <http://uapatents.com/7-87178-avtomobilna-chorna-skrinka-black-motor-car-box.html#about>.

*Дубняк М. В., к.ю.н., старший викладач
ФСП КПІ ім. Ігоря Сікорського*

ПОНЯТТЯ ТА ПРАВОВИЙ СТАТУС ТЕХНОЛОГІЧНОГО КОНТРАКТУ

У міжнародній торгівлі важливе місце займають зовнішньоекономічні контракти, правове регулювання яких є досить системним і складається з національних та міжнародних документів. З розвитком сучасних інформаційних технологій у цифровій економіці з'являються все нові способи й механізми для реалізації волі сторін і скорочення часу на здійснення різноманітних транзакцій. Разом з тим, такі нововведення не завжди ефективно регулюються в рамках традиційного законодавства. Тому, для повноцінного розвитку цифрової економіки необхідне вдосконалення правового регулювання застосування нових технологій. Зокрема, це стосується комп'ютерних технологій, що сприяють укладенню та виконанню контрактів, які останнім часом отримали назву розумних (смарт) контрактів. Таким чином, вирішення правових проблем, які виникають у зв'язку із застосуванням розумних (смарт) контрактів, є актуальним.

Під смарт-контрактом, з урахуванням теоретичних положень наведених в роботі [1], будемо розуміти контракт, умови якого викладені у формі програмного коду на платформі Blockchain, який забезпечує автономність і автоматизацію фіксації виконання умов такого контракту, у разі настання заздалегідь визначених в ньому обставин.

Особливістю смарт-контракту є те, що фіксація умов його виконання здійснюється без участі сторін. Це відбувається завдяки тому, що істотні умови договору перенесені в програмний код: у момент програмування смарт-контракту і від моменту його внесення до децентралізованої платформи їх неможливо змінити, а фіксація виконання умов контракту відбувається автоматично та не залежить від подальшої волі сторін.

Традиційно договори укладаються у вигляді формулювання умов, з настанням яких сторонам слід вчинити певні дії. Момент вчинення цих дій фіксується за допомогою окремих документів – актів приймання-передавання, накладних на відвантаження продукції тощо.

Програмування умов смарт-контракту викладаються за логікою «якщо-то-інакше», тому вони мають бути сформульовані таким чином, що не потребують внесення додаткових відомостей про виконання певних етапів контракту.

Наприклад, смарт-контракт поставки продукції вважається виконаним, коли у середовищі його виконання зафіксовано дані про надходження товару на склад. При цьому, такі дані ідентифікуються за допомогою чіпів, сенсорів, трек-кодів, які можливо співставити із номенклатурою замовлення. Після цього автоматично виконується транзакція щодо розрахунків між сторонами. Або інший приклад: смарт-контракт оренди офісу. У випадку, якщо орендодавець не отримає в обумовлений строк кошти, відбувається автоматичне блокування вхідного замка у приміщенні.

Одразу відзначимо, що не всі істотні умови договору, укладеного в загальному порядку (ст. 181 ГК України), можливо запрограмувати у смарт-контракті, так як, відсутні джерела цифрових даних, обробка яких обумовлює виконання умов смарт-контракту. Це пов'язано з емпіричністю даних, які неможливо перетворити у цифрові дані для їх ідентифікації смарт-контрактом (*наприклад, питання якості надання послуг, факт належного пакування та маркування товару, визначення відповідальності сторін, порядок вирішення спорів*). Підтвердження виконання певних умов смарт-контракту відбувається за допомогою спеціальних програмних засобів — «оракулів», які містять цифрові дані з оточуючого світу, придатні для обробки в блокчейн-системах (*наприклад, вчинення нотаріусом дій щодо зміни правовласника майна, акт прийому-передачі товарів, робіт, послуг тощо*).

Така ситуація призводить до різних правових фікцій щодо правового статусу смарт-контракту.

На даному етапі розвитку технологій та правового регулювання суспільних відносин, пов'язаних з їх використанням, доцільніше вести мову про технологічні контракти. В свою чергу, це обумовлює необхідність розмежування понять смарт-контракту та технологічного контракту.

Технологічний контракт – це договір, укладений в загальному порядку, з дотриманням всіх вимог законодавства, в якому за домовленістю сторін визначено технологічну складову, за допомогою якої відбувається автоматична фіксація виконання умов договору на базі будь-яких технологічних рішень.

Саме за такою схемою було здійснено транзакцію купівлі-продажу нерухомого майна за криптовалюту [2]. Сторонами було укладено попередній договір у загальному порядку, в якому фіксувалось волевиявлення сторін щодо продажу майна, а умови щодо перерахування коштів були реалізовані за допомогою резервування коштів у криптогаманцях. Виконання транзакції

залежало від зміни правовласника нотаріусом. Отже, мав місце договір купівлі-продажу, укладений у загальному порядку, умови виконання якого містили технологічну складову.

Отже, технологічна складова умов договору щодо перерахування криптовалюти виконувалась після традиційних процедур зміни правовласника, які не можуть виконуватись автоматично у середовищі смарт-контракту.

Таким чином, правове становище технологічного контракту може визначатися як спосіб забезпечення виконання зобов'язання. Вбачається, що використання технологічної складової у договорі не суперечить приписам ч.1 ст. 199 ГК України, відповідно до якої, за погодженням сторін, можуть застосовуватися передбачені законом, або такі, що йому не суперечать, види забезпечення виконання зобов'язань, які звичайно застосовуються у господарському (діловому) обігу та ч.2 ст. 546 ЦК України, за якою договором або законом, можуть бути встановлені інші види забезпечення виконання зобов'язання.

Отже, у правовій моделі технологічного контракту як способу забезпечення зобов'язання, варто укладати договір у загальному порядку із дотриманням вимог ст. 203 ЦК України та зазначення істотних умов, які стосуються певного виду договору, а також умов про технологічну складову, які відображають особливості способу забезпечення виконання зобов'язання, з використанням будь-яких технологічних рішень. Наприклад, технологічна складова щодо умов оплати робіт/послуг може бути така: децентралізована блокчейн-платформа (чи інше технологічне рішення) є способом забезпечення виконання зобов'язання сторони А перед стороною Б, в т.ч. грошового, за цим договором. Крім того, доцільно зазначати електронні адреси сторін; адреси електронно-цифрових гаманців; місця укладання чи виконання контракту; умови про конфіденційність паролів; відповідальність програміста та третіх осіб за точність відображення волі сторін в технологічному контракті (що відповідає приписам ст. 511 ЦК України); дії сторін у разі похибки програмного забезпечення; грошовий еквівалент криптовалюти до національної одиниці чи іноземної валюти (дотримання ст. 524 ЦК України).

Крім того, в умовах цифрової економіки доцільно врахувати вимоги щодо змісту і форми зовнішньоекономічних контрактів (*далі ЗЕД-контракти*), як таких, що найбільш часто будуть використовувати технологічну складову.

У випадку, коли сторонами технологічного контракту є суб'єкти з різних держав, доцільно проаналізувати національні законодавства про зовнішньоекономічну діяльність на предмет виявлення правових ризиків та особливостей укладання та виконання технологічних контрактів.

Наприклад, відповідно до ст. 1 Закону України «Про зовнішньоекономічну діяльність» зовнішньоекономічний договір (далі ЗЕД-контракт) - це домовленість двох або більше суб'єктів зовнішньоекономічної діяльності, та їх іноземних контрагентів, спрямована на встановлення, зміну, або припинення їх взаємних прав та обов'язків у зовнішньоекономічній діяльності.

Права та обов'язки сторін ЗЕД-контракту відображаються в умовах договору, визначаються матеріальним та процесуальним правом місця укладання контракту, якщо сторони не погодили інше [3].

Отже, дискусійні питання визначення юрисдикції технологічних контрактів можуть вирішуватись відповідно до правового регулювання ЗЕД-контрактів, із зазначенням в умовах технологічного контракту місця його укладання або обрання юрисдикції та норм міжнародного права, які до нього будуть застосовуватись.

У постанові Кабінету Міністрів України визначено типові платіжні умови ЗЕД-контрактів [4]. В умовах цифрової економіки, крім рекомендованих форм здійснення платежу, доцільно використовувати і ті, які пов'язані зі здійсненням розрахунку за допомогою електронних гарантів. Перевага даного способу полягає у тому, що вартість зобов'язань резервується в електронному гаранті у момент програмування смарт-контракту, а перерахунок автоматично залежить від фіксації виконання умов договору та не залежить від подальшої волі та дій сторін, тобто не може відбутись волюнтаристська відмова від платежу.

Висновки. Основним призначенням блокчейн-технології є формування довіри між учасниками ринку, а смарт-контрактів – уникнення економічного волюнтаризму у відносинах між сторонами. Такі технології призначені для спрощення реалізації договірних відносин та забезпечення їх реального виконання. Правові проблеми щодо застосування смарт-контрактів та інших нових технологій виникають, коли технологічні рішення намагаються перевести у поняття та категорії матеріального світу та правових доктрин, що концептуально видається не завжди можливим. Тому, застосовано інший підхід – визначення правового статусу технологій у вже сформованій правовій доктрині та вимогах традиційного договірної права. Положення договору, укладеного у загальному порядку, деякі умови якого виконуються за домовленістю сторін з використанням будь-яких технологічних рішень (технологічний контракт або договір з технологічною складовою), загалом відповідає концепції традиційного договірної права.

Список використаних джерел:

1. Савельев А.И. Договорное право 2.0 : «умные» контракты как начало конца классического договорного права // Вестник гражданского права. – 2016. – № 3. – С. 32-60. URL: <https://elibrary.ru/item.asp?id=26468044>

2. Эксперты рассказали подробности первой в мире продажи недвижимости через смарт-контракт URL: <https://forklog.com/eksperty-rasskazali-podrobnosti-pervoj-v-mire-prodazhi-nedvizhimosti-cherez-smart-kontrakt/>

3. Положення про форму зовнішньоекономічних договорів (контрактів) : наказ Міністерства економіки та з питань європейської інтеграції України від 6 вересня 2001 р. № 201, URL: <http://zakon3.rada.gov.ua/laws/show/z0833-01>

Про типові платіжні умови зовнішньоекономічних договорів (контрактів) і типові форми захисних застережень до зовнішньоекономічних договорів (контрактів), які передбачають розрахунки в іноземній валюті: постанова Кабінету

*Тихонова Д. М., студент
ФСП КПП ім. Ігоря Сікорського
Науковий керівник:
Яшарова М. М., к.ю.н., доцент
ФСП КПП ім. Ігоря Сікорського*

ОСОБЛИВОСТІ ОХОРОНИ АВТОРСЬКИХ ПРАВ В МЕРЕЖІ ІНТЕРНЕТ

Наразі інтернет відіграє важливе значення у створенні інформаційного простору глобального суспільства та стає все більш популярним обміном, розповсюдженням та використанням інформації, але не завжди використання цієї інформації є законним. Не секрет, що інтернет став найпопулярнішим способом відображення інформації, тому що він є більш дешевим, зручним та масштабним для її розповсюдження. І тому дослідження даного питання щодо охорони майнових та особистих немайнових прав авторів є досить актуальною у світі інформаційного прогресу.

Метою статті є дослідження деяких аспектів правового регулювання відносин, що виникають у процесі неправомірного використання об'єктів авторського права в цифровій мережі Інтернет та шляхи удосконалення законодавства відповідно досвіду європейських країн.

Відповідно до Закону України «Про авторське право і суміжні права» поняття «авторське право» невизначено, хоча у ст.8 Закону України «Про авторське право і суміжні права» та ст.433 Цивільного кодексу України надано перелік об'єктів, які відносяться до авторського права, зокрема:

1) літературні та художні твори (романи, поеми, статті та інші письмові твори; лекції, промови, проповіді та інші усні твори; драматичні, музично-драматичні твори, пантоміми, хореографічні, інші сценічні твори; музичні твори (з текстом або без тексту); аудіовізуальні твори та інші групи об'єктів);

2) комп'ютерні програми;

3) компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;

4) інші твори [1; 2].

Перелік об'єктів, яким надана правова охорона, є не вичерпним, відповідно з розвитком технічного та цифрового процесу, він надалі буде збільшуватися і потребувати якісної охорони від правопорушень прав осіб і авторських прав в першу чергу.

О.А. Підпригора визначає поняття “авторське право” у суб'єктивному та об'єктивному значенні. В об'єктивному значенні – це цивільно-правовий інститут, що регулює відносини, які складаються у зв'язку зі створенням і використанням творів літератури, науки і мистецтва. У суб'єктивному значенні авторське право –

це ті особисті немайнові та майнові права, що належать особам, які створили твір літератури, науки і мистецтва або їх правонаступникам чи іншим суб'єктам авторського права [3, с. 28].

Інколи особа випадково порушує авторські права, наприклад, копіює фотознімок та виставляє його у своїх ресурсах або ж накладає аудіо на відеоролик, але не усвідомлює, що фото або аудіо створенні іншою особою, тобто така особа є власником (а отже і носієм авторського права).

Досліджуючи досвід інших країн, то цікавим є охорона авторського права наприклад в США, де використовується поняття “fair use”, що означає “добросовісне використання”, тобто особа може вільно використовувати захищенні авторським правом матеріали за умови дотримання обмежень, а саме мова йде про використання в навчальних чи дослідницьких цілях, новинах, коментарях. В Україні ж принцип «добросовісності» існує, але він закріплений як загальний в цивільному праві і не роз'яснюється у інших джерелах авторського права.

Щодо охорони авторського права в інтернеті зі сторони держави, то існує судовий порядок врегулювання спорів. Згідно ст.432 Цивільного кодексу України – правовласник має право на звернення до суду, вимагати застосування заходів щодо припинення та запобігання порушення авторського права, відшкодування збитків, та втраченої вигоди [2].

Також існує альтернативний спосіб врегулювання, який розглянемо на прикладі відомої соціальної мережі «Instagram», яка є великим та популярним хостингом та постійно слідкує за оригінальністю завантаженого контенту та має зворотній зв'язок зі своїми користувачами. Тобто, якщо ваші права порушили, ви маєте право написати скаргу на файл, яка повинна містити докази порушеного права. Потім подана вами скарга розглядається уповноваженими особами і після рішення вони повідомляють особу, яка розмістила об'єкт авторського права, про порушення права іншої особи та зобов'язують її видалити його або видаляють його самостійно та попереджають про відповідальність за порушення авторських прав.

Як висновок можна сказати, що захист авторських прав у мережі Інтернет в Україні існує, але законодавство потребує вдосконалення та створення нормативних актів, які б прямо вказували врегулювання відносин у мережі Інтернет, тому що світ не стоїть на місці і в майбутньому інтернет-відносини будуть передовими і потребуватимуть відповідної охорони.

Список використаних джерел:

1. Цивільний кодекс України. -URL:<http://zakon2.rada.gov.ua/laws/show/435-15>.

2. Про авторське право та суміжні права : Закон України від 23 грудня 1993 р. № 3792-ХІІ.- URL:<http://zakon4.rada.gov.ua/laws/show/3792-12>.

Підпригора О. А. Поняття авторського права / О. А. Підпригора // Часопис цивілістики. - 2012. - Вип. 13. - С. 28-38. – URL: http://nbuv.gov.ua/UJRN/Chac_2012_13_7

*Мерзленко І. О., студент
ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Баранов О. А., д.ю.н., доцент, професор
ФСП КПІ ім. Ігоря Сікорського*

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА КРИПТОВАЛЮТ ТА ФІАТНИХ ГРОШЕЙ

Поняття “криптовалюта” набуло розголосу в 2009 році, коли з’явився перший bitcoin. У той період **700-1600** bitcoins можна було купити за **1 долар** США, сьогодні один bitcoin коштує понад **шість з половиною** тисяч доларів. Тепер, поряд з bitcoin, ми можемо побачити багато інших видів криптовалюти (більше 400), окрім цього існує понад 500 криптовалютних бірж, кількість яких з кожним днем зростає, а світова капіталізація ринку криптовалют перевищила 700 мільярдів доларів США. Тому з упевненістю можемо говорити про те, що криптовалюта - це початок нової історії, новий етап існування високотехнологічного ринку.

Багато науковців прогнозують навіть витіснення фіатних грошей криптовалютою (**фіатні гроші** - (англ. fiatcurrency) - тип грошей або валюти, цінність яких походить не від власної вартості або гарантії обміну на золото або іншу валюту, а від державного наказу (fiat) використання їх як засобу платежу[1]).

За словами відомого футуролога Томаса Фрея, до 2030 року криптовалюти однозначно залишаться та витіснять приблизно 25% національних валют, тому що вони набагато ефективніші [2]. На думку Білла Гейтса, bitcoin перевершує класичні валюти, забезпечуючи гнучкість і зручність транзакцій, особливо великих [3].

Для того, щоб зрозуміти, чи дійсно криптовалюта може сьогодні якісно замінити фіатні гроші, розглянемо, перш за все, її здатність виконувати функції фіатних грошей.

Фіатні гроші виконують такі функції: міра вартості, засіб обігу, засіб платежу, спосіб накопичення, світові гроші [4].

Як виконує ці функції криптовалюта?

Міра вартості, тобто здатність надати кількісного виразу економічним процесам і явищам.

За допомогою криптовалюти сьогодні можливо встановити ціну на товар. У багатьох розвинених країнах, таких як США, Канада, Китай, Великобританія, у Європейському союзі криптовалюта виконує цю функцію.

Засіб обігу, тобто здатність бути посередником в товарному обміні.

Ця функція тісно пов’язана з попередньою функцією, вони взаємозалежні, оскільки обіг без ціни неможливий, так само як і відсутність сенсу в ціні та неможливість її визначення, коли немає обігу.

Сьогодні можна купити товар за криптовалюту. За даними UBR.ua [5], криптовалюту як оплату приймають найбільші компанії світу, такі як Microsoft, Dell, Galactic, AirBaltic, Innovecs, «VirginGalactic», «The New York Times», «CNN», «Reuters», «Zynga», «Overstock» і «Tiger Direct». Достатньо потужним поштовхом у розвитку системи «Bitcoin» стало її включення як одного зі засобів оплати товарів до найбільшого світового онлайн-магазину «eBay», що відбулося в квітні 2015 року.

Функція засобу платежу, тобто здатність погасити боргові зобов'язання (продаж товару у кредит, повернення позики, виплата заробітної плати, сплата комунальних платежів).

У США, наприклад, заробітні плати, що виплачуються працівникам у криптовалютах, є об'єктами федерального прибуткового податку і податків на заробітну плату[6].

У Японії деякі фірми пообіцяли виплачувати співробітникам зарплату в bitcoin - за бажанням. Таким чином, криптовалюта сьогодні виконує функцію засобу платежу[6].

Засіб накопичення, тобто тимчасове вилучення грошей з обігу з метою збільшення їх кількості та без втрати цінності.

Криптовалюта може зберігатися тривалий час в електронному гаманці, вона не повинна бути постійно в обігу, проте немає гарантій, що той чи інший вид криптовалюти не втратить свою цінність протягом певного проміжку часу. Через власну анонімність та відсутність будь-якого забезпечення криптовалюта сьогодні не може виконувати цю функцію.

Функція світових грошей полягає в обслуговуванні грошми руху вартості в міжнародному економічному обороті і забезпеченні реалізації взаємовідносин між державами.

Так як сьогодні криптовалюта є децентралізованою, її функціонування в якості світових грошей поки неможливе. Криптовалюта поки що виконує роль усього лиш посередника в розрахунках, які здійснюються переважно в доларах.

Але функцію світових грошей криптовалюта зможе виконувати тоді, коли стане законним засобом платежу з врегульованим курсом.

Таким чином, сьогодні криптовалюта виконує лише деякі функції фіатних грошей, а саме: міра вартості, засіб обігу, засіб платежу. Цього явно недостатньо, щоб замінити фіатні гроші.

Незважаючи на це, криптовалюта з кожним днем набуває популярності та має такі переваги над фіатними грошима:

- 1) **прозорість** — завдяки технології блокчейн кожен учасник спільноти може перевірити, які операції здійснювалися з будь-якого моменту;
- 2) **анонімність** - ніхто з учасників спільноти не має інформації про інших, оскільки йому доступний запис у вигляді набору цифр і букв;
- 3) **децентралізація** — база даних операцій з криптовалютами зберігається у вигляді копії у кожного учасника спільноти. Зруйнувати цю

систему обліку, засновану на технології блокчейн, можна лише за умови одночасного відключення всіх її учасників, які можуть перебувати у різних частинах світу. Таким чином, децентралізовану базу даних на відміну від централізованої практично неможливо знищити;

4) **швидкість** — переказ криптовалюти за допомогою технології блокчейн, як правило, відбувається досить швидко;

5) **захищеність** — блоки даних про операції з криптовалютами зашифровуються за допомогою хеш-функцій та спеціальних алгоритмів шифрування.

б) **гарантія** — система обліку операцій з криптовалютами на основі технологій блокчейн гарантує незмінність записів та їх збереження.

На мою думку, питання використання цифрових грошей як єдиного способу розрахунку – це лише питання часу. Увесь світ зараз займає «позицію вичікування» стосовно криптовалют замість того, щоб вирішити питання врегулювання цього явища на законодавчому рівні.

Однак, враховуючи постійно зростаючу популярність криптовалют, постійний стрімкий інноваційний розвиток, цифрові гроші – можна впевнено стверджувати, що це, є близьким майбутнім нашого інформаційного суспільства.

Список використаних джерел:

1. Фіатні гроші Futurist [Електронний ресурс]: доступ із веб-сайту <https://uk.wikipedia.org> (дата оновлення 14.10.2018) - URL: https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D0%B0%D1%82%D0%BD%D1%96_%D0%B3%D1%80%D0%BE%D1%88%D1%96 (дата звернення 14.10.2018).

2. Cryptocurrency Will Replace National Currencies By 2030, According to This Futurist. - URL:<http://time.com> (дата оновлення 14.10.2018) URL: <http://time.com/money/5178814/the-future-of-cryptocurrency/> (дата звернення 14.10.2018).

3. Билл Гейтс о криптовалюте номер один. Новые деньги - это биткоин Futurist. -URL:<https://altcoin.info>(дата оновлення 14.10.2018),URL:https://altcoin.info/opinions/bill_gejts_o_kriptoaljute_nomer_odin_novyue_dengi_eto_bitkojn-928.html (дата звернення 14.10.2018).

4. Деньги и их функции [Електронний ресурс]: міжнародний науковий журнал «Иновационная наука»/ Х.М. Халліуліна, Н.С. Шарафієва// Бібліотечний вісник. – 2017. – № 02-1/2017. – с. 109-113. – URL: <https://cyberleninka.ru/article/n/dengi-i-ih-funktsii>(дата звернення 14.10.2018).

5. UBR [Електронний ресурс]: доступ із веб-сайту <https://ubr.ua/> (дата оновлення 14.10.2018) URL: <https://ubr.ua/>(дата звернення 14.10.2018).

6. Регулирование криптовалют. Исследования опыта разных стран.- URL: <http://www.eurasiancommission.org> (дата оновлення 14.10.2018) URL: <http://www.eurasiancommission.org/ru/act/dmi/workgroup/Documents/digest/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%20%D0%B2%20%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B0%D1%85%20%D0%BC%D0%B8%D1%80%D0%B0.pdf>(дата звернення 14.10.2018).

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

ВПЛИВ РОБОТОТЕХНІКИ НА СУСПІЛЬНІ ВІДНОСИНИ В ПРОМИСЛОВІЙ СФЕРІ

Сьогодні ніхто не може уявити своє життя без робототехніки. Чому так ?, тому що роботи роблять багато корисної роботи для кожного особисто і людства в цілому навіть на побутовому рівні не кажучи вже про великі підприємства. Якщо брати побутовий рівень то роботи займаються прибиранням будівель, пранням, миють посуд, тощо, якщо взяти підприємства то роботи та роботизовані системи роблять великий обсяг роботи, починаючи від збирання дрібних деталей закінчуючи складними процесами які людині не під силу зробити самостійно. На сьогоднішній день роботи можуть та, у високорозвинених країнах, вже створюють конкретну конкуренцію людині. Так як роботів застосовують у різних сферах діяльності, багато робітників можуть залишитись без робочого місця, що вплине рівень безробіття в країні у бік стрімкого його підвищення. Тому постає велике питання: яким буде подальший розвиток робототехніки для суспільства та людства, а саме це позитив чи негатив даного втручання роботів у наше життя? Розглянемо такий приклад: припустимо, що на якомусь заводі працює 100 працівників. Люди працюють, отримують заробітну плату, годують свої сім'ї. Господар цього заводу вирішує купити 50 роботів. Причина проста їм не потрібно платити заробітну плату, відсутні відпустки, можлива цілодобова праця та ін. - так йому, у фінансово-економічному плані та плані виробничого управління, буде вигідніше. І він звільняє не менше половини робочих, залишивши їх без роботи. Це призводить до того, що товари цього заводу стають дешевшими і господар заробляє більше. З часом поступово він замінить роботами і переважну більшість працівників, які ще залишилися. Це погано для цих робітників. Та й один з одним вони будуть ворогувати і боротися за робоче місце. Їх зарплата буде падати, тому що деякі будуть готові працювати на господаря і за менші гроші. В кінці кінців господар замінить останнього робочого роботом і на підприємстві будуть працювати одні роботи. В даному випадку, в плюсі залишається лише господар, якому не потрібно платити нікому заробітної плати та нести інші соціальні витрати, а витратити лише певні кошти на забезпечення праце спроможності роботів. Для робітників суцільна роботизація промислової сфери буде великим мінусом, у зв'язку з тим, вони залишаються дуже суттєво скорочуються можливості добування для свого та своєї родини засобів існування. Розглянемо ще одну ситуацію: уявимо що ці 100 осіб яких, звільнили з попереднього підприємства, побудували своїми руками цей завод. Самі на ньому працюють, отримують заробітну плату і годують свої сім'ї. І спільно відкладають певну суму коштів. Раптом на відкладені кошти вони вирішили купити 50 роботів. Постає

питання чи будуть вони когось звільняти? –напевно ні. Навіщо можна просто працювати менше в 2 рази, або позмінно, стільки ж заробляти, але більше часу приділяти на інші потреби а також сім'ї і більше відкласти. Вони не можуть когось звільнити, так як кожен з них , тій чи іншою мірою, є господарем. В даному випадку нема мінусів для когось, всі в рівних умовах, ніхто не залишається без роботи. Тому питання впровадження роботів на підприємствах залежить від тих хто володіє підприємствами ? Це з одного боку, а з іншого, саме головне, від фінансово-економічних переваг та характеру виробництва. Для прикладу візьмемо шахтарську справу. Раніше для того щоб добувати руду людині потрібно було спускатись глибоко під землю, дихаючи пилом та парами газів, на сьогодні та сама людина може знаходитись в кріслі якогось офісу та управляти за допомогою комп'ютера роботом який замість неї тепер виконує його роботу.

З великою інтенсивністю розвитку та застосування робототехніки в промисловості її ділять на три покоління:

- перше покоління – це прості роботи, що мають одну або кілька «рук» засновані на застосування автоматичних пристроїв, своє застосування вони знаходять при виконанні автоматизації транспортних операцій;

- друге покоління – це адаптивні роботи що контролюються через шину адаптивного управління, такі роботи здатні адаптуватися за допомогою датчиків зворотного зв'язку, можуть адаптуватися в зовнішньому середовищі виробничого процесу;

- третє покоління – це універсальні комп'ютерні систем, що здатні в процесі активної взаємодії з навколишнім середовищем навчатися, простіше це називається: роботи що мають штучний інтелект.

На сьогодні існують узагальнені обмеження для роботів, а саме:

- роботи не можуть заподіяти людині шкоди або допустити щоб своєю бездіяльністю людині було заподіяно шкоду, дане обмеження роботи вже порушили;

- роботи повинні підкорюватись усім наказам людини, окрім тих, що суперечать першому обмеженню;

- своєю безпекою роботи повинні піклуватися такою мірою, що не суперечить першому і другому обмеженню.

Отже можна зробити висновок, що впровадження роботів в промисловість:

- є еволюційним процесом розвитку як світового, так і національного суспільства;

- впровадження робототехніки безумовно впливають на зміни виробничих та загальних суспільних відносин;

- наслідки змін від впровадження робототехніки, у багатьох, залежать від державної політики у цій сфері, адекватності встановлення правовідносин зазначеним процесам.

РОЛЬ СОЦІАЛЬНО-ГУМАНІТАРНИХ ДИСЦИПЛІН В ПРОЦЕСАХ ФОРМУВАННЯ АКСІОСФЕРИ ВИЩИХ УЧБОВИХ ЗАКЛАДІВ

Освіта, без сумніву, є одночасно соціальним інститутом й комунікаційним процесом, галуззю, і інститутом соціокультурної сфери суспільства, яка із особливою гостротою відчуває вплив інформаційно-комунікаційних технологій (ІКТ) на процеси цивілізаційно-культурних змін і суспільної свідомості громадян. Освіта є найважливішим фактором соціалізації, навчання, виховання, інкультурації. Освіта – це й формування неповторності особистості, індивідуальності, і історія суспільства, і історія культури. Вища школа – найважливіший інститут у розвитку вітчизняної системи освіти, основними функціями якого сьогодні залишаються наступні: передача накопичених знань; забезпечення наступності соціального досвіду; засвоєння цінностей домінуючої культури; розкриття й розвиток здатностей особистості; просування особистості до більш високого соціального статусу, вплив на соціальну мобільність; капіталовкладення в майбутнє. Зміни в змісті й структурі освіти розгортаються у двох різноспрямованих тенденціях: комп'ютеризація системи освіти; гуманітаризація освіти [1].

Сьогодні цілісний аналіз вищої школи (поряд з такими теоретико-методологічними підходами, як комплексний, системний, структурно-функціональний, компетентнісний, порівняльно-історичний, комунікативний) [2] неможливий без аксіологічного, або ціннісно-значеннєвого теоретичного підходу.

Зміст аксіологічного підходу неможливо зрозуміти без розкриття змісту аксіології – філософської дисципліни, яка займається дослідженням цінностей як змістоутворюючих підстав людського буття, що й задають спрямованість і вмотивованість людському життю, діяльності й учинкам.

Інформаційно-комунікаційна парадигма сучасності напряму пов'язана із процесами глобалізації і широкої майже тотальною інформатизацією суспільства. Остання вибудовується на процесах пізнання і філософського осмислення понять про інформацію, надаючи їм низку нових рис, тенденцій і вимог до науково-освітніх.

Поява Internet й сучасних ІКТ спочатку розглядалася як чергове технічне досягнення цивілізації й один з багатьох інших наукових напрямків людських знань. Однак, швидкість їх розвитку й рівень впливу на абсолютно всі сфери сучасного суспільства привели до того, що це саме ті комунікативні технології, зміна яких рішучим образом змінює економічний і соціокультурний простір людського суспільства. Вивчення ІКТ, таким чином, стає не просто окремою галуззю науки й техніки, а основою нової економіки, соціального й культурного життя, принципово нової епохи, окремі риси якої видні вже сьогодні:

1. У топі 100 провідних компаній світу – перші десять місць займають ті компанії, які не існували буквально десять років тому й усі вони пов'язані з ІКТ. Бурхливий розвиток ІТ-сфери починає змінювати структуру економіки й економічний уклад, що склався.

2. Розвиток дистанційної освіти поступово змінить не тільки освітні технології, але й саму традиційну систему освіти, роблячи доступним набуття будь-яких знань у будь-якій точці планети для всіх людей будь-якого віку.

3. Застосування ІКТ у медицині, особливо в напрямку посилення фізичних та психічних можливостей людини, вихід за рамки її біологічних можливостей приведе до інтенсифікації діяльності не тільки якогось одного органа почуттів людини, як це було раніше при зміні комунікативних технологій, але й усього людського організму.

4. Наступає занепад «ери мас» і падіння ефективності традиційних мас-медіа у вигляді радіо, телебачення, друкованих ЗМІ й поп-культури, яку вони просувають і яка панувала протягом останнього часу.

5. Крім природного й соціального середовища проживання людини з'являється нове середовище – віртуальне, яке, безсумнівно, має свої особливі ознаки й закономірності розвитку й існування.

6. Наростаюча індивідуалізація все більше буде проявлятися в запереченні традиційних, століттями існуючих форм соціальності.

Список основних характеристик нової епохи ІКТ вже активно обговорюється представниками різних галузей знань. Однак всі вони вимагають теоретичного осмислення й узагальнення.

Найважливішою проблемою вищої освіти за таких умов стає вивчення понять та набуття під час занять ціннісноговиміру змістовної інформації. Вона має два головних виміри: перший – це орієнтація на нову соціально-політичну кон'юнктуру, що вимагає підготовки фахівців за новими спеціальностями, яких потребує ринок праці; другий – це вимоги до орієнтації процесу навчання і виховання науково-технічних фахівців на наявні духовні національні традиції, однією з яких є орієнтація на працю в колективі. Все це сходить до джерел вітчизняної гуманістичної педагогіки і психології нашого народу. Таким чином, сучасна вища школа повинна стати центром інтелектуального й духовного відтворення (культуро-центризм). Синтез ідей культууро-центризму, соціоцентризму й антропоцентризму віддзеркалюється в системі освітніх компетентностей, які декларуються у наукових і освітніх стандартах вищої освіти. Вимоги до професійної компетентності вихованців інженерно-технічних вищих навчальних закладів, їх загальнокультурної компетентності, яка включає до себе екологічну, політичну, економічну, правову, гуманітарну, естетичну, комунікативну, рекреаційну компетентності, постійно зростають. Синтез названих підходів у національних моделях сучасної вищої школи потенційно забезпечує відповідальність особистості за загальнозначущі людські цінності (відношення до життя, здоров'я, гідність, захист громадянських свобод, екологію середовища),

вільне ціннісне самовизначення й особистісну самоактуалізацію. Все це актуалізує обговорення теми щодо повноти викладання соціально-гуманітарних, юридичних і комунікативних дисциплін в освітніх програмах вітчизняних закладів вищої інженерної освіти.

Оптимальною моделлю вищої школи сьогодні вбачається культуро-творча модель, яка, безумовно, дозволяє уникнути однобічностей ринкових моделей, які руйнують фундаментальність і духовно-моральні орієнтири вітчизняної освіти. Безумовно, заняття мають проводитись так, щоб слухачам було цікаво, і вбачається само по собі, що заняття з викладачем покликано організувати просторово-часовий континуум⁹ освітнього процесу відповідно до логіки образу світу, співвіднесеного до власних можливостей становлення особистості. Можливо вона буде здатна уникнути витрати освіти на виховання молоді в стилі «пепсі», коли вища школа з інституту навчання й виховання перетворюється в один з інститутів ринку й суспільства споживання, коли студентам потрібні «корочки» диплома, «лейбл».

На нашу думку, проблема реальних, а не деклараційних цінностей вищої освіти пов'язана з раціональними й ірраціональними складовими аксіосфери інформаційно-комунікативного простору сучасних вищих учбових закладів, із процесами засвоєння змістусенсу самої освіти, із розумінням проблем виховання, інтеріоризацією¹⁰, соціалізацією, вдосконалення методів навчання, переконаннями, пов'язаними із критичною рефлексією контенту отриманої інформації.

Відзначимо, що освітні стандарти освіти і «втомленість» або невідповідність вимогам часу викладачів утворюють так звану раціональнукладову інформаційно-комунікативного просторув учбовому закладі і його аксіосферане просто сукупність ідей, образів і символів, що означають зміст/сене, мету, критерії оцінного відношення людини до світу речей і явищ, але існує і як віртуальна реальність. Ірраціональне в цьому просторі транслюється повсякденністю, повсякденним досвідом, засобами масової комунікації (ЗМК) і засобами масової інформації (ЗМІ), і, насамперед, – телебаченням і глобальними інформаційно-комунікаційними мережами. Усе це багато в чому і визначає аксіосферу вищої освіти.

Найбільш гнітючим у постмодернізмі є стирання ключових зв'язків або відмінностей, ерозія розрізнення між високою культурою й, так званою, масовою, або поп-культурою, ЗМК і ЗМІ, які є частиною масової культури, контент якої звернений, насамперед, до почуттів, емоцій, підсвідомості читача й глядача.

⁹ *КОНТИНУУМ* (утворено від латинського слова: *CONTINUUM* – безперервне, суцільне). Континуум – це безперервна сукупність, тривалість або послідовність. У філософії поняття континууму розглядається в рамках категорій безперервності і переривчастості, що характеризують буття і мислення.

¹⁰ *Інтеріоризація* (від лат. *interior* – внутрішній) – психологічне поняття, що означає формування розумових дій і внутрішнього плану свідомості через засвоєння індивідумом зовнішніх дій з предметами і соціальних форм спілкування. Інтеріоризація (англ. *interiorisation*) – присвоєння цінностей, їх вростання в особистість. Процес формування внутрішніх структур психіки. Процес переходу від зовнішніх (реальних) до внутрішніх (ідеальних) дій – психічних актів.

Основну інформацію про навколишній світ людина з дитинства сприймає не через слово, не через вербальний текст, а, як відзначають культурологи, «квантами візуальних образів» у їхньому русі.

Нові ІКТ, які використовуються в системі комунікацій вищого навчального закладу, мають такі характеристики, як оперативність, мала витратність, мультимедійність, персоналізація, інтерактивність, відсутність посередників і прямий доступ до інформації тощо. Однак, актуальним залишається питання щодо керованості усім масивом і контентом ЗМК, ЗМІ й Internet в інформаційно-комунікативному просторі вищої школи. Австрійський професор, президент Міжнародної асоціації за прогрес Г. Кехлер¹¹ із тривогою наголошує на тому факті, що «internet-свобода» в епоху глобалізації приводить до появи деяких небезпечних рис «віртуальної громадськості», «віртуальної юрби», або «цифрової юрби», схожих з описаними ще в 1895 році Г. Лебоном такими психологічними рисами мас, як анонімність, імпульсивність, піддатливість до впливів, легковір'я, керованість свідомістю й поведінкою в інтересах груп, «ефект сніжного кома».

Таким чином, аксіосфера вишів, в яких виховуються студенти, які значну частину вільного часу витрачають на Internet й інші мережі, сьогодні являє собою досить суперечливу сферу, керовану лише почасти. В умовах часткової керованості комунікативного простору вищого навчального закладу й аксіосфери студентів особливо актуалізується культуро-творча модель вищої освіти, що синтезує кращі традиції в системі західної й вітчизняної освіти. Саме така модель заснована на взаємозалежних підходах антропоцентризму, культуро-центризму й соціоцентризму, і в центрі її перебуває людська особистість. Стратегія орієнтації й на культуру, і на суспільство, і на людей дасть можливість реалізувати вітчизняним вищим навчальним закладам макросоціальну, інновативну місію й стати інтелектуальними центрами об'єднання інститутів влади, бізнесу й громадянського суспільства.

Список використаних джерел:

1. *Бабосов Е.М.* Социология образования. Изменения содержания обучения // Новейший социологический словарь /Сост. А.А.Грицанов, В. Л. Абушенко и др. – Минск: книжный Дом, 2010, с. 1053-1055.

2. *Гнатюк О.Л.* Современные модели высшей школы Часть 1. Высшая школа сегодня: методология исследования // Вестник ЛГУ им А.С.Пушкина. Философия. 2014. Т.2, с.154-158.

¹¹ Кехлер Ганс (Hans Kochler) – Професор філософії Інсбрукського університету (Австрія), президент Міжнародної асоціації за прогрес.

РЕЗУЛЬТАТИ НАУКОВОЇ ДІЯЛЬНОСТІ ЯК ОБ'ЄКТИ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Чітке відокремлення результатів наукової діяльності від результатів науково-технічної діяльності необхідне при прийнятті рішень щодо фінансування наукових і науково-технічних досліджень, науковій, науково-технічній та судовій експертизі, таких результатів, визнанні цих результатів об'єктами права інтелектуальної власності, тощо. У той же час, в законах та підзаконних актах відсутні критерії, за якими можна було б чітко відокремити результати наукової діяльності від результатів науково-технічної діяльності.

Так, Закон України «Про наукову і науково-технічну діяльність» визначає, що «науковий результат—це нове наукове знання, одержане в процесі фундаментальних або прикладних наукових досліджень та зафіксоване на носіях інформації. Науковий результат може бути у формі звіту, опублікованої наукової статті, наукової доповіді, наукового повідомлення про науково-дослідну роботу, монографічного дослідження, наукового відкриття, проекту нормативно-правового акту, нормативного документа або науково-методичних документів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову, тощо». [1] Відмітимо, що носій інформації є матеріальним, а зафіксоване на ньому нове наукове знання – нематеріальним.

У цьому ж законі наведено визначення науково-технічного результату: «науково-технічний (прикладний) результат - одержані під час проведення прикладних наукових досліджень, науково-технічних (експериментальних) розробок нові або істотно вдосконалені матеріали, продукти, процеси, пристрої, технології, системи, нові або істотно вдосконалені послуги, введені в дію нові конструктивні чи технологічні рішення, завершені випробування, розробки, що впроваджені або можуть бути впроваджені в суспільну практику. Науково-технічний (прикладний) результат може бути у формі ескізного проекту, експериментального (дослідного) зразка або його діючої моделі, конструкторської або технологічної документації на науково-технічну продукцію, дослідного зразка, проекту нормативно-правового акту, нормативного документа або науково-методичних документів тощо» [1].

В останньому визначенні змішані два різновиди результатів. Матеріальні, до яких відносяться: матеріали, продукти, пристрої, введені в дію нові конструктивні чи технологічні рішення, експериментальні (дослідні) зразки або його діючі моделі. А також нематеріальні, що відображені на матеріальному носії: ескізні проекти, конструкторська або технологічна документація, проект нормативно-правового акту, нормативного документа або науково-методичних документів.

Для ясності, пропонуємо нематеріальні результати науково-технічної діяльності віднести до результатів наукової діяльності, а в переліку науково-

технічних результатів залишити тільки матеріальні результати. Розділення результатів наукової і науково-технічної діяльності на наукові результати і науково-технічні результати за принципом «матеріальне-нематеріальне» дозволить уникнути багатьох помилок при прийнятті управлінських рішень щодо фінансування і оцінки результатів наукових та науково-технічних проектів і програм.

Оцінка результатів наукової і науково-технічної діяльності здійснюється шляхом проведення наукової і науково-технічної експертизи. Однак, в статті 53 Закону України «Про наукову і науково-технічну експертизу», що носить назву: «Об'єкти наукової і науково-технічної експертизи» змішані наукові і науково-технічні результати експертизи, що не дає можливості експертам обґрунтовано вибрати критерії для їх оцінки, оскільки критерії для наукових об'єктів експертизи одні, а для науково-технічних – інші.[2]

Якщо вважати, що наукові результати є нематеріальними, тобто такими, що не мають лінійних розмірів і маси, хоча вони і відображені на матеріальному носії (на папері, електронному носії, тощо), та за законом повинні бути новими, а за своєю сутністю - результатами інтелектуальної, творчої діяльності, то у відповідності до законодавства України про інтелектуальну власність, наукові результати повинні визнаватися об'єктами права інтелектуальної власності.[1] У той же час науково-технічні результати не є об'єктами права інтелектуальної власності, оскільки вони матеріальні, незважаючи на те, що у своєму складі вони можуть містити об'єкти права інтелектуальної власності.

Список використаних джерел:

1. Закон України «Про наукову і науково-технічну діяльність» (Відомості Верховної Ради (ВВР), 2016, № 3, ст.25).

2. Закон України «Про наукову і науково-технічну експертизу» (№52/95-ВР від 10.02.95).

Розділ 6

НАПРЯМИ РОЗВИТКУ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА В ІНФОРМАЦІЙНІЙ СФЕРІ

*Лук'янчиков Є. Д., д.ю.н., професор
ФСП КПІ ім. Ігоря Сікорського.*

НЕГЛАСНІ СЛІДЧІ (РОЗШУКОВІ) ДІЇ - ЗАСОБИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ

Сучасна злочинність характеризується не тільки кількісними, а більшою мірою якісними змінами. З'являються нові види злочинів (у сфері високих технологій, розкрадання в бюджетній та фінансово-кредитній сферах), зростає корисливо-насильницька злочинність, дії злочинців стають жорстокими та зухвалими, підвищується професіоналізація, організованість та корумпованість

злочинності. З різних обставин, у тому числі недовіра правоохоронним органам, знижується активність законослухняних громадян у наданні цим органам інформації про злочини. Суттєве зростання навантаження на правоохоронні органи і збільшення кількості злочинів, що залишаються нерозкритими є об'єктивною передумовою подальших пошуків, розроблення і застосування нових пізнавальних засобів і прийомів роботи з джерелами інформації про обставини злочинів, які перебувають у провадженні слідчого.

Зважаючи на сучасний характер злочинності, необхідність своєчасного виявлення злочинів, що готуються та розслідування вже вчинених, законодавець суттєво розширив засоби пізнавальної діяльності. Чинний КПК України містить главу 21, яка регулює порядок проведення негласних слідчих (розшукових) дій.

Оцінюючи зміни, що відбулися у КПК України А. Солодков зазначає, що до нього імплементовано європейські стандарти у галузі захисту прав людини ..., які багаторічною практикою застосування в європейських країнах довели свою ефективність [1, с. 55-56]. Значною мірою це стосується інституту слідчих (розшукових) дій, який зберіг основні засоби отримання інформації про обставини злочину та запровадив новий інститут засобів пізнавальної діяльності з розслідування – негласні (слідчі) розшукові дії.

Слідчі дії – один з устелених інститутів кримінального процесу. Витоки їх нормативного закріплення та врегулювання містяться у Зводі законів Російської імперії 1857 р. (ст. ст. 21, 197, 356, 360, 376, 377 та ін.), Статуті кримінального судочинства 1864 р. (ст. ст. 250-258, 292, 294, 468, 1158 та ін.), в яких безпосередньо мова іде про загальні положення проведення слідчих дій. Ряд інших норм присвячено допиту, очній ставці, огляду, освідчуванню, обшуку тощо. Аналіз їхнього змісту дозволяє дійти висновку, що усі вони спрямовані на пошук джерел інформації про злочин та їх дослідження. Тобто усі вони мають пошукову, пізнавальну спрямованість. Так, в ст. 254 Статуту кримінального судочинства про розшук згадується у наступному контексті «при проведенні дізнання поліція усі потрібні їй відомості збирає шляхом *розшуків*, словесними розпитуваннями та негласним спостереженням» (виділено – Є. Л.). Розшук покладался на поліцію, але його сутність не розкривалася, перелік дій, які мали охоплюватися цим поняттям не наводився. Крім того, жоден із попередніх нормативних актів, окрім назви (слідчі дії), не надавав визначення таких дій, що сприяло формуванню серед науковців різних поглядів на їхню сутність та віднесення тих або інших процесуальних дій до слідчих.

В результаті тривалих дискусій науковцями було сформовано визначення слідчих дій. Під ними розуміють передбачені кримінально-процесуальним законом дії, спрямовані на отримання (розшукування, збирання), або перевірку вже отриманих доказів у конкретному кримінальному провадженні. Вони є різновидом (частиною) більш широкого за змістом поняття процесуальних дій, проводяться уповноваженою особою у стадії досудового розслідування відповідно

з визначеними процедурними вимогами, мають пізнавальну спрямованість, тобто завжди спрямовані на отримання, фіксацію або перевірку доказів [2, с. 365].

Всі інші дії слідчого у кримінальному провадженні, слухно наголошує М. А. Погорецький, хоча вони є процесуальними, оскільки здійснюються уповноваженим суб'єктом процесу у визначеній КПК України процесуальній формі й спрямовані на досягнення мети вирішення завдань кримінального провадження, проте не мають значення слідчих (розшукових) дій [3, с. 49].

Аналізуючи поняття слідчі (розшукові) дії слід звернути увагу на те, що таке їх визначення є новелою чинного КПК України. Тривалий час законодавство, теорія та практика користувались поняттям слідчі дії, проведено відповідні дослідження для визначення його змісту та сутності. Відмінності поняття слідчі (розшукові) дії від попереднього «слідчі дії» законодавець, як і зазвичай, не наводить. Науковцям залишається невдячна робота, спробувати здогадатися про думки законодавця, та обґрунтувати, чому традиційні слідчі дії набули назви розшукові.

Аналіз кримінального-процесуального законодавства окремих країн (Грузії, Естонської Республіки, Киргизької Республіки, Молдови, Республіки Білорусь, РФ, ФРН) показав, що у деяких з них йдеться не про «слідчі дії», а про засоби і методи доказування. В окремих КПК йдеться про слідчі дії, але у жодному не зустрічається вказівка на «розшукові», незважаючи на те, що вони усі можуть застосовуватися для відшукування як відомих слідчому, так і невідомих до певного часу об'єктів, документів, відомостей. У такому разі постає питання, а чим не задовольнило розробників чинного КПК України традиційне визначення таких дій як слідчі без додаткового слова «розшукові».

Вперше в теорії криміналістики про право слідчого доручати органам дізнання проведення «окремих слідчих розшукових дій» згадує О. Н. Колесніченко [4, с. 352]. Таким чином, в науковому обігу більше ніж півстоліття тому з'являється нове словосполучення «слідчі розшукові дії». Цікаво, що таку назву сприйняли розробники нового КПК України, глава 20 якого має назву «Слідчі (розшукові) дії». В статті 3 цього Кодексу «Визначення основних термінів», як і у попередньому КПК визначення слідчих дій не наводиться. Проте у ст. 223 зазначається, що ними є дії, спрямовані на отримання (збирання) доказів або перевірку вже отриманих доказів в конкретному кримінальному провадженні. Наголос робиться саме на пошуково-пізнавальний характер процесуальних дій, за яким їх відносять до слідчих (розшукових) дій.

Слід зазначити, що в теорії криміналістики проводиться розмежування між слідчою і розшуковою діяльністю. Р. С. Белкін вбачає її у тому, що метою розшукової діяльності є встановлення та виявлення злочину та злочинця, а метою розслідування – доказування факту вчинення злочину та вини злочинця. Одним із елементів розшукової діяльності слідчого він називає слідчі дії, та наголошує, що вони проводяться відносно відомих, встановлених об'єктів [5, с. 192-193].

Піддаючи аналізу пізнавальний інструментарій з розслідування злочинів, неможливо не відмітити, що чинний КПК України, з одного боку, суттєво розширює засоби одержання інформації слідчим, а з іншого, наділяє його правом застосування пізнавальних прийомів, що є притаманними оперативним підрозділам, за своєю сутністю вони нагадують оперативно-розшукові заходи, які назвали слідчими (розшуковими) діями. На цій підставі окремі науковці вважають, що відбулося часткове злиття кримінально-процесуального та оперативно-розшукового законодавства [6, с. 107]. Натомість М. Є. Шумило вказує на часткове об'єднання не законодавства, а поліційної (оперативно-розшукової) та процесуальної діяльності, що передбачає перевірку первинних даних про можливий злочин у сфері кримінального провадження під контролем кримінального процесуального закону з дотриманням його форм і гарантій [7, с. 228-229].

В свій час А. Я. Дубинський звертав увагу на те, що зрощування цих двох функцій (видів діяльності) неприпустимо, оскільки воно може негативно позначитися на оцінці доказів, об'єктивності розслідування, формуванні висновків у кримінальній справі [8, с. 89].

Разом з тим важко знайти роботу присвячену розкриттю злочинів, у якій не наводились рекомендації щодо організації взаємодії між слідчими і оперативними підрозділами правоохоронних органів. Вони торкалися порядку обміну інформацією, в першу чергу зібраною застосуванням оперативно-розшукових заходів на різних етапах досудового провадження.

Подібне ставлення до можливості і форм використання інформації, що отримана застосуванням оперативно-розшукових заходів певною мірою можна вважати виправданим. На той час сторона захисту була суттєво обмежена у збиранні і поданні відомостей на користь свого підзахисного.

На даний час можливості захисту змінилися і суттєво розширені у виявленні і поданні до суду джерел інформації на користь підзахисного. Крім того слід зазначити, що самостійність слідчого у прийнятті процесуальних рішень і проведенні слідчих дій суттєво обмежена.

На завершення слід зазначити, що пошуки сучасних ефективних засобів отримання інформації для розкриття злочинів з метою притягнення винних до відповідальності і поновлення порушених прав потерпілих будуть продовжуватися і надалі. Вже сьогодні КПК доповнено ст. 269-1 «Моніторинг банківських рахунків», розроблено пропозиції щодо доповнення глави 16 КПК параграфом «Заходи забезпечення кримінального провадження у сфері інформаційних технологій».

Список використаних джерел:

1. Солодков А. Забезпечення права на справедливий суд у кримінальному провадженні: окремі питання правозастосування. *Право України*. 2013. №11. С. 55-62.

2. Кримінальний процес: підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін.. ; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Х. : Право, 2013. 824 с.

3. Погорецький М. А. Поняття, зміст та структура кримінального процесу: проблеми теорії та практики. *Право України*. 2013. №11. С. 42-54.

4. Колесниченко А. Н. Розыск. *Криминалистика*. М. : Юридическая литература, 1963. С. 352-357.

5. Белкин Р. С. Криминалистическая энциклопедия. М. : Издательство БЕК, 1997. 342 с.

6. Ходанович В. О. Проведення негласних процесуальних дій за кримінально-процесуальним законодавством Німеччини, Швейцарії та Франції. *Вісник Академії адвокатури України*. К. : ВЦ Акадакатури України, 2016. Том 13. Число 3(37). С. 106-114.

7. Шумило М. Є. Поліційна і кримінально-процесуальна діяльність: на стику минулого і сучасного. *Вісник Академії адвокатури України* : наук. журн. К. : Акад. адвокатури України, 2015. Том 12. Число 2(33). С. 223-234.

8. Дубинский А. Я. Исполнение процессуальных решений следователя. *Правовые и организационные проблемы*. К. : Наукова думка, 1984. 182 с.

*Жиляєв І. Б., д.е.н., с.н.с.,
Семенченко А. І., доктор наук з
державного управління, професор,
Фурашев В. М., к.т.н., доцент, с.н.с.
ФСП КІІ ім. Ігоря Сікорського*

ГЕНЕЗА ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ УКРАЇНСЬКОЇ ІКТ-ПОЛІТИКИ

Мета статті: на основі аналізу іноземного та вітчизняного досвіду провести ретроспективний аналіз становлення та розвитку правової бази української політики у сфері ІКТ та довести необхідність (важливість) комплексного (інтегрального) правового регулювання ІКТ-сфери, більш широкого, ніж сформульовано у відповідних стратегічних актах з питань нормативного регулювання окремих сфер та напрямів ІКТ-політики.

Гіпотеза дослідження: В Україні сформована певна сукупність ІКТ-політик, кількість яких постійно збільшується, що стимулює активний розвиток їх правового забезпечення.

Вступ. Основними тенденціями кінця ХХ – початку ХХІ століть є:

- 1) швидкий розвиток ІКТ, що прискорюється;
- 2) ІКТ-розвиток вимагає створення відповідної системи національного та державного регулювання ІКТ-сфери (артикульованих у вигляді ІКТ-політики);
- 3) формування сукупності ІКТ-політик, кожна з яких регулює певний сегмент ІКТ-сфери;
- 4) бурхливий розвиток правового регулювання (нових «масивів» нормативно-правових актів) актуальних суспільних відносин, пов'язаних із

впровадженням новітніх ІКТ, що є важливим (вирішальним) елементом кожної ІКТ-політики.

1. Завдання аналізу концепцій українських ІКТ-політик:

- Виділити національні / державні ІКТ-політики в Україні – визначивши їх сукупність (ландшафт);
- Визначити відповідні методи та елементи аналізу;
- Дослідити динаміку розвитку правової бази ІКТ-політик за «життєвим циклом» та виявити закономірності їх розвитку.

2. Елементи аналізу української ІКТ-політики:

- *Основні:*
 - Концепції (напрями) української ІКТ-політики **К**;
 - Нормативно-правові акти (правова база) **Л**;
 - Фактор часу **Т**;
- *Додаткові:*
 - Завдання (заходи) **Р**;
 - Ресурси **Р**;
 - Результати (ефекти) **Е**.

Проведення ретроспективного аналізу систем правового забезпечення сукупності українських ІКТ-політик передбачає проведення кількісного та якісного аналізу на основі виділених елементів з формуванням двомірних та тримірних матриць залежності цих елементів.

Українське законодавство визначає «аналіз політики» як методику та практику демократичного урядування, що полягає у всебічному вивченні ситуації та визначенні проблеми у певній сфері (секторі) державного управління, аналізі її причин, визначенні альтернативних шляхів її розв'язання та виборі оптимальних рішень на основі оцінки впливу та із врахуванням позицій різних зацікавлених сторін¹².

3. Аналіз визначення змісту поняття «політика» в українському законодавстві (формулювання)

З розвитком суспільних та економічних відносин у певній сфері настає час юридично формалізувати (легітимізувати) цю сферу, сформувавши єдине бачення на політику. Зазначене зазвичай стимулює розвиток правової бази цієї політики.

В українському законодавстві не існує єдиного стандарту визначення змісту та складових поняття «політика». Кожного разу законодавець, конструюючи поняття «політика» у певній сфері суспільних та економічних відносин, виходить із деяких своїх уявлень щодо її змісту та складових.

Деякі вимоги щодо змісту, технології формування та реалізації державної політики центральними органами виконавчої влади встановлено регламентом уряду, згідно з яким: 1) забезпечення формування та реалізації державної політики у сферах віднесених до компетенції уряду здійснюється міністерствами;

¹² ПОРЯДОК ДІЯЛЬНОСТІ ГРУП АНАЛІЗУ ПОЛІТИКИ У ЦЕНТРАЛЬНИХ ОРГАНАХ ВИКОНАВЧОЇ ВЛАДИ, ЗАТВЕРДЖЕНИЙ НАКАЗОМ ГОЛОВДЕРЖСЛУЖБИ УКРАЇНИ ВІД 02.04.2010 № 91 [HTTP://ZAKON.RADA.GOV.UA/LAWS/SHOW/Z0309-10](http://zakon.rada.gov.ua/laws/show/z0309-10)

2) для вирішення питань суспільно-економічного життя, які потребують визначення концептуальних засад реалізації державної політики, пріоритетів та стратегічних напрямів соціально-економічного розвитку, послідовності дій, вибору оптимальних шляхів і способів розв'язання проблеми, проведення реформ, розробляються політичні пропозиції щодо реалізації державної політики; 3) концепція реалізації державної політики у відповідній сфері базується на оптимальному варіанті розв'язання проблеми та містить розділи: проблема, яка потребує розв'язання; мета і строки реалізації концепції; шляхи і способи розв'язання проблеми; очікувані результати; обсяг фінансових, матеріально-технічних, трудових ресурсів.¹³

4. Концепції (напрями) українських ІКТ-політик К

Поштовхом до формування української ІКТ-політики стало прийняття в 1998 році низки законів України про інформатизацію. В наступному, у зв'язку із новими проблемами в сфері ІКТ та артикуляцією нових поглядів на розв'язання цих проблем відокремлювались нові сегменти – формувалась сукупність ІКТ-політик (політика інформатизації була першоджерелом всіх наступних ІКТ-політик). Зазначені політичні рішення щодо концепцій розвиток ІКТ-сфери легітимізувались у базових нормативно-правових актах, які створювали «ядро» відповідної правової бази цих ІКТ-політик.

- **Інформатизація** (Національна програма інформатизації, три закони 1998) – 134 пов'язаних між собою акти;
- **Телекомунікації** (закон 2003) – 1985 актів;
- **Інформаційне суспільство** (Закон 2007; Стратегія 2013) – 76 актів;
- **Електронне урядування** (Концепції 2010; 2017) – 50 актів;
- **Відкритий Уряд** (Ініціатива «Партнерство «Відкритий Уряд» 2012) – 30 актів;
- **ІКТ-безпека: 1) інформаційна** (Доктрина, 2017) – 7 актів; 2) **комп'ютерна безпека** (2001, конвенція), яка у наступному отримала назву – **кібербезпека** (Стратегія, 2016; закон, 2018) – 32 акти; 3) **безпека інформаційних ресурсів**; 4) **безпека критичної інформаційної інфраструктури держави**¹⁴ (захист інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, зокрема – інформаційних технологій та телекомунікацій (електронних комунікацій)¹⁵;
- **Програмна продукція** (Закон, 2012) – 3 акти;
- **Цифрова економіка та суспільство** (концепція, 2018) – не виявлено пов'язаних актів;

¹³ РЕГЛАМЕНТ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ, ЗАТВЕРДЖЕНИЙ ПОСТАНОВОЮ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ВІД 18.07.2007 № 950 (У РЕДАКЦІЇ ПОСТАНОВИ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ВІД 09.11.2011 № 1156) [HTTP://ZAKON.RADA.GOV.UA/LAWS/SHOW/950-2007-п](http://zakon.rada.gov.ua/LAWS/show/950-2007-п)

¹⁴ Див.: ПОРЯДОК ФОРМУВАННЯ ПЕРЕЛІКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ, ЗАТВЕРДЖЕНИЙ ПОСТАНОВОЮ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ВІД 23 СЕРПНЯ 2016 Р. № 563

¹⁵ ПРИМІТКА: СУЧАСНОЮ ТЕНДЕНЦІЄЮ У СЕГМЕНТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІКТ-СФЕРИ Є УСКОПЛЕННЯ ТА ДЕТАЛІЗАЦІЯ ПО ОКРЕМИМ (БІЛЬШ-МЕНШ АВТОНОМНИМ) ВИДАМ ІКТ-БЕЗПЕКИ.

- **Пріоритети:** 1) **пріоритетні галузі економіки** (для інвестиційних цілей) – віднесено «виробництво нових та імпортозаміщуючих видів комп'ютерів, електронної та оптичної продукції, машин і устаткування» (закон 2012; постанова 2013); 2) **науково-технічні пріоритети** (закон 2001; постанова 2011) + програми; 3) **інноваційні пріоритети** (закон 2011, державні – постанови 2012, 2017; галузеві – постанова 2017) + державні програми з розвитку ІКТ;

- Галузеві та регіональні (територіальні) політики в сфері ІКТ;

5. Приклад 1: аналіз розвитку системи правового забезпечення визначеної української ІКТ-політики (на прикладі політики інформатизації)

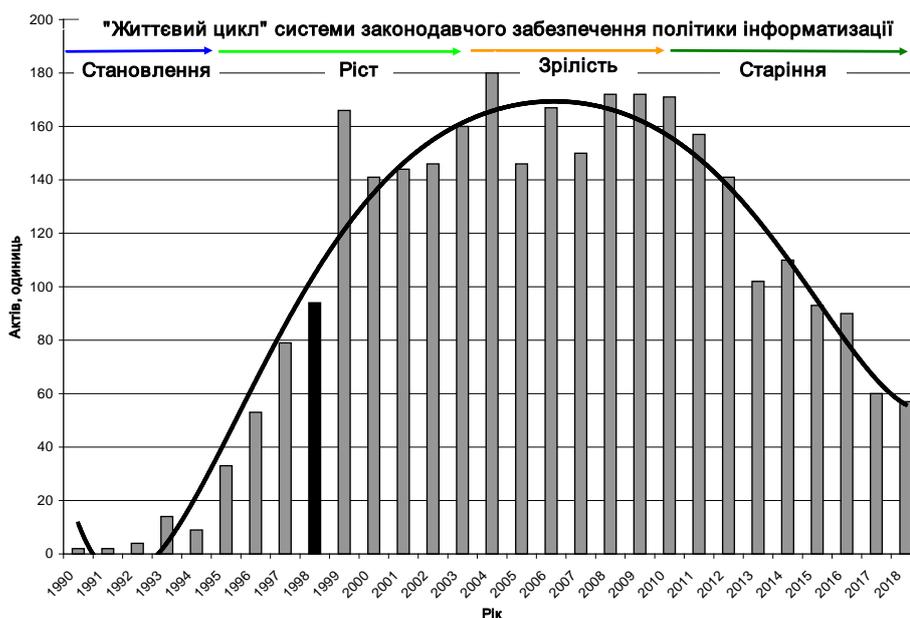
- Об'єкт: Національна програма інформатизації, 1998
- Термін аналізу: 1990-2018 РР.
- Масив нормативно-правових актів > 3000
- Кількісний аналіз динаміки

«Життєвий цикл» української політики інформатизації

Суспільна увага до певної державної / національної політики призводить до потреби формування відповідної правової основи для неї. Динаміка формування зазначеної правової бази також (окрім інших елементів політики) демонструє відповідний «життєвий цикл» цієї політики.

Яскравим прикладом є законодавча база української політики інформатизації, яка існує понад 20 років. На рис. 1 представлена нормативно-правова база з питань інформатизації (більш, ніж 3 тис. актів, згрупованих за роком їх прийняття), на якому можна чітко виділити чотири цикли цієї політики: 1990-1995 рр. – становлення; 1996-2003 рр. – стадія росту, 2004-2010 рр. – зрілість, 2011-2018 рр. старіння.

Рис. 1. Чисельність нормативно-правових актів політики що регулюють інформатизацію (з використанням терміну "інформатизація") у 1990-2018 рр. (за роком схвалення)



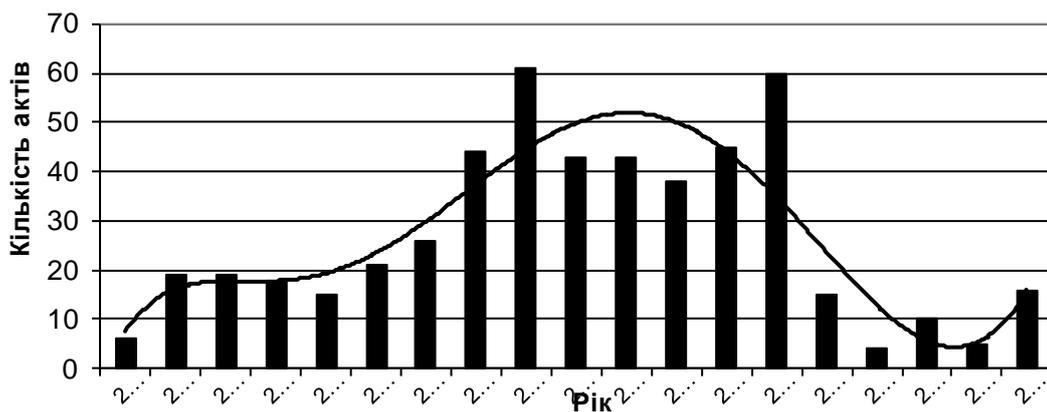
Джерело даних: База даних «Законодавство України» (станом на 18.10.2018)

6. Приклад 2: аналіз розвитку системи правового забезпечення визначеної європейської ІКТ-політики (на прикладі прийняття актів ЄС з інформаційного суспільства чи кібербезпеки)

Наявність «життєвого циклу» ІКТ-політики є притаманним явищем як для політиків у конкретних сферах економіки (у нашому прикладі – у сфері ІКТ), так й для конкретних країн.

На рис. 2 розглянуто, як змінювалась правова база європейської ІКТ-політики щодо інформаційного суспільства. В базі даних європейського права EUR-Lex станом на 24.10.2018 зафіксовано 510 документів щодо інформаційного суспільства, з них 403 акти європейського права. Можна бачити, що майже 2/3 документів європейського права щодо регулювання інформаційного суспільства було прийнято протягом 2007-2013 років (на стадії зрілості життєвого циклу цієї ІКТ-політики).

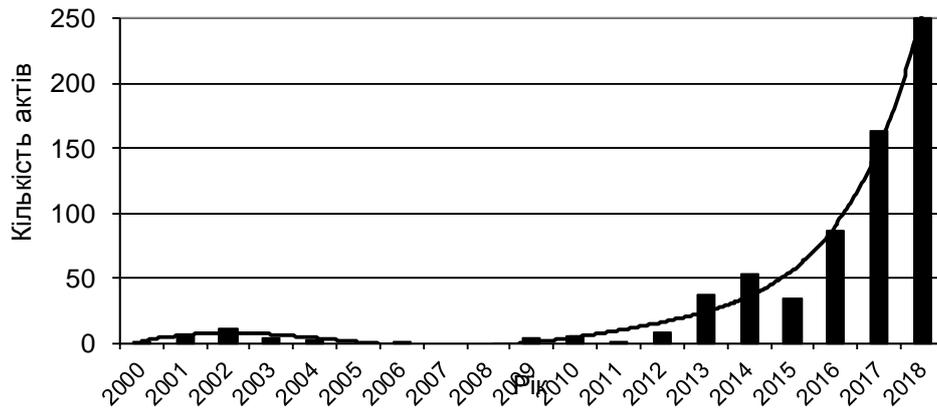
Рис. 2. Кількість актів європейського права з політики інформаційного суспільства (Information society), 2000-2018 рр.



Джерело даних: База даних «EUR-Lex» (станом на 24.10.2018)

По-іншому виглядає розвиток правової бази більш «молодої» європейської ІКТ-політики кібербезпеки (Cybersecurity). В базі даних європейського права EUR-Lex станом на 24.10.2018 зафіксовано 668 документів з питань кібербезпеки, з них 5953 акти європейського права. На рис. 3 можна бачити, що майже 2/3 документів європейського права з кібербезпеки було прийнято протягом 2017-2018 років (на стадії бурхливого росту життєвого циклу цієї ІКТ-політики). При цьому актуальність цієї проблеми примушує законотворця все інтенсивніше врегульовувати суспільні відносини у цій сфері.

Рис. 3. Кількість актів європейського права з політики кібербезпеки (Cybersecurity), 2000-2018 рр.



Джерело даних: База даних «EUR-Lex» (станом на 24.10.2018)

Висновки:

1. Україна достатньо динамічно формує ІКТ-політичний ландшафт, його правову базу.
2. Однак, сучасний ландшафт сукупності українських ІКТ-політик є:
 - фрагментарним – політики часто дублюють одне одну, використовують відмінні терміносистеми (несистемність та адитивність);
 - таким, що має «розриви» між ІКТ-політиками та «розриви» у ланцюжку їх життєвого циклу (від старту – створення до фінішу – утилізації);
 - таким, що динамічно змінюється, «відкидаючи» попередні ІКТ-політики, що є часто невиправданим;
 - змінним під впливом нових іноземних концепцій та ініціатив (залежним від ресурсів донорів);
 - проблемними з точки зору результативності / ефективності: існує «невідповідність амбіцій амуніції» (ресурсів, що виділяються поставленим цілям політики, втрата довіри до концепцій політики).

3. Бракує досліджень природи нових правових масивів, пов'язаних з появою нових ІКТ-політик; механізмів формування таких масивів, їх впливу на суспільні відносини, право, його систему та структуру, правозастосовну практику.

Пропозиції:

- розглянути необхідність формування інтегрованої національної ІКТ-політики; уніфікувати (формалізувати підходи) до змістовної частини формування та реалізації окремих ІКТ-політик;
- систематизувати нормативно-правові акти щодо регулювання ІКТ-сфери (усунення дублювання та суперечностей, формування єдиної терміносистеми, відміна застарілих актів тощо);

- забезпечити випереджаючу розробку правового регулювання суспільних відносин, пов'язаних із появою новітніх та прогнозованих ІКТ¹⁶, активізуючи імплементацію норм європейського права.

*Дранник В. А., викладач
ФСП КПІ ім. Ігоря Сікорського*

НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ СФЕРИ

З розвитком науки та техніки вельми актуальним сьогодні є розвиток новітніх інформаційних технологій.

Процес комунікації та отримання інформації займає важливе місце в житті кожної людини. Зараз, в вік нових інформаційних технологій, отримати будь-яку інформацію не становить складності. Сучасна людина проводить багато дій, що пов'язані з комунікацією, з подачею та отриманням інформації.

На протязі всього життя людини на неї ззовні відбувається інформаційний вплив, втручання до внутрішнього світу людини, подекуди навіть примус та маніпулювання, обумовлений створеною соціальною необхідністю, потребою для кар'єрного росту, професійного і соціального підтвердження визначеного статусу та інше. Але, з іншого боку, людина потребує інформації з огляду її жадоби до пізнання навколишнього світу, необхідності прояву людиною закладених у неї здібностей, соціального самоствердження тощо.

З огляду на важливість ролі комунікації та отримання інформації, на перший план постає ефективність обміну інформацією, від якої залежить розвиток людства та успішна діяльність кожної людини зокрема, у вирішенні глобальних та конкретних завдань тощо. Але в цьому процесі людина стикається з питаннями достовірності або не достовірності інформації та збереження чи розповсюдження без згоди її персональних даних.

Постає проблема складності у розпізнаванні достовірності інформації та захисту персональних даних, а також моральність та етика в інформаційних технологіях, що потребує нагального вирішення.

Подальші напрями розвитку цієї теми можуть бути направлені на розвиток інформаційної безпеки, а саме, забезпечення виконання вимог щодо контролю за коректним використанням персональних даних особистості та нерозповсюдження їх там, де законом це не передбачено. Також, звернути особливу увагу на підвищення рівня інформаційної культури (мораль і етика) людства у питаннях обміну та розповсюдження інформації.

¹⁶ ТРАДИЦІЙНО ТЕОРІЯ ПРАВА ВІДНОСИТЬ ДО СФЕРИ ПРАВОВОГО РЕГУЛЮВАННЯ СУСПІЛЬНІ ВІДНОСИТИ, ЯКІ: 1) МОЖУТЬ І ПОВИННІ БУТИ Є ВРЕГУЛЬОВАНИМИ; 2) МОЖУТЬ І ПОВИННІ БУТИ ТА Є НЕВРЕГУЛЬОВАНИМИ. ЦИФРОВА ЕПОХА ПОТРЕБУЄ ПРАВОВОГО ВРЕГУЛЮВАННЯ НОВОЇ ГРУПИ ВІДНОСИН – ЯКІ ПОВИННІ БУТИ, АЛЕ НА СУЧАСНОМУ ЕТАПІ НЕ МОЖУТЬ БУТИ ВРЕГУЛЬОВАНІ ПРАВОМ.

*Соснін О. В., д.п.н., професор,
заслужений діяч науки і техніки України,
Інститут держави і права ім. В. М.
Корецького НАН України,
Повидиш В. В., аспірант Національного
юридичного університету імені Ярослава
Мудрого, м. Харків*

ТЕХНОКРАТИЧНА РЕАЛЬНІСТЬ ПРАВОВИХ ПРОБЛЕМ ВИБУДОВИ СУЧАСНОГО ІНФОРМАЦІЙНОГО ПРАВА

Актуальність проблем правової і моральної регуляції інформаційно-комунікаційних процесів і інформаційно-комунікаційної діяльності взагалі постійно зростає в зв'язку із впровадженням новітніх систем електронного управління в державних і комерційних установах. Зрозуміло, що на тлі процесів становлення інформаційного суспільства виникають і нові виклики, як то: кібертероризм, інформаційні війни, «цифрова нерівність» в правах і свободах громадян при користуванні інформацією і ресурсами глобальних мереж. Особливої уваги потребує захист персональних даних громадян, дітей в онлайн-середовищі тощо. Вирішення багатьох політико-правових проблем вимагають і багато інших проблем, які пов'язано із процесами інформатизації суспільства, скажімо, в процесі самоорганізації населення всередині різноманітних груп і співтовариств за допомогою сучасних інформаційно-комунікаційних технологій (ІКТ). Віртуальна електронна комунікація підштовхує всіх учасників до вироблення строго нормованих юридичних норм і правил при використанні культурних або моральних норм в мережевій взаємодії. На тлі процесів впровадження міжнародних кодексів (ООН, ЮНЕСКО та ін.) і, відповідно, стандартів, які задають орієнтири світу, що інформатизується, процес набуває обертів і в Україні. Вчені-гуманітарії і правознавці зокрема приймають активну участь в цих процесах соціалізації, виховання та утворення нової організаційно-правової культури спілкування в оцифрованому світі. Без неї ми не бачимо майбутнього функціонування нового інформаційно-комунікаційного середовища людства, в якому воно вступає в XXI століття, ініціюючи гуманітарні експертизи і норми етичного аналізу розвитку при впровадженні високих технологій майбутнього. На них суспільство покладає завдання своєчасно оцінювати глобальність, економічну ефективність і взагалі оцінку систем ціннісних пріоритетів в сучасному світі.

Сучасна наука виділяє такі найважливіші ознаки комунікації, як то: глобальність, анонімність, дистанційність, миттєве поширення, дискриптивність (ліберальність) контенту і його доступність для всіх користувачів інформаційно-комунікаційних мереж і сховищ інформації без обмеження. Незважаючи на існуючі мережеві правила, адміністрування і прийняття міжнародних кодексів, які регулюють процеси в кіберпросторі, інформаційно-етична регламентація поки що відбувається майже спонтанно. Багато оголошених правил соціально-мережевого

спілкування формуються, безумовно, як зони «свободи» при цьому часто фактично пропонується інформувати як декларацію свободи від моралі. Виникають навіть морально-правові парадокси: стеження за повідомленнями, перехоплення і збору даних про особу тощо. Часто все це відбувається начебто «з метою захисту права на» ..., однак, порушуючи норми недоторканності особистого життя, і вступають в протиріччя із існуючими нормами захисту інформації. Фактами незаконного оприлюднення інформації, кібератаками, «тролінгом», хакерством, «піратством» та іншими формами девіантної поведінки¹⁷ наповнено наше інформаційно-комунікаційне середовище. Українським законодавством поки що не регулюють морально-етичні колізії, а застосування правових норм сильно ускладнено. Це означає, що формування інформаційного права є тривалим процесом і потребує значних інтелектуальних сил суспільства в процесі формування єдиних глобальних норм інформаційної безпеки.

Всі запропоновані за останні десятиліття моделі і комплексні теорії безпеки комунікації і захисту інформації намагаються обґрунтувати (прояснити) природу і сутність інформації – її генезис і способи пізнання визначають і актуальність нового наукового напрямку в структурі наукового знання – філософії інформації, вимагаючи регламентації процесів функціонування інформації на рівні прийняття законів і документів різного рівня: від глобальних до регіональних і місцевого самоврядування зокрема, аж до визначення «благ і зла Internet», його своєрідної «естетики» норм практичного застосування в сучасному споживацькому світі на всіх рівнях.

Предметність зростаючих проблем впровадження нових систем обміну і контролю, скажімо, в процесі державних закупівель в сучасному інформаційно-комунікативному просторі, безумовно, стають турботою юридичних наук і потребують спеціального вивчення. Огляд низки робіт, присвячених цій темі, дозволяє бачити чисельні виявлені в процесі наукових розвідок особливості, кожна з яких пов'язана з природою інформації.

У практичному плані інформаційно-комунікативний простір України виявляється достатньо засміченим, а інформація на окремих напрямках в диспозиціях різних каналів комунікації, засобів і способів генерування, поширення (передачі) і використання інформації та комунікативних повідомлень стає вразливим для агресивних дій, оскільки сам феномен комунікації трактують по-різному, часто розуміючи його як «широкосмугову» соціально-культурну взаємодію.

Комунікація, безумовно, є конституюючим¹⁸ процесом. У загальному плані вона є засобом людського існування, основним соціальним процесом, в якому

¹⁷Девіантність, девіантна (від лат. DEVIATION – відхилення) - це незвичайне, але при цьому стійке відхилення від статистичних норм. Іншими словами, девіантною вважається стійкий образ дій, поведінки або мислення, який не типовий для загальної популяції. Девіантна поведінка – тип соціальної поведінки, який суперечить прийнятим у даному суспільстві правовим, моральним, соціальним нормам і стереотипам.

¹⁸Конституювати - установлювати, визначати склад, зміст чого-небудь. *Конституювати президію конференції.* Словник української мови: в 11 томах. — Том 4, 1973. — Стор. 266.

людина взаємодіє з іншими людьми, створюючи соціальні світи і простори. Комунікації, як феномену інформаційно-сислової взаємодії, на сьогодні, присвячено багато досліджень, які пов'язано, зокрема, з необхідністю розширення концептуальних і предметних меж розгляду цього феномену. Змістовний і соціокультурний аспекти комунікації сьогодні більш ґрунтовно розкриваються, коли акцентується увага на значенні медіа і медіасфери в сучасному суспільстві. Однак, з цього починаються багато інших процесів обміну інформації, які пов'язано із глобальною інформатизацією. Вони разом із медіа формують довгі соціальні мережі, структури і процеси, схеми соціально-культурної взаємодії тощо, а різноманіття комунікації обумовлює неоднорідність комунікативного простору в функціональному аспекті. Аспекти неоднорідності інформаційно-комунікативного простору проявляються в багатьох практиках інформаційно-сислових взаємодій в сучасному соціумі. Вони відрізняються не тільки масштабами і об'єктною основою, але часто належать до різних видів реальності (речова, віртуальна, мережева), де не тільки якісно різні просторові метрики інформації, але й різна відповідальність за її збереження, або інший тип простору.

Правова теорія інформаційно-комунікаційних відносин, як область наукових знань, не дуже давно з'явилася у порівнянні з іншими напрямками гуманітарних знань, однак, дуже динамічно вивчає зміни, що відбуваються в житті сучасного суспільства під впливом інформатизації. До найпростішого розуміння комунікації як акту передачі інформації додалися три основні підходи вивчення предмета. В основі першого підходу лежить лінійна перспектива передачі інформації, яка вважає/вбачає, що правильна побудова процесу комунікації приведе до бажаного ефекту. Цей підхід має тенденцію зосереджуватись на ефектах комунікації. Другий – розглядає комунікацію як виробництво й обмін знаннями. Це пов'язано зі створенням повідомлень із використанням знакових систем і процесом добування знань із повідомлень. (Інтерпретація може привести до різних дієвих результатів.) Третій – вивчає те, як ми використовуємо комунікації в розбудові нашої соціально-економічної реальності. Тут виділяють різні способи нашого спілкування з людьми, постійний пошук й обмін ідеями як цінностями, які, впливаючи на нас, зокрема підсилюють, або руйнують нашу ідентичність, розглядаючи комунікацію як основну й обов'язкову умову існування людини в будь-якому суспільстві. Інформація всюди розглядається в самому широкому сенсі, включаючи думки, ідеї й емоції. Людина як соціальна істота постійно комунікує, використовуючи слова, невербальні жести, знаки й символи.

Сьогодні нагальною проблемою, на наш погляд, стає необхідність розробки нових підходів до вивчення сенсу правових процесів при роботі із змістовною інформацією в існуючих системах комунікації. На необхідність змін, доповнень та теоретичних пояснень впливають, головним чином, зміни, які відбуваються сьогодні в сфері розвитку та застосуванні нових можливостей інформаційно-

комунікаційних технологій, відкриваючи широкий простір для співпраці гуманітарних і юридичних наук із інженерно-технічними.

*Цирфа Г. О., к.і.н., доцент
ФСП КПІ ім. Ігоря Сікорського*

ПРАВО НА ОТРИМАННЯ ІНФОРМАЦІЙНИХ ПОСЛУГ У СОЦІАЛЬНІЙ СФЕРІ: ПРОБЛЕМИ Й ІННОВАЦІЙНІ ПЕРСПЕКТИВИ

На законодавчому рівні правовий режим інформаційних послуг в Українській державі знаходиться в стадії формування. Зрозуміло, що такі послуги повинні мати особливий правовий режим і особливі форми їх надання.

У соціальній сфері види соціальних послуг та форми їх надання визначає стаття 5 Закону України від 19 червня 2003 року № 966-IV «Про соціальні послуги». До видів соціальних послуг, зокрема, таких як: соціально-побутові, психологічні, соціально-педагогічні, соціально-медичні, соціально-економічні, з працевлаштування та юридичні послуги, законодавець відносить і *інформаційні послуги*. Виходячи з абзацу 10 цієї статті, *інформаційні послуги* – це надання інформації, необхідної для вирішення складної життєвої ситуації (довідкові послуги); розповсюдження просвітницьких та культурно-освітніх знань (просвітницькі послуги); поширення об'єктивної інформації про споживчі властивості та види соціальних послуг, формування певних уявлень і ставлення суспільства до соціальних проблем (рекламно-пропагандистські послуги).

Основними формами надання соціальних послуг є матеріальна допомога та соціальне обслуговування, механізм надання яких прописаний у чисельних законодавчо-нормативних актах, які регламентують забезпечення виконання загальнодержавних, галузевих і регіональних програм та відповідних норм законодавства у сфері інформування та комунікації.

Наразі постає питання: чи можна вважати сучасну національну систему нормативно-правових баз України в галузі соціального захисту та соціального забезпечення ефективною, сучасною та максимально наближеною до потреб кожного українця як у місті, так і в селі? Чи є достатньою інформація, яка надається споживачеві з боку державних органів, основними з яких виступають територіальні центри соціального обслуговування? Чи достатньо продуманими є стратегії соціальної політики нашої держави? Щоб відповісти на ці запитання, необхідно поставити ще одне важливе запитання: чи можна де-факто назвати Україну соціальною державою, як це проголошує принципове положення Конституції?

На Заході термін «Соціальна держава» увійшов у політичний обіг у 50-х роках минулого століття. Наближено до такого розуміння сформулював це поняття наш співвітчизник, соціолог В.Жмир. За його визначенням соціальною вважається держава, що послідовно проводить політику, спрямовану на захист

прав людини. У такому розумінні термін «Соціальна держава» увійшов і в Основний наш Закон – Конституцію України (ст. 1).

Соціальна політика - це, безумовно, феномен людини, показник його комфортності. Отже, в соціальній державі імператив цінності людини повинен бути на першому місці. Виходячи з цього тезису, українські чиновники - керівники будь-якої державної адміністрації та місцевого самоуправління повинні більш детально аналізувати нагальні соціальні проблеми і при цьому дослуховуватись до думки споживачів, а не діяти на власний розсуд, самовпевнено вважаючи, що мають «великий досвід». Людина зі свого боку прагне якнайшвидше вийти зі складної життєвої ситуації, що склалася, і відтак їй потрібна інформація як це зробити. Тобто, їй потрібна фахова допомога. Цю допомогу на сьогодні поряд із територіальними центрами соціального обслуговування надають і в інших відповідних установах: управліннях міністерства соціальної політики, пенсійних фондах, фонді соціального страхування, центрах комплексної реабілітації для осіб з інвалідністю, центрах молоді і сім'ї тощо. Проблемою, вважає автор цієї статті, є той факт, що в цих державних установах таку допомогу в більшості надають посадові особи, які не мають відповідної фахової освіти. І доволі часто, звернення до відповідної установи залишає у людини досить неприємний осадок і думку: «краще б я не звертався до цієї установи». У такому випадку на людину впливає і недобросовісне ставлення з боку посадовця, і якісь психологічні моменти, а головне – отримання неякісної, непрофесійної інформації.

Поряд із цим в деяких сферах відчувається катастрофічний брак інформації (можна сказати «інформаційний голод»). Часто людина зі своєю проблемою (наприклад, якщо йдеться про батьків дитини з фізичним чи психічним відхиленням) не може розібратись, зокрема, до якого типу соціальних центрів їй звернутись, які, скажімо, методи реабілітації існують тощо. Також слід зазначити, що в рамках існуючої соціальної політики на сьогодні, на жаль, поки що не бачать для себе кращого майбутнього і самі люди з особливими потребами.

В нашій країні, особливо в останні роки, різні люди (з власної ініціативи, з власного покликання) збирають пакунки, речі та багато іншого для людей, які потрапили в біду, а ще більш можна говорити про те, яка допомога від небайдужих людей (від тих хто має, і хто не має грошей) надходить нашим військовим. Ці люди (як правило волонтери) перебирають на себе обов'язки державних установ, які безпосередньо повинні займатись цими питаннями. Власне, волонтери стали соціальними працівниками, тільки вони це роблять стихійно, тоді як такі повноваження повинні належати професіоналам.

Соціальний працівник - це, в першу чергу, соціальний менеджер, це керівник, який керує ситуацією у суспільстві. Власно кажучи відверто: керівники будь-якої державної адміністрації, керівники місцевого самоуправління повинні мати освіту соціального працівника, тому що саме вони і є соціальними працівниками. Соціальний працівник - поняття багатогранне, тому що саме він

повинен розуміти всі процеси, які відбуваються у суспільстві. Соціальний працівник не тільки менеджер, як вже було зазначено, він і психолог, і педагог, тому що він працює з людьми (з молоддю, з дітьми), для роботи з якими потрібні саме такі знання; до того ж він ще і консультант і у першу чергу з правових питань соціального захисту і соціального забезпечення, тобто він повинен знати політику держави у цій сфері і відповідні норми законодавства, щоб надати професійну допомогу відповідним верствам населення. І, нарешті, роботу соціального працівника, безумовно, можна порівняти з роботою лікаря. Лікар лікує фізичні (тілесні) хвороби, соціальний працівник в свою чергу працює над лікуванням хвороби у суспільстві. У цьому зв'язку, безперечно, необхідно слід вважати спеціальність 231 «Соціальна робота». Галузь знань «Соціальна робота» передбачає навчання за спеціальностями: соціальна робота, соціальне забезпечення. На сьогодні все більше вищих навчальних закладів готують фахівців за цією спеціальністю. У цьому зв'язку, на думку автора статті, якісно новий рівень у соціальному розвитку суспільства можна досягти в першу чергу, виходячи з професійного підходу до соціальних проблем. Професіоналізм завжди націлений на вирішення певних завдань впровадження інновацій.

Інтеграція України в європростір потребує інновацій і у сфері соціальних послуг. Інноваційний розвиток соціальних послуг має ґрунтуватися на інформаційно-комунікаційних технологіях, ефективній системі обміну інформацією. В національній доповіді «Інноваційна Україна 2020», підготовленій Національною академією наук, визначені основні шляхи інноваційного розвитку соціальних послуг. Серед інших визначимо, зокрема, такі: всі види допомоги, субсидій, пільг та соціальних послуг мають бути поєднані у загальну (комплексну) систему. Будь-який вид підтримки у цій системі має надаватися, зважаючи на реальні потреби та конкретні життєві обставини, а не визначатися винятково статусом та/або доходом; має бути налагоджена співпраця та обмін інформацією між усіма органами, що задіяні у роботі з клієнтами (органами соціального захисту, службою зайнятості, освітніми та медичними закладами, органами правопорядку, недержавними організаціями з надання соціальних послуг) [1].

В останні роки в нашій державі досить інтенсивно впроваджуються все нові, і нові інформаційні Internet сервіси, які починають охоплювати нові аспекти життєдіяльності наших громадян. У соціальній сфері це сприяє застосуванню нових технологій у виявленні та обліку самотніх непрацездатних малозабезпечених громадян, які мають право на надання соціальних послуг, вдосконаленню організації надання соціальних послуг, з метою підтримання життєдіяльності громадян, які не здатні до самообслуговування у зв'язку з похилим віком, інвалідністю, хворобою, інших категорій осіб.

Проблемні питання підвищення надання інформаційних послуг актуалізуються в програмах розвитку місцевого самоврядування. Реалізація таких програм дозволить досягти: створення прозорої системи прийняття управлінських

рішень органом місцевого самоврядування, підвищення рівня довіри до органу місцевого самоврядування; створення єдиної системи інформаційно-аналітичного забезпечення діяльності органів місцевого самоврядування, підвищення якості та оперативного інформування; розповсюдження позитивного досвіду діяльності органів місцевого самоврядування всіх рівнів, спрямованого на поступовий комплексний соціально-економічний розвиток; підвищення рівня інформованості та правової освіти тощо[2].

Справедливості ради слід зазначити, що окремі українські міськадміністрації, завдяки новаторським підходам до роботи та глобальним баченням перспектив, у своїх містах вже запроваджують соціальні інновації. Фахівцями міськадміністрацій вивчається і впроваджується кращий міжнародний досвід, нові технології соціальної роботи, що вимагає як адаптації до українських реалій, так і наукового обґрунтування й доопрацювання нових впроваджень.

Отже, нові умови існування органів місцевої влади вимагають правового, методичного, кадрового та інформаційного забезпечення органів місцевого самоврядування. Підсумовуючи вищезазначене, вважаємо за необхідне встановити в Українській державі на законодавчому рівні особливий правовий режим інформаційних послуг.

Список використаних джерел:

1. Інноваційна Україна 2020 : національна доповідь / за заг. ред. В.М. Гейця та ін.; НАН України. – К., 2015. – 336 с.

2. Про затвердження Програми підтримки органів місцевого самоврядування та сприяння реалізації ініційованих проектів, спрямованих на соціально-економічний розвиток громади на 2018-2020 роки. URL: <https://chervonenska-gromada.gov.ua/>

*Мищенко О. О., студент
ФСП КПІ ім. Ігоря Сікорського*

Науковий керівник:

*Фурашев В. М., к.т.н., с.н.с., доцент
ФСП КПІ ім. Ігоря Сікорського*

ПРОБЛЕМИ ІНФОРМАЦІЙНИХ ПРАВОВІДНОСИН В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Стаття присвячена висвітленню сутності поняття «гібридна війна» та її впливу на інформаційні правовідносини.

Ключові слова: інформаційні правовідносини, гібридна війна, правове регулювання, агресор, інформаційний простір, ЗМІ

Постановка проблеми. З початку 2014 року України перебуває в стані не оголошеної війни. Анексія АР Крим, збройний конфлікт в Луганській та Донецькій областях України вперше за період незалежності показали реальні проблеми держави в системі національної інформаційної безпеки. Нездатність держави забезпечити надійний інформаційний простір і правове регулювання

інформаційних відносин в умовах війни, що в міжнародному осередку набула назви «гібридна війна» та являє собою перш за все війну на інформаційному рівні, ставить перед собою необхідність одного з найголовніших пріоритетів наукового дослідження. Подальше вивчення феномену гібридної війни та її впливу на інформаційні правовідносини дозволить розробити ефективну систему законодавчого регулювання інформаційних відносин та забезпечити належний рівень їх захисту.

Виклад основного матеріалу. В умовах знаходження України у стані гібридної війни, основною складовою якої є інформаційна війна, інформаційне поле держави піддається різноманітним загрозам, серед яких незаконний збір інформації, поширення дезінформації, засоби пропаганди, зміна інформаційної якості та порушення інформаційної безпеки в цілому. Регуляція процесів поширення та захисту інформації, забезпечення передбаченого нормами міжнародного та національного права вільного доступу до інформації, як ніколи потребує змін, корекції, доповнень та законодавчого закріплення відповідно до викликів, що постають в суспільних відносинах.

Поняття «гібридна війна» одним із перших став застосовувати американський дослідник М. Маклюен, який у своїх працях аналізував роль інформації в сучасному світі. У своїх дослідження вчений дійшов до висновку, що істинно тотальна війна – це війна за допомогою інформації. На основі власних досліджень він довів, що сучасні війни зазвичай ведуться в інформаційному просторі та за допомогою інформаційних видів озброєнь [1, с. 202].

Полковник генерального штабу Збройних Сил Німеччини у відставці Родеріх Кізеветтер описує визначення терміну «гібридна війна» як: «Комбінація класических военных элементов и массивной обработки общественности, то есть, пропаганды и дезинформации. Все это дополняется невоенными методами: требованием выборов, захватом телецентров, использованием социальных сетей, телевидения и радио для распространения дезинформации. А в переговорах идти на уступки ровно настолько, чтобы сохранить лицо и, одновременно, дать своим силам возможность сделать еще шаг вперед за рамки соглашений» [2].

Гібридна війна різко відрізняється від поняття війни в загальному розумінні, головний напрям ведення гібридної війни не зосереджується на збройному конфлікті, а перш за все націлений на інформаційний простір.

Засобами ведення гібридної війни в інформаційному полі є будь-які засоби передачі інформації — ЗМІ, комп'ютерні мережі, поштова агітація і навіть розповсюдження пліток серед інформаційно не захищеного населення тощо.

Інформаційний вплив в умовах гібридної війни зосереджується на вигідному стороні агресора спотворенні фактів та їх нав'язуванні іншій стороні.

Швейцарські дослідники у сфері державної безпеки Марі Безнер та Патріс Робін у своїй праці «Кібернетична та інформаційна війна в українському конфлікті» пояснюють, що внаслідок кібернетичної та інформаційної війни, яку веде Росія проти України, жителі окупованої частини східної України та

анексованого Росією Криму стали «повністю ізольованими від інформації, що надходить із зовнішнього світу», адже вони мають доступ лише до російського радіо та телебачення. «Підтримання ізоляції є важливою частиною російської інформаційної війни, метою якої є контролювати думку громадськості та впливати на її рішення на користь Росії», йдеться у дослідженні [3].

Російська пропагандистська діяльність відбувається з використанням усіх каналів передачі інформації, серед яких телебачення, друковані ЗМІ і звичайно інтернет мережі, що дозволяє донести пропаганду до великої кількості людей. При цьому використання відкритих соціальних мереж, форумів та чатів, що не мають засобів перевірки і сортування інформації, роблять її поширення ще більшим та не регульованим.

Під час розгортання подій в Криму та на сході України Росією було вжито всі можливі заходи, щодо ізоляції цих територій з метою не допущення іноземних ЗМІ для отримання об'єктивної інформації про ці події. «Той факт, що західні ЗМІ не могли підтвердити присутність російських військових в Україні протягом майже усього 2014 року», у свою чергу, вказує на значний прогрес в російській інформаційній тактиці. Як зазначають дослідники, Росія використовує тактику «забруднення інформаційних каналів», щоб ввести зовнішній світ в оману [3].

Підірив якості інформаційного простору ускладнює прийняття найважливіших політичних рішень і при виробленні державної політики призводить до значного зменшення авторитету органів державної влади в суспільстві та на міжнародній арені, порушення функціонування системи державного управління і контролю.

З метою запобігання незаконного впливу на інформаційний простір України починаючи з 2014 року інформаційна політика держави почала новий напрям розвитку та реформування.

Відповідно до постанови Верховної ради України від 2 грудня 2014 року було створено Міністерство інформаційної політики.

Судовими рішеннями за позовом Національної ради з питань телебачення і радіомовлення у березні-серпні 2014 р. було зупинено ретрансляцію на території України 14 російських пропагандистських телеканалів: «Первый канал. Всемирная сеть»; «ртр-Планета»; «россия 24»; «НТВ-Мир»; «тVCI (тВ центр)»; «россия 1»; «НТВ»; «тНт»; «Петербург 5»; «Звезда»; «реН-тВ»; «Life News»; «Russia Today»; «рбк-т». З метою контролю за цими ухвалами 19 серпня 2014 р. міністр внутрішніх справ України А. Аваков підписав наказ про спільні дії МВС і Національної ради, відповідно до якого територіальні підрозділи МВС повинні сприяти виявленню та зупиненню пропагандистської діяльності [4].

У березні 2014 року зусиллями провідних українських експертів у галузі міжнародних відносин, комунікацій та зв'язків з громадськістю створено громадську організацію **Український кризовий медіа-центр**, щоб надавати світовій спільноті об'єктивну інформацію про події в Україні, виклики та загрози

національній безпеці, зокрема у військовій, політичній, економічній, енергетичній та гуманітарній сферах [5].

Проте, разом із деякими кроками в реформуванні інформаційної політики, основний масив інформаційних відносин все ще потребує свого правового врегулювання та закріплення, такі законодавчі акти як Закон України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» були прийняті та набули чинності ще в 90-х роках ХХ століття і через майже 30 років свого існування не були адаптовані під реалії сьогодення.

Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року «**Про Доктрину інформаційної безпеки України**» було визначено пріоритетні засади формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [6]. Разом з тим законодавчі акти вживаючи термін гібридна війна не дають його визначення, тож не можливо одним прийнятим рішенням охопити всю важливість проблеми гібридної війни, та забезпечити заходи її запобігання та протидії.

Належне регулювання інформаційних відносин можливе лише за умови скоординованих дій та взаємодії всіх суб'єктів інформаційного простору, пов'язаних із законодавчим регулюванням інформаційних відносин, забезпеченням належного рівня захисту та поширення інформації.

Висновки. В умовах гібридної війни інформація та використання інформаційного простору вцілому, стають важливими факторами досягнення стратегічної мети країни агресора. Рівень інформатизації суспільства без належних механізмів захисту та правового регулювання інформації спричиняє деморалізацію суспільства підриваючи державний лад та порушує процеси поширення та використання інформації.

Процеси світової глобалізації новітніх інформаційних технологій, формування інформаційного суспільства посилюють важливість такої складової національної безпеки, як інформаційна безпека.

В умовах ведення гібридної війни, з метою розвитку та реформування власної системи інформаційної безпеки Україна має бути готова до забезпечення належного рівня інформаційного захисту, при цьому необхідно розробити чітку стратегію регулювання інформаційних відносин.

На сьогодні забезпечення належного рівня інформаційних відносин може бути реалізоване за умови створення скоординованої взаємодії суб'єктів державної влади, щодо вирішенням задач, які постають перед Україною вже сьогодні:

- прийняття чіткої державної інформаційної політики України з запобіганням зовнішнього впливу;
- створення оновленої нормативно правової бази регулювання інформаційних відносин ;

- узгодження та координування діяльності різних відомств під час створення ефективної системи захисту вітчизняного інформаційного простору, контроль за використанням інформаційного простору України;
- забезпечення високого рівня якісної інформації;
- забезпечення політики держави, що надає вільний доступ громадян до якісної інформації тощо.

Список використаних джерел:

1. Маклюен Г. М. Внешние расширения человека / Г. М. Маклюен ; пер. с англ. В. Николаева ; закл. ст. М. Вавилова. – М. ; Жуковский / Канон-пресс-ц / Куликово поле, 2003. / 464 с.
2. Александр Варкетин / ««Гибридная война» - новая угроза или пропагандистский трюк?» / газета Deutsche Welle / 25.02.2015/. - URL:<https://p.dw.com/p/1Eh3F>
3. «Кібернетична та інформаційна війна в українському конфлікті» Марі Безнер та Патріс Робін / 2017 Center for Security Studies (CSS), ETH Zürich / 31 с. /.- URL:<http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pd/перекладhttps://www.radiosvoboda.org/a/28580039.html>
4. В Україні заборонили мовлення 14 російських телеканалів.- URL:<http://vgoru.org/index.php/all-news/euromaydan/item/7004v-ukrajini-zaboronili-movlennya-14-rosijskikh-telekanaliv>.
5. Український кризовий медіа центр.-URL:<http://uacrisis.org/ua/about>
6. Указ президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»» / Документ 47/2017/. -URL:<http://zakon.rada.gov.ua/laws/show/47/2017>

*Троян А. П., аспірант
НДШіП НАПрН України*

ПРОБЛЕМИ ПРАВОВИХ ЗАСАД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АДВОКАТСЬКОЇ ДІЯЛЬНОСТІ

Наразі у Верховній Раді України зареєстровано три законопроекти «Про адвокатуру та адвокатську діяльність». Вже сам факт наявності декількох альтернативних законопроектів свідчить як про наявність проблем у правовому регулюванні цієї сфери, так і про наявність різних думок щодо їх вирішення:

1. Законопроект № 9055 від 06.09.2018 р., внесений Президентом України [0].
2. Законопроект № 9055-1 від 14.09.2018 р., внесений народним депутатом Писаренко В.В. [2].
3. Законопроект № 9055-2 від 20.09.2018 р., внесений групою народних депутатів на чолі з Ківаловим С.В. [3].

З точки зору проблем інформаційної безпеки адвокатської діяльності запропоновані законопроекти доцільно розглядати у двох аспектах:

- щодо видів адвокатської діяльності;

- щодо поняття адвокатської таємниці.

Чинний на цей час Закон України «Про адвокатуру і адвокатську діяльність» статтею 19 встановлює наступні види адвокатської діяльності:

1) надання правової інформації, консультацій і роз'яснень з правових питань, правовий супровід діяльності юридичних і фізичних осіб, органів державної влади, органів місцевого самоврядування, держави;

2) складення заяв, скарг, процесуальних та інших документів правового характеру;

3) захист прав, свобод і законних інтересів підозрюваного, обвинуваченого, підсудного, засудженого, виправданого, особи, стосовно якої передбачається застосування примусових заходів медичного чи виховного характеру або вирішується питання про їх застосування у кримінальному провадженні, особи, стосовно якої розглядається питання про видачу іноземній державі (екстрадицію), а також особи, яка притягається до адміністративної відповідальності під час розгляду справи про адміністративне правопорушення;

4) надання правової допомоги свідку у кримінальному провадженні;

5) представництво інтересів потерпілого під час розгляду справи про адміністративне правопорушення, прав і обов'язків потерпілого, цивільного позивача, цивільного відповідача у кримінальному провадженні;

6) представництво інтересів фізичних і юридичних осіб у судах під час здійснення цивільного, господарського, адміністративного та конституційного судочинства, а також в інших державних органах, перед фізичними та юридичними особами;

7) представництво інтересів фізичних і юридичних осіб, держави, органів державної влади, органів місцевого самоврядування в іноземних, міжнародних судових органах, якщо інше не встановлено законодавством іноземних держав, статутними документами міжнародних судових органів та інших міжнародних організацій або міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України;

8) надання правової допомоги під час виконання та відбування кримінальних покарань [4].

Всі три законопроекти, з невеликою різницею у формулюваннях, до цього переліку, зокрема, додають надання інформації, консультацій і роз'яснень з питань медіації, забезпечення правового супроводу процедури медіації та її завершення.

При цьому, законопроектами № 9055-1 та № 9055-2 пропонується встановити такий вид адвокатської діяльності, як «участь в організації та проведенні процедури медіації у якості медіатора».

Слід зазначити, що законопроектом «Про медіацію», який перебуває на розгляді Верховної Ради України ще з 2015 року і наразі був прийнятим у першому читанні 03.11.2016 року встановлено певні вимоги до особи медіатора – це фізична особа, яка досягла двадцяти п'яти років, має вищу або професійно-

технічну освіту та пройшла професійне навчання медіації, що має включати 90 академічних годин початкового навчання, в тому числі не менше 45 академічних годин навчання практичним навичкам [5].

Таким чином, створюється ситуація, коли в межах процедури медіації особа, яка є медіатором, матиме обов'язок зберігати адвокатську таємницю, якщо така особа є адвокатом.

Щодо самої адвокатської таємниці, то законопроекти № 9055-1 та № 9055-2 залишають її в чинному вигляді, навіть із збереженням номеру статті у законі.

Натомість, законопроектом №9055 пропонується розширити як саме поняття адвокатської таємниці, так і надати адвокату право не розголошувати її навіть за наявності згоди клієнта.

Так, адвокатською таємницею запропоновано вважати:

1) факт звернення особи за правничою допомогою;

2) будь-яка інформація, що стала відома адвокату, адвокатському бюро, адвокатському об'єднанню, помічнику адвоката або іншій особі, яка перебуває у трудових відносинах з адвокатом, у зв'язку з наданням правничої допомоги або зверненням особи за правничою допомогою;

3) інформація, яка стосується надання правничої допомоги, в тому числі така, що стала відома адвокату, адвокатському бюро, адвокатському об'єднанню, помічнику адвоката або іншій особі, яка перебуває у трудових відносинах з адвокатом, до звернення клієнта за правничою допомогою, якщо розкриття такої інформації може, на думку адвоката, зашкодити інтересам клієнта;

4) зміст будь-якого спілкування, листування та інших комунікацій (у тому числі з використанням засобів зв'язку) адвоката, помічника адвоката з клієнтом або особою, яка звернулася за правничою допомогою, адвоката з помічником адвоката;

5) зміст порад, консультацій, роз'яснень, документів, відомостей, матеріалів, інформації, підготовлених, зібраних, одержаних адвокатом, помічником адвоката або наданих ним клієнту або особі, яка звернулася за правничою допомогою, незалежно від часу вчинення відповідних дій, а також обставини, пов'язані із наданням, отриманням, підготовкою таких порад, консультацій, роз'яснень, документів, відомостей, матеріалів, інформації [1].

Перший пункт, на нашу думку, було додано за пропозицією органу адвокатського самоврядування, адже ще на З'їзді адвокатів 2017 року до Правил адвокатської етики було внесено аналогічний пункт щодо віднесення факту звернення до адвоката за допомогою до адвокатської таємниці[6].

Також позитивною пропозицією є необмеженість у часі обов'язку збереження адвокатської таємниці – адже на практиці адвокатів часто викликають на допити слідчі органи щодо інформації про клієнтів, якими адвокат надавав допомогу раніше. Відсутність в чинному законі прямої норми створює правову невизначеність щодо дії адвокатської таємниці у часі.

Недопрацьованим, на нашу думку, є питання захисту адвокатської таємниці під час здійснення фідучіарної діяльності, яка пропонується вперше. Адже згідно термінів та визначень, викладених у статті 1 всіх трьох законопроектів, така діяльність не є правничою допомогою, в той час як саме визначення адвокатської таємниці в законопроектах пов'язується саме з цим видом адвокатської діяльності.

Слід відмітити, що наразі не пропонується будь-яких змін, якими б встановлювалося превалювання суспільного інтересу над приватним, як це вже практикується в європейських державах [7].

Зокрема, не пропонується встановити обов'язок адвоката розголошувати адвокатську таємницю у випадках загрози національній безпеці або скоєнню злочинів із можливими масовими жертвами.

Таким чином, можливо зробити наступний висновок.

На цей час в Україні триває формування правових засад адвокатської діяльності, у тому числі – в питаннях захисту адвокатської таємниці як одного з основних елементів системи прав і основоположних свобод людини і громадянина.

Позитивним є те, що триває робота над альтернативними законопроектами, спрямованими на усунення невизначеностей та неузгодженостей в питаннях захисту адвокатської таємниці. На даному етапі нормотворчість вже не є сліпим копіюванням і запозиченням іноземного досвіду, який не завжди гармонізується з правовою системою України, що розбудовується.

В той же час, суб'єктами законодавчої ініціативи не приділяється належної уваги взаємозв'язку пропонованих змін до Закону України «Про адвокатуру і адвокатську діяльність» з іншими законами, а також не пропонується розширення функцій адвокатури як інституту правозахисної діяльності за межі надання професійної правової (правничої) допомоги.

Список використаних джерел:

1. Проект Закону про адвокатуру та адвокатську діяльність №9055 від 06.09.2018. - URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=64557 – Назва з екрана.
2. Проект Закону про адвокатуру та адвокатську діяльність № 9055-1 від 14.09.2018. – URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=64595 – Назва з екрана.
3. Проект Закону про адвокатуру та адвокатську діяльність № 9055-2 від 20.09.2018. – URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=64636 – Назва з екрана
4. Про адвокатуру та адвокатську діяльність. Закон України. – Відомості Верховної Ради. № 27/2013. – ст.282.
5. Проект Закону про медіацію. – URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=57463 – Назва з екрана.
6. Правила адвокатської етики. – Затверджені 09.06.2017 р. звітно-виборним з'їздом адвокатів України 2017 року. – Вища кваліфікаційно-дисциплінарна комісія адвокатури. -URL:<http://vkdka.org/pravila-advokatskoji-etiki-zatverdzeni-zvitno-vibornim-zjzdom-advokativ-ukrajini-2017-roku/> – Назва з екрана.

7. Троян А.П. Адвокатська таємниця в умовах конфлікту приватного та суспільного інтересів. Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2018, №2. С.193-196.

*Лапишина Аннабелла-Ніколь,
студент ФСП КПІ ім. І. Сікорського*

ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Електронне голосування, що є невід'ємною складовою концепції електронної демократії та електронного урядування, є похідним явищем від синтезу основних принципів інформаційного суспільства, в якому головна роль віддається не стільки спожитим чи виробленим продуктам, а саме виробленій та спожитій інформації. У такому суспільстві вирішальними аспектами у житті людей є швидкість отримання та обміну інформації. Це свідчить про те, що більша частина інтелектуальної діяльності людини поступово переходить на новий рівень абстракції – у цифровій вимір.

Інтернет та інформаційно-комунікативні технології (ІКТ) створюють сприятливе середовище для комунікації між бізнесом, владою та суспільством та розвитку електронної демократії. Тож запитання щодо здійснення волевиявлення в режимі онлайн є вкрай актуальним в умовах розвитку та становлення інформаційного суспільства.

Рада Європи визначає [1] е-демократію як використання ІКТ урядами, політичними партіями, громадянами та іншими учасниками політичних процесів на місцях, в регіонах, на національному або міжнародному рівнях з метою розширення участі громадян в процесах прийняття державних рішень. Поняття «електронна демократія» включає «електронне» визначення базових понять політичного процесу. Ці базові поняття надано в Рекомендаціях Комітету міністрів Ради Європи CM/Rec(2009) країнам-учасникам Ради Європи з електронної демократії. Таким чином, до складових е-демократії належить: е-парламент (це використання ІКТ депутатами, а також політичними та публічними службовцями з метою активізації залучення громадян до законотворчої діяльності), е-законодавство, е-правосуддя, е-звернення, е-голосування, е-референдуми, та е-петиції, що передбачають створення е-підрахунку голосів та е-агітацій.

Електронне голосування є невід'ємною складовою та інструментом електронної демократії, що передбачає здійснення волевиявлення громадян шляхом використання електронних пристроїв для ідентифікації, запису та підрахунку голосів.

Електронне голосування дає можливість здійснювати громадянам волевиявлення у будь-якій точці Землі, що вирішує актуальну для України проблему високого проценту неявки виборців на дільницях, а також знижує

вартість виборів, оскільки знижується необхідність у адміністративних виборчих дільницях та папері для бланків. Наприклад, за даними Центральної виборчої комісії, у виборах президента України у 2014 році явка виборців склала 60% громадян. Із 34 692 976 осіб, що мали право голосу скористались своїм правом лише 18 022 236 [2].

Електронне голосування забезпечує легітимність, оскільки голоси підраховуються без працівників державних установ, шляхом програмного забезпечення, тож будь-які маніпуляції з даними та ймовірність підтасовки голосів виключена.

Щодо реалізації, то наприклад, у Естонії голосування здійснюється шляхом ID карт, завдяки яким громадяни можуть пройти ідентифікацію та віддати свій голос через інтернет. В Україні вже запрацювала ініціатива Mobile-ID, яка дозволяє ідентифікувати громадян шляхом спеціальної сім-карти у смартфонах на якій міститься електронний підпис. Відповідно через мобільний додаток громадяни можуть отримувати електронні послуги, застосовуючи свій смартфон. У майбутньому, коли відповідні реєстри будуть створені та створено певну інформаційну інфраструктуру, українці зможуть голосувати на виборах, чи підписувати петиції через інтернет не виходячи з дому застосовуючи функцію Mobile-ID.

Єдиною загрозою для е-голосування є атака на отримані дані, однак для цього можна використовувати децентралізовані бази даних, тобто блокчейн, оскільки кожен новий блок інформації містить про себе дані про всі попередні записи у реєстрі, тому знищити інформацію чи якимось чином змінити її неможливо. Крім того, технологію блокчейн можна застосовувати під час голосування у залі Верховної Ради, у цьому випадку, окрім цифрового підпису ідентифікація має проходити через біометричні дані, наприклад, відбиток пальця. Таким чином, біометрична ідентифікація під час голосування має подолати сумнозвісне «кнопкодавство», тобто безособове голосування.

За даними порталу Electoral Knowledge Network [3], спеціалісти називають наступні переваги імплементації системи електронних виборів.

- Здійснення волевиявлення людьми з обмеженими можливостями.
- Електронне голосування сприяє швидшому підрахунку голосів і оголошенню остаточних результатів виборів.
- Очікується, що електронне голосування призводить до більш надійних результатів, оскільки виключені помилки, які виникають внаслідок людського фактору.
- Е-голосування пропонує більше способів подання багатомовних бюлетенів для голосування.
- Довгострокова економічність за рахунок зменшення часу опитування працівників, поштових зборів, витрат на друк.
- Віддалене інтернет-голосування може забезпечити можливості для поліпшення доступу окремих груп до виборчого процесу, таких як люди з вадами

зору, ті, хто не може відвідувати виборчі дільниці (військовослужбовці та громадяни, які проживають за кордоном).

- Віддалене голосування в Інтернеті дозволяє виборцям голосувати в інших виборчих округах, а не тих, де вони зареєстровані, і полегшує процес голосування для громадян, які раніше голосували поштою.

- Ризики застосування електронних виборів [4]:

- Хакерські атаки.

- Складності перерахування голосів.

- Відсутність узгоджених (міжнародних) стандартів на сертифікацію .

- Висока залежність від продавців обладнання та розробників ПО.

- Потреба в освітніх кампаніях.

- Ризик (втрати) довіри громадськості до процесу виборів / референдуму.

- Збільшення витрат (придбання та підтримка системи електронного голосування).

- Потенційне порушення таємниці голосування, особливо в системах, які виконувати перевірку автентичності виборців і голосувати голосування.

- Ризик маніпулювання інсайдерами привілейований доступ до системи або хакери ззовні.

- Необхідність розробки спеціальної законодавчої бази.

Згідно з прогнозами компанії Ericsson [4], до 2020 року проникнення мобільних пристроїв серед жителів України складатиме 71%, станом на 2017 рік цей показник був на рівні 40%. Таким чином, ми можемо спостерігати активний ріст користувачів мобільних пристроїв. Саме завдяки смартфонам держава може налагодити прямий зв'язок зі своїми громадянами. Тож електронне голосування – питання часу, оскільки технологічна інфраструктура вже починає розбудовуватись самостійно. Однак вкрай важливим залишається питання безпеки, збереження персональних даних та таємниці голосування. Для цього необхідно використовувати безпечні методи шифрування та передачі даних, а також створити відповідне програмне забезпечення.

Важливим також є питання законодавчої бази, оскільки для впровадження електронного голосування також необхідна політична воля. Однак, завдяки Закону України про децентралізацію, рішення про проведення експериментального е-голосування може прийматись на місцевому рівні. Перші етапи волевиявлення мають проводитись у тестовому режимі, щоби визначити всі недоліки та переваги програмного забезпечення. І лише після експерименту на підставі аналізу перебігу електронного виборчого процесу може бути ухвалене рішення про застосування е-голосування на практиці.

Список використаних джерел:

1. https://onat.edu.ua/wp-content/uploads/2018/05/Part_003_Feb_2018.pdf
2. http://www.cvk.gov.ua/info/protokol_cvk_25052014.pdf
3. <http://aceproject.org/ace-en/focus/e-voting/countries>

4. <http://www.eods.eu/library/IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf>
5. <https://www.ericsson.com/en/mobility-report>

*Сказко О. М., аспірант
НДІІП НАПрН України*

ПРОБЛЕМИ ГАЛУЗЕВОЇ НАЛЕЖНОСТІ ПРАВОВИХ НОРМ У СФЕРІ ВИРІШЕННЯ ДОМЕННИХ СПОРІВ

Ефективність вирішення доменних спорів в Україні значною мірою залежить від досконалості правових норм, якими регулюється означений вид інформаційної діяльності. Аналізуючи дані судової практики, можна переконатися, що у судовому порядку спори у вказаній сфері вирішуються переважно у порядку цивільного і господарського, рідше – адміністративного судочинства, при цьому їх кількість щорічно зростає. Предметом спору досить часто стають визнання права користування доменним ім'ям та зобов'язання вчинити певні дії (цивільне судочинство), визнання права на володіння та користування та на делегування доменного імені, припинення використання певного комерційного найменування у доменному імені (господарське судочинство). У практиці Європейського суду з прав людини (наприклад, справа «Пайн Веллі Девелопмент та інші проти Ірландії» (Pine Valley Development Ltd and Others vs. Ireland, № 12742/87, рішення від 29 листопада 1991 року), «Стретч проти Об'єднаного Королівства» (Stretch vs. United Kingdom, № 44277/98, рішення від 24 червня 2003 року), «Федоренко проти України» (Fedorenko vs. Ukraine, № 25921/02, рішення від 1 червня 2006 року) концепція власності трактується досить широко та має на увазі, зокрема, рухоме та нерухоме майно, акції та інші цінні папери, патенти, право на виконання рішення суду, яке набрало законної сили, ліцензії на проведення діяльності, економічні інтереси, пов'язані з веденням бізнесу, право продовження оренди нерухомості, доменні імена, право на податкові кредити, правомірні очікування настання певних обставин. Однак, з огляду на відносну новизну категорії «доменне ім'я» як об'єкта державного захисту, судова практика у цій сфері певним чином випереджає науково-методологічне обґрунтування у теоретичних працях. Отже, як і для багатьох інших феноменів інформаційної сфери, для доменного імені притаманним є певне відставання інформаційно-правової теорії від актуального стану розвитку суспільних відносин.

Як відомо, предмет інформаційного права складають суспільні відносини, що визначають правове регулювання створення, зберігання, володіння, використання, користування, поширення інформації, формування та використання інформаційних ресурсів, встановлення режимів доступу до інформації, створення та використання інформаційних систем, використання інформаційного продукту, забезпечення прав суб'єктів при отриманні повної та об'єктивної інформації,

забезпечення інформаційної безпеки суб'єктів інформаційних відносин, а також проведення державної інформаційної політики [1, с.6]. Відповідно до положень ст.1 Закону України «Про телекомунікації» домен – це частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється [2]. Доменне ім'я, згідно положень ст.1 Закону України «Про охорону прав на знаки для товарів і послуг» - це ім'я, що використовується для адресації комп'ютерів і ресурсів в Інтернеті [3]. Слід сказати, що у правових актах та у теоретичних джерелах містяться й деякі інші визначення доменного імені, однак їх сутність зводиться до виділення як основної їх ознаки того, що доменні імена виступають засобом ідентифікації інформаційних ресурсів у мережі Інтернет.

Оскільки суспільні відносини, пов'язані із формуванням та використанням інформаційних ресурсів, входять до предмету інформаційного права, можна зробити висновок, що правове регулювання діяльності, пов'язаної з використанням доменних імен, також здійснюється засобами інформаційного права. Однак, як ми вказували вище, вирішення доменних спорів у правовому порядку переважно здійснюється у межах цивільного та господарського судочинства. У науці цивільного права з цього приводу сформувалося два основних підходи – майновий і процесний (процедурний). У межах першого з них вважається, що право на доменне ім'я є майном, а право на нього носить абсолютний характер. Прихильники другого підходу відстоюють думку, що право на доменне ім'я має відносний характер і виникає внаслідок укладення договору. У будь-якому разі у дослідженнях з цивільного права та цивільного процесу досить часто констатується належність правовідносин, пов'язаних з вирішенням доменних спорів, до відповідних правових галузей.

Відносно вказаної позиції ми погоджуємося з думкою І. В. Панової, яка вважає, що сьогоденний етап розвитку інформаційного суспільства неможливо забезпечити в рамках адміністративного, або цивільного права з огляду на підвищення рівня життя, починаючи від дозвілля, побуту, глобального інформаційного обміну, електронної торгівлі, модернізації виробничих процесів й управління малими, середніми підприємствами та глобальними корпораціями та закінчуючи створенням дедалі новіших інформаційно-програмних та апаратних засобів, без яких вже важко уявити подальше існування та розвиток людства. При цьому нині в Україні поки що не розроблена концепція теоретичних засад розвитку окремих галузей права. Це стосується й інформаційного права. Як сукупність правових норм система права не співпадає із системою законодавства. Так, інформаційне право на відміну від інформаційного законодавства, як системи нормативно-правових актів, що регулюють інформаційно-правові відносини, включає різні інформаційно-правові норми, у тому числі норми права, що містяться в актах інформаційного законодавства, а також і норми права, що входять до складу нормативно-правових актів джерел інших галузей законодавства, зокрема адміністративного та цивільного [4].

Із наведеного вище можна зробити наступні висновки. По-перше, функціонування системи доменних імен як засобів ідентифікації інформаційних ресурсів належить до кола суспільних відносин, що входять до предмету інформаційного права. По-друге, особливістю інформаційно-правових норм є комплексний характер багатьох з них, включення до складу інформаційно-правової норми як суто інформаційного елементу, так і елементу, що може належати до іншої галузі права, і саме ця ознака притаманна нормам, призначеним регулювати вирішення доменних спорів. По-третє, причина неможливості ефективно здійснювати правове регулювання суспільних відносин, що виникають під час вирішення доменних спорів, полягає у надзвичайно складному і багатозначному понятті категорії «інформація», щодо матеріальності якої у правовій науці вже багато десятиліть точаться дискусії. Вказане породжує різноманіття концептуальних підходів до категорії «інформаційний ресурс», що не може не відобразитися на розумінні сутності доменного імені як засобу ідентифікації таких ресурсів. Ми вважаємо, що вирішення цих теоретичних питань у правовій науці може потребувати глибокого їх усвідомлення та аналізу протягом довгого проміжку часу. Однак для отримання можливості детально дослідити особливості вирішення доменних спорів на сьогоднішній день достатньо усвідомлення комплексного характеру інформаційно-правових норм, що виникають у вказаній сфері, і подальшого вивчення властивостей інформаційних, цивільних, господарських та міжнародних правовідносин, пов'язаних з різноманітними аспектами реалізації права на доменне ім'я суб'єктами вказаних відносин.

Список використаних джерел:

1. Калюжний Р.А., Марценюк А.Г. *Правова інформатика*. 2008. №3(19). С.5-9.
 2. Про телекомунікації: Закон України. *Відомості Верховної Ради України*. 2004. №12. С.155.
 3. Про охорону прав на знаки для товарів і послуг: Закон України. *Відомості Верховної Ради України*. 1994. №7. С.36.
- Панова І.В. Парадигма сучасного інформаційного права України. *Інформація і право*. 2014. №3 (12). С.31-39.

*Ціпцюра Т. студент
ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Чукот С. А., доктор наук з державного
управління, професор
ФСП КПІ ім. Ігоря Сікорського*

НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ В УКРАЇНІ З УРАХУВАННЯМ КРАЩИХ ЄВРОПЕЙСЬКИХ ПРАКТИК

Розвиток інформаційних технологій сприяв виникненню нових комунікаційних інструментів між владою та громадськістю, налагодженню взаємозв'язку та взаємодії при виробленні, прийнятті та реалізації управлінських рішень. Завдяки сучасним технологіям існує можливість здійснювати швидкий обмін інформацією (надавати доручення та вказівки уповноваженим особам, надсилати запити тощо), проводити спілкування з громадянами (отримання та опрацювання звернень громадян, проведення громадського обговорення) та забезпечувати більш ефективно управління.

Україна не може бути осторонь прогресу, саме тому в нашій країні особлива увага прикута до розвитку електронного урядування. Свідченням цього, стали працюючі сервіси електронних петицій на сайтах Верховної Ради України, Президента України та Кабінету Міністрів України, на сторінках місцевих органів влади, створюються і наповнюються різноманітні інформаційні ресурси органів державної влади та місцевого самоврядування, запроваджуються електронні послуги, зокрема у сфері публічних закупівель створено електронний сервіс Prozorro. [1]

Впровадження електронного урядування в Україні, зокрема надання якісних електронних послуг, неможливе без вивчення та дослідження досвіду зарубіжних країн. Це потрібно для того, щоб «вчитися на чужих помилках» та ефективно вирішувати проблеми, які виникають під час запровадження тих чи інших послуг електронним чином. Враховуючи Асоціацію України з Європейським Союзом, особливу зацікавленість викликають кращі практики європейських країн, які досягли успіху на цьому шляху. Найбільш яскравим, на наш погляд, є досвід електронного урядування в Естонії. На сьогодні можливості, які мають громадяни в Естонії завдяки використанню сучасних ІКТ, є досить значними. Так, майже 95% населення задіяні в електронній системі ID. У 2015 році вперше відбулися вибори через мережу Інтернет: близько 31% голосів були подані саме дистанційно. В Естонії досить розвинений інтернет-банкінг та створені умови для подання податкових декларацій через відповідну електронну систему. При цьому, зареєструвати бізнес також можна через Інтернет, а кожен пацієнт має власну електронну медичну справу. [2]

На нашу думку, Україні слід використати позитивний досвід Естонії та здійснити наступні заходи для ефективного розвитку електронного урядування, зокрема надання якісних електронних послуг.

По-перше, передбачити утворення інформаційного ресурсу, який би поєднав громадськість, бізнес та владу. Цей інформаційний ресурс має бути захищеним від зовнішнього втручання, ідентифікація учасників має здійснюватись за електронним підписом, який має бути наданий кожній особі безкоштовно. Інформаційний ресурс має бути універсальним та надавати доступ до різних державних та приватних послуг, тобто особа повинна мати можливість за допомогою цього сервісу отримати довідку, звернутися із запитом до будь-якого органу, подати заяву на оформлення пенсії чи соціальної допомоги, зареєструвати бізнес, зареєструвати нове місце проживання, подати податкову декларацію, подати позов чи інший процесуальний документ до суду, отримати консультацію фахівця. Такий сервіс має передбачати взаємодію держави з громадянами, тобто постійне опрацювання в режимі он-лайн інформації фахівцями та надання відповіді операторами на звернення громадян. Також за допомогою такої системи особи повинні мати можливість звернутися до обраного лікаря, обрати заклад освіти, отримати юридичні послуги, тобто скористатися послугами приватних осіб. Отже, необхідно утворити таку систему, на якій в режимі одного вікна особа зможе авторизуватися, після чого скористатися будь-якою послугою, які будуть розміщені за блоками (освіта, медицина, юридичні послуги, правосуддя, реєстраційні послуги тощо). Така модель позбавлятиме необхідності постійної авторизації для отримання кожної послуги та зробить зручним користування ресурсами для отримання послуг. Зрештою, такий сервіс забезпечить комунікацію всіх ланок громадянського суспільства, оскільки громадяни зможуть звернутися не лише до держави, а й до приватного бізнесу, який має бути підключений до такої системи. Наприклад, у разі оформлення бізнесу особа має відкрити рахунок у банку, тому в такій системі їй має бути запропонований перелік банківських установ.

По-друге, варто вдосконалити правовий механізм та максимально спростити процедури отримання послуг. Більшість процедур мають здійснюватись в один клік, без кількох візитів до державних органів. Все це можливо зробити, якщо скасувати бюрократичні обмеження та прискіпливе ставлення державних службовців до пакету документів, обсяг якого у певних випадках (наприклад, при оформленні пенсії) є не виправдано великим, оскільки в органів влади вже існує доступ до такої інформації. Реєстрація місця проживання, як і постановка на облік до військового комісаріату для хлопців, має здійснюватись в один клік – шляхом внесення змін до відповідного реєстру, без візитів та черг до відповідних органів за попереднім місцем проживання. [1]

По-третє, запровадження електронного урядування потребує підвищення інформаційної грамотності населення. Необхідно привчати людей старшого віку до використання інформаційних ресурсів, проводити інформаційну кампанію щодо зручності використання ID-паспортів та електронного цифрового підпису (окрім того, всі громадяни повинні мати можливість безоплатно обміняти паспорт старого зразку на ID-картку), безпеки в інформаційному просторі. На жаль, велика

частина людей з недовірою ставиться до інструментів електронного урядування, що необхідно виправляти шляхом інформаційної освіти та роз'яснення громадянам переваг нової моделі.

Таким чином, за рахунок здійснення заходів правового та просвітницького характеру, створення відповідної матеріальної бази можливе надання якісних електронних послуг, що сприятиме розвитку електронного урядування в Україні. Успішний досвід Естонії та інших європейських країн дає підстави вважати, що перспективи для побудови дієвого механізму електронного урядування цілком реальні й залежать від зусиль, що здійснюються державою, громадськістю й населенням, проте найбільше – від політичної волі державних уповноважених.

Список використаних джерел:

7. Концепція електронного урядування в Україні від 20.09.2017.-
URL:<http://zakon.rada.gov.ua/laws/show/649-2017-%D1%80>

8. Естонський досвід електронного урядування – Україні.-
URL:<http://reformsguide.org.ua/ua/news/estonia-shares-e-government-experience-with-ukraine/>

Дудіна О. О., студент

ФСП КПІ ім. Ігоря Сікорського

Науковий керівник:

Фурашев В. М., к.т.н., доцент, с.н.с.

ФСП КПІ ім. Ігоря Сікорського

ПРОБЛЕМНІ ПИТАННЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА В ІНФОРМАЦІЙНІЙ СФЕРІ

Разом із науково-технічним прогресом на сучасному етапі розвитку суспільства поширеним є явище впровадження інформаційних технологій у всі сфери життя, чи то окремого індивіда, чи то суспільства в цілому, навіть на державному рівні. Більш того, інформація стає показником розвиненості та могутності будь-якого суспільства та має чималий вплив на формування нових багатоманітних сфер життя людини.

В умовах інформаційної революції виникла необхідність правової регламентації нових видів правовідносин у сфері інформаційного права. Основоположним законом в цій сфері є Закон України «Про інформацію». Цим законом у 1992 році було закріплено гарантованість права на інформацію, свободу вираження поглядів та низка інших принципів інформаційних відносин. Ще одним вагомим щаблем, що почав розбудову законодавства в сфері інформаційного права є Конституція України. Її положеннями у 1996 році було встановлено загальні правові засади, зокрема закріплено право громадян «вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб» (ст. 34). До переліку законодавчих актів України поступово додалися такі закони України, як: «Про інформаційні агентства», «Про друковані

засоби масової інформації (пресу) в Україні», «Про телебачення та радіомовлення», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо.

Окрім цього існує низка нормативних документів у галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування комплексної системи захисту інформації (КСЗІ).

Говорячи про законодавство України, можна сказати, що однієї з найбільших вад нормативно-правових актів в сфері інформаційного права є те, що вони спрямовані лише на вирішення тактичних завдань. З огляду на те, що галузь інформаційного права виникла лише на межі 20-го та 21-го століть і є доволі молодою, на даному етапі потрібно приділити увагу перспективам її розвитку та сформулювати стратегію щодо подальшого врегулювання специфічних відносин цієї галузі права. Законодавство потрібно будувати таким чином, щоб воно діяло «на випередження» та могло повноцінно регулювати швидко еволюціонуючі відносини.

Наступною вагомою проблемою законодавства України в сфері інформаційного права є відсутність чіткої ієрархічної єдності законів. Особливо слід наголосити на відсутності так званого «Інформаційного кодексу» як внутрішньо цілісного складного нормативно-правового акту, що об'єднує норми всієї галузі права. Це спричинило іншу проблема – велику кількість законів та підзаконних нормативних актів.

В умовах відсутності узгодження понятійного апарату поширені термінологічні неточності, які призводять до виникнення колізій в інформаційному праві. Нові правові акти в сфері суспільних інформаційних відносин часто не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу.

Більш того, все більш гострою стає потреба держави у досвідчених фахівцях з інформаційного права: з кожним роком посилюється беззаперечно негативний вплив ззовні на український інформаційний простір, - виникає загроза так званого «розмивання» моральних цінностей, етнічних традицій, що відповідають за національну самовизначеність суспільства. Неналежною є підготовка нових фахівців у вищих навчальних закладах: їх рівень обізнаності у питаннях інформаційного права та правової інформатики є досить низьким, що спричиняє критичний стан застосування технічних засобів та інформаційно-комп'ютерних технологій у галузі державного управління та міжнародних комунікацій.

Отже, попри різноманітність та всебічність правової бази досі існує достатня кількість проблемних питань національного законодавства в інформаційній сфері, які потребують негайного вирішення. До таких питань належать:

– відсутність стратегічного аспекту нормативної бази щодо еволюціонуючі відносин в сфері інформаційного права;

- відсутність чіткої ієрархічної єдності законів;
- велика кількість законів та підзаконних нормативних актів;
- відсутність узгодження понятійного апарату, термінологічні неточності;
- нові правові акти в сфері суспільних інформаційних відносин часто не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу;
- потреба держави у досвідчених фахівцях з інформаційного права;
- загроза так званого «розмивання» моральних цінностей, етнічних традицій, що відповідають за національну самовизначеність суспільства;
- неналежна підготовка нових фахівців в сфері інформаційного права.

На нашу думку, під час розробки та впровадження власного національного законодавства в сфері інформаційного права доцільним буде дослідження досвіду зарубіжних держав.

Список використаних джерел:

1. Конституція України: Ухвалена 28 червня 1996 року на 5-й сесії Верховної Ради України 2-го скликання.- URL: <http://zakon4.rada.gov.ua/laws/show/254к/96-вр>, вільний;
2. Закон України «Про інформацію». N 2658-ХІІ (2658-12) від 02.10.92. - URL:<http://zakon0.rada.gov.ua/laws/show/2657-12>, вільний.

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

МІНСЬКІ ДОМОВЛЕНОСТІ – ПРАВОВА ПРИРОДА УГОДИ ТА ЇЇ ВПЛИВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ УКРАЇНИ

Воєнний конфлікт на Сході України створив ряд значних загроз національній безпеці, в тому числі й в інформаційній сфері. Проте, якщо протягом вже майже 5-и років протистояння на фронті вдалося досягти певної стабілізації ситуації, в інформаційній сфері про позитивні зрушення говорити важко. Більше того, на нашу думку, так звані «Мінські угоди» зіграли в інформаційному протистоянні зовсім не на користь України. Для того, щоб обґрунтувати таку думку нам необхідно уважно дослідити природу і зміст даної «угоди».

«Мінські домовленості» стали поворотною точкою в регулюванні воєнного конфлікту на Сході. Як відомо, саме у відповідності до цих домовленостей Президентом України – Верховним Головнокомандувачем Збройними Силами України військам було віддано накази про припинення наступу на східному напрямку, відведення важкого озброєння від лінії зіткнення (фронту) тощо.

Попри значний, переломний вплив на хід воєнних дій «Мінських домовленостей», їхня правова природа і практична ефективність викликають питання.

Досліджуючи природу та зміст «Мінських угод» варто визначити їх відповідність поняттю «міжнародний договір», адже окрім нормативно-правових актів національних компетентних органів, правові наслідки для України можуть створювати лише міжнародні договори.

Адже стаття 9 Конституції України визначає наступне:

«Чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України.»

Укладення міжнародних договорів, які суперечать Конституції України, можливе лише після внесення відповідних змін до Конституції України.»

У відповідності до положень ст. 2 Віденської конвенції про право міжнародних договорів, під міжнародним договором слід розуміти міжнародну угоду, укладену між державами в письмовій формі і регульовану міжнародним правом, незалежно від того, чи викладена така угода в одному документі, двох чи кількох зв'язаних між собою документах, а також незалежно від її конкретного найменування.

Враховуючи, що згідно з наведеними положеннями Віденської конвенції міжнародні договори можуть укладатись лише між державами, особливої уваги та аналізу заслуговують особи учасників перемовин – підписантів «Мінських домовленостей».

Від України «Мінський протокол» підписував Другий Президент України – Леонід Кучма, який не був належно уповноважений на підписання будь-яких юридично значущих документів (в т.ч. міжнародних договорів) від імені України, оскільки не був носієм відповідних владних повноважень.

Від ОБСЄ – посол Гайді Тальявіні, яка була правомочним представником даної міжнародної організації.

Від так званої «ДНР» – Олександр Захарченко, який ніколи не був представником будь-якої держави або іншого суб'єкта міжнародних відносин, ніколи легітимним шляхом не отримував жодних владних повноважень.

Від так званої «ЛНР» – Ігор Плотницький, який, аналогічно Захарченку, ніколи не був представником будь-якої держави або іншого суб'єкта міжнародних відносин, ніколи легітимним шляхом не отримував жодних владних повноважень.

Від Росії – посол РФ в Україні Михайло Зурабов. Варто нагадати, що офіційно Російська Федерація заперечує свою будь-яку причетність до організації й підтримки діяльності незаконних збройних формувань так званих «ДНР/ЛНР» на території України, і з точки зору права не було жодних причин для участі представника РФ у перемовинах щодо врегулювання конфлікту, який Росія називає винятково внутрішнім для України. Таким чином, участь Росії у Мінських перемовинах ще раз підтвердила причетність РФ до розв'язування воєнних дій на Сході України, а з правової точки зору не мала підстав і сенсу.

Як бачимо, «Мінський протокол» було підписано особами, які не мали належних повноважень на укладання міжнародного договору.

З вищевикладеного цілком закономірно витікає той факт, що по сьогоднішній день ратифікації Верховною Радою України положень «Мінських домовленостей» не було здійснено, а отже, відповідні положення, під якими поставили підписи не уповноважені на те належним чином особи – учасники перемовин, в будь-якому разі не можуть нести для України жодних (та решти підписантів) обов'язкових правових наслідків.

Цілком передбачувано, Російською Федерацією та її маріонетковими самопроголошеними «республіками» документ також не було жодним чином ратифіковано.

Разом з тим, слід зазначити, що «Мінські угоди» знайшли певне правове відображення як у міжнародних, так і в національних нормативно-правових актах, зокрема:

- резолюцією Ради Безпеки ООН 2202 (2015), прийнятою на її 7384-у засіданні 17 лютого 2015 року, схвалюється Комплекс заходів щодо виконання Мінських угод;

- посилання на Мінські «меморандум» і «Комплекс» заходів містяться й у рішенні РНБО України «Про додаткові заходи щодо мирного врегулювання, нормалізації ситуації та зміцнення безпеки в окремих районах Донецької та Луганської областей» від 12 березня 2015 року.

Таким чином, маємо досить непередбачувану і юридично неприпустиму ситуацію, коли в актах міжнародного і національного права домовленість неправомочних суб'єктів згадується як певна юридично значуща подія, що несе конкретні правові наслідки.

Самі ж положення «Мінського протоколу» торкаються надзвичайно важливих питань, вирішення низки з яких входить до виняткової компетенції національних органів державної влади України, зокрема «Мінський протокол» містить наступні положення-зобов'язання підписантів:

«Забезпечити негайне двостороннє припинення застосування зброї...»

«Здійснити децентралізацію влади, в тому числі шляхом ухвалення Закону України «Про тимчасовий порядок місцевого самоврядування в окремих районах Донецької і Луганської областей» (Закон про особливий статус)...»

«Ухвалити закон про недопущення переслідування і покарання осіб у зв'язку з подіями, що сталися в окремих районах Донецької і Луганської областей України...»

У відповідності до українського законодавства:

- питання застосування/не застосування зброї ЗСУ – належить до компетенції Президента України – Верховного Головнокомандувача ЗСУ та в межах Законів України, Статутів ЗСУ і наказів Верховного Головнокомандувача – до компетенції командирів і начальників у відповідності до існуючої системи підпорядкування;

– питання прийняття Україною законів, децентралізації влади і т.д. – належить до виняткової компетенції Верховної Ради України. Вичерпний перелік суб'єктів, які мають право законодавчої ініціативи, надається національним законодавством України;

– притягнення до відповідальності осіб «у зв'язку з подіями, що сталися в окремих районах Донецької і Луганської областей України» – компетенція правоохоронних органів України.

Положення «Мінського протоколу» стосовно цих та інших надзвичайно важливих для України питань не повинні в обов'язковому порядку виконуватись Україною, оскільки для цього немає жодних належних підстав. Втім, Україна продовжує фактично в односторонньому порядку виконувати положення «Мінського протоколу», ставлячи під загрозу власні національні, зокрема й безпекові інтереси.

В усього вищевикладеного можемо зробити висновок, що «Мінські домовленості» мають винятково політичну, а не правову природу. Хоч вони й створили поштовх для появи ряду нормативно-правових актів, направлених на правове врегулювання конфлікту, вони не можуть бути визнані актом міжнародного права, й, відповідно, сторони-підписанти «Мінських угод» не можуть нести відповідальність за невиконання положень угоди, яка не є актом міжнародного права. Відповідно, сторони-підписанти не мають й реального правового обов'язку виконувати положення «угоди».

Як підсумок, змушені констатувати, що на сьогодні комплексне міжнародно-правове регулювання воєнного конфлікту на Сході України не створено. А нав'язувана суспільству політичною елітою думка про успішне регулювання ситуації з допомогою «Мінських угод» лише створює ілюзію контрольованості конфлікту, яка в свою чергу є загрозою для інформаційної безпеки суспільства.

Адже, переконані у стабільності та контрольованості ситуації українці починають забувати про те, що на території їх держави все ще йде війна. Це означає, що в свою чергу продовжується й інформаційне протистояння, одна з цілей якого – вплив на свідомість кожного з нас. В таких умовах держава не повинна створювати ілюзій безпеки для власного народу, а навпаки, повинна максимально згуртовувати націю для протистояння нависаючій загрозі.

*Казьмірова І. В., аспірант
ФСП КПП ім. Ігоря Сікорського*

ПРОЦЕСУАЛЬНІ ЗАСОБИ ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

В процесі доказування використовуються різноманітні процесуальні засоби отримання інформації: тимчасовий доступ до речей і документів (які містять

охоронювану законом таємницю), що є заходом забезпечення кримінального провадження, зняття інформації з транспортних телекомунікаційних мереж та зняття інформації з електронних інформаційних систем, що є негласними слідчими (розшуковими) діями.

У зв'язку з можливістю такого широкого доступу до інформації про особу на практиці інколи виникає проблема меж співвідношення заходу забезпечення кримінального провадження - тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, та можливістю проведення певних видів негласних слідчих (розшукових) дій [1].

Зазначене й обумовило необхідність докладніше дослідити питання щодо практичного співвідношення зазначених процесуальних засобів отримання інформації.

Відповідно до ч. 2 ст. 159 КПК України, тимчасовий доступ до речей і документів здійснюється на підставі ухвали слідчого судді.

За приписами ч.ч. 1, 4 ст. 258 КПК України, ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді (за винятком, здобуття відомостей з електронних інформаційних систем або їх частин, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту). Різновидами втручання в приватне спілкування, в тому числі, є зняття інформації з транспортних телекомунікаційних мереж; зняття інформації з електронних інформаційних систем.

Отже, зняття інформації в обумовлених випадках здійснюється на підставі ухвали слідчого судді.

Важливе значення розмежування випадків звернення до того чи іншого процесуального засобу зняття інформації полягає в тому, що від останнього залежить ступінь обмеження конституційних прав і свобод особи. У ч. 1 ст. 159 КПК України законодавець передбачив можливість здійснення тимчасового доступу до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення. Одночасно, ст.ст. 263, 264 КПК України передбачають зняття інформації з транспортних телекомунікаційних мереж та зняття інформації з електронних інформаційних систем.

Судова практика виходить з того, що тимчасовий доступ надається до документів, які містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання тощо і не дають можливості втрутитися у приватне спілкування, тобто отримати доступ до змісту інформації, що передається. А зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК) є різновидом втручання у приватне

спілкування, оскільки здійснюється доступ до змісту повідомлень будь-якого виду та інформації, що передається особою під час зв'язку [1].

Зняття інформації із транспортних телекомунікаційних мереж з'являється з винаходом телефону та розвивається разом з розвитком технічних каналів зв'язку та інформаційних технологій [3, с. 121].

Зняття інформації з транспортних телекомунікаційних мереж поділяється на: 1) контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється; 2) зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються [4].

В аспекті зазначеного, суттєве значення має з'ясування питання щодо можливості отримання від операторів, провайдерів в порядку тимчасового доступу до речей і документів безпосередньо змісту інформації, що передається відповідними телекомунікаційними мережами (доступ до змісту спілкування). Адже, наявність чи, навпаки, відсутність такої можливості фактично виправдовує або ж нівелює той ступінь обмеження конституційних прав і свобод особи, що передбачає застосування такої негласної (слідчої) розшукової дії як зняття інформації з транспортних телекомунікаційних мереж.

Відповідно до ст. 9 Закону України «Про телекомунікації», охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом. Оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Отже, можемо зробити висновок про обмежений характер тимчасового доступу до інформації, що міститься в мобільних терміналах систем зв'язку, з огляду на неможливість втручання у приватне спілкування (доступу до змісту спілкування). В свою чергу, це зумовлює необхідність здійснення зняття інформації з транспортних телекомунікаційних мереж за потреби в отриманні інформації щодо безпосереднього змісту розмови, що передається транспортними телекомунікаційними мережами.

Щодо питання про співвідношення тимчасового доступу до електронних інформаційних систем шляхом зняття копії інформації та зняття інформації з електронних інформаційних систем як негласної слідчої (розшукової) дії зазначимо наступне.

Зміст поняття «електронна інформаційна система» на законодавчому рівні не розкрито. Натомість, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» визначає поняття «інформаційна (автоматизована) система», що являє собою організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів (ст. 1 Закону).

Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача полягає в одержанні інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі [4].

На думку Луцика В.В., з таким визначенням можна погодитись лише частково, оскільки одержання інформації, що міститься в комп'ютерній мережі за загальним правилом повинно охоплюватись такою НСРД, як зняття інформації з транспортних телекомунікаційних мереж. Отримання такої інформації в межах зняття інформації з електронних інформаційних систем можливе лише в тому випадку, коли жоден з елементів локальної мережі не під'єднаний до глобальної мережі [5].

У зв'язку з подібною невизначеністю, нами було проаналізовано судову практику. В переважній більшості випадків, порушення питання щодо зняття інформації з електронних інформаційних систем передбачає зняття інформації з електронної поштової скриньки, що розцінюється судом як різновид втручання у приватне спілкування і відноситься до негласної слідчої (розшукової) дії (Ухвала Рівненського міського суду Рівненської області від 24.10.2018 у справі № 569/19022/18, Ухвала Тернопільського міськрайонного суду Тернопільської області від 15.05.2018 у справі № 607/7608/18).

Судова практика щодо тимчасового доступу до електронних інформаційних систем залишається невизначеною і часто пов'язана зі зняттям копії інформації з електронних інформаційних систем зв'язку, коли фактично відбувається ототожнення з тимчасовим доступом до мобільних терміналів систем зв'язку (Ухвала Печерського районного суду м. Києва від 30.07.2013 у справі №757/16548/13-к).

В будь-якому випадку, ключовим у співвідношенні зазначених вище процесуальних засобів виступає саме факт втручання/невтручання у приватне спілкування.

Додатково зазначимо, що розглянуті процесуальні засоби додатково різняться за суб'єктами застосування. Зокрема, якщо з клопотанням про тимчасовий доступ до речей і документів можуть звернутися обидві сторони

кримінального провадження, то у здійсненні негласних слідчих (розшукових) дій сторони кримінального провадження не є рівними, оскільки сторона захисту може лише ініціювати їх проведення.

Також, зазначені негласні слідчі (розшукові) дії проводяться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів. Виняток становить зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту, що проводиться незалежно від тяжкості злочину.

Список використаних джерел:

1. Узагальнення судової практики щодо розгляду слідчим суддею клопотань про застосування заходів забезпечення кримінального провадження (Витяг) від 07.02.2014: Вищий спеціалізований суд України з розгляду цивільних і кримінальних справ. - URL: <http://zakon3.rada.gov.ua/laws/show/n0001740-14>
2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI / Верховна Рада України. URL: <http://zakon2.rada.gov.ua/laws/show/4651-17>.
3. Уваров В. Г. Зняття інформації з телекомунікаційних мереж. *Актуальні проблеми вітчизняної юриспруденції*. 2017. № 2. С. 121-124.
4. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Наказ Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5.-URL:<http://zakon.rada.gov.ua/laws/show/v0114900-12>
5. Луцик В. В. Зняття інформації з електронних інформаційних систем.- URL: file:///C:/Users/%D0%90%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80/Downloads/vchfo_2014_4_25.pdf
6. Про телекомунікації : Закон України від 18.11.2003 № 1280-IV/ Верховна Рада України. - URL: <http://zakon.rada.gov.ua/laws/show/1280-15>
7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР/ Верховна Рада України. - URL: <http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
8. Ухвала Рівненського міського суду Рівненської області від 24.10.2018 у справі № 569/19022/18. - URL: <http://reyestr.court.gov.ua/Review/77347225>
9. Ухвала Тернопільського міськрайонного суду Тернопільської області від 15.05.2018 у справі № 607/7608/18. - URL : <http://reyestr.court.gov.ua/Review/74178885>
10. Ухвала Печерського районного суду м. Києва від 30.07.2013 у справі №757/16548/13-к. - URL: <http://reyestr.court.gov.ua/Review/54930322>

РОЗДУМИ ПРО ГЕНДЕРНУ ТЕРМІНОЛОГІЮ ТА ВРЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН

Бурхливий розвиток глобальних інформаційних мереж заторкає потреби та інтереси як соціальних груп так і окремих індивідів. Ставлення до інформації у суспільстві пов'язане не лише із розвитком інформаційних технологій, а й зі сприйняттям наукових даних, оформленістю та способами подачі наукової інформації. Комплексний підхід до інформаційного права, як і будь-якої нової галузі знань, бере початок з упорядкування термінів, понять та дефініцій. Згідно з Окінавською хартією, використання інформації як суспільного ресурсу пов'язане із вільним обміном знаннями, взаємною терпимістю і повагою до особливостей людей [3]. Звісно, множина прав і обов'язків учасників суспільних відносин, також, тісно пов'язана із мораллю, традиціями та побутуючими уявленнями про нормативність, зокрема гендерно-рольовим статусами громадян. Дослідники інформаційного права відзначають важливість уніфікації глосаріїв з інформаційно-правової тематики та потребу у формуванні, на основі концептуально оновленої методології інформаційного права, засад інформаційної аксіології (Р. Калюжний, І. Сопілко, М. Швець, В. Цимбалюк) [7, с. 27]. Суб'єкти та об'єкти регулювання суспільних відносин, соціальні факти, що використовуються у інформаційному праві мають гендерний вимір. З'ясування закономірностей розвитку такої складної системи виходить за рамки прикладних наук, а міждисциплінарність гендерної проблематики спонукає до філософських роздумів.

Вирішення прикладних завдань інформаційної безпеки, біоетики та біополітики, також, нерозривно пов'язані з гендерною системою суспільства. У багатьох країнах проблеми проституції та порнографії є у фокусі інформаційного права, інформаційної та кібербезпеки. Наразі наукові пошуки вирішення завдань врегулювання гендерної взаємодії в Україні ускладнені рядом чинників. Серед яких - клерикалізація, псевдонаука та лженаука, що проникли у інформаційний простір, освіту та систему гуманітарного знання. Розвиток інформаційного права на сучасному етапі значною мірою визначається процесами європейської інтеграції України. Варто наголосити, що зміст інформаційних правовідносин у сфері біополітики нерозривно пов'язаний із положеннями, концептами та визначеннями сучасної гендерної теорії і не може бути визначеним без урахування гендерної складової. Зокрема, це право фізичної особи створювати, одержувати, знати, фіксувати, використовувати, поширювати та зберігати інформацію про статеві контакти, батьківство, материнство, донорство репродуктивних матеріалів та ін..

Зауважимо, що гендерна термінологія досі перебуває у стані активного розвитку. У Міністерстві освіти і науки України з 2016 на громадських засадах

започатковано посаду радника Міністра освіти і науки України з питань політики гендерної рівності та антидискримінації в освіті. Першим кроком на шляху досягнення гендерної рівності стало вживанням фемінітивів у публічних виступах посадовців міністерства, проте незмінною залишилась гендерно сліпа термінологія кваліфікацій професій та освітніх стандартів. Цікаво, що Стратегія упровадження гендерної рівності та недискримінації у сфері освіти «Освіта: гендерний вимір – 2020», яка була розроблена Робочою групою з питань політики гендерної рівності та протидії дискримінації в освіті, досі не прийнята, з проблеми «небажаності» гендерної термінології в українському законодавстві. Під час цього річних зустрічей представників Всеукраїнської ради Церков і релігійних організацій з міністром освіти і науки України знову піднімались теми «недопустимості впровадження в освітній процес «гендерної ідеології» і «пропаганди гомосексуалізму» [0]

Всеукраїнська рада церков відкрито виступила також проти ратифікації Україною Конвенцію Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульська конвенція) під приводом «неприйнятності» для українського законодавства терміну «гендер» та його тлумачення науковцями [1]. Зазначимо, що у рамковому законі України «Про забезпечення рівних прав та можливостей жінок і чоловіків» базовий термін «гендер» не визначається. На нашу думку, у сфері інформаційного права гендер доцільно визначити як соціально-рольовий та суспільно-нормативний статус громадян України, що пов'язаний зі статтю людини.

Загалом, проблемною залишається адаптація правової системи України до законодавства ЄС та міжнародних угод. Так, Україна може стати повноправною учасницею Гаазької конвенції про захист дітей і співробітництво з питань міждержавного усиновлення (1993 р.) після ухвалення Верховною Радою закону про приєднання до цієї конвенції. «Такий законопроект було розроблено Міністерством юстиції за участі всіх зацікавлених органів влади», проте «ми досі не приєдналися до Конвенції» [4]. Українська законотворчість часто послуговується термінами, що вийшли з європейського ужитку в середині минулого століття [5]. Як позитив, зазначимо, що цього року Президент підписав Закон України «Про внесення змін до Кримінального кодексу України щодо захисту дітей від сексуальних зловживань та сексуальної експлуатації».

Застарілі концепти релігійної моралі, проникаючи до статей українського законодавства, значно ускладнюють вирішення суспільно важливих завдань. Як приклад можна навести термінологію, пов'язану із проблемою проституції, що закріплена у чинному Кримінальному кодексі України: «вчинення розпусних дій», «місця розпусти», «звідництво», «бузувірство», «статева розпуста» тощо. Не виправить ситуацію, а скоріше, погіршить її, запровадження термінології, відсутньої в міжнародних конвенціях щодо протидії торгівлі людьми та сексуальної експлуатації; термінології, проти якої виступають правозахисні організації з протидії проституції, зокрема використання термінів «секс-робота»,

«секс-працівник», «секс-послуги» тощо. Натомість застосування термінів та визначень з міжнародних конвенцій та Глосаріїв ООН слугуватиме посиленню боротьби з цим явищем, зокрема сприятиме зменшенню попиту на сексуальну експлуатацію і уможливить внесення до Кримінального кодексу України статті про відповідальність покупців в проституції, за прикладом Швеції, Норвегії, Ісландії, Франції, Республіки Ірландії, Канади та Північної Ірландії.

Проте, пошук термінологічної досконалості – справа віддаленої перспективи. На сьогодні, значна частина гендерних визначень у прийнятому в рамках гармонізації з європейським простором законодавстві, не дає можливості навіть визначити об'єкти та суб'єкти правовідносин. На розгляді Верховної ради перебуває законопроект, що передбачає цілковите вилучення з українського законодавства, усталеної у міжнародних нормах, гендерної термінології [6]. Цим же законопроектом знову передбачається покарання за «пропагування одностатевих сексуальних стосунків», що стане ще однією проблемою інформаційного права.

Оскільки стратегія розвитку інформаційного суспільства має супроводжуватись розвитком людських ресурсів [3], сучасна гендерна термінологія, що визначена у законодавстві України, повинна відображати приватний та публічний гендерний зрізи суспільних відносин. Отже, врегулювання міжгендерної взаємодії потребує подальшої соціально-філософської ревізії українського законодавства з урахуванням глобальних процесів та застосуванням наукової термінології гендерних досліджень.

Список використаних джерел:

1. Всеукраїнська рада Церков обговорила з міністром освіти здобутки у галузі інтеграції духовної та світської освіти // Релігія в Україні.- URL:<https://www.religion.in.ua/?do=search>
2. Зустріч із Всеукраїнською радою церков // Вісник Міжфракційного депутатського об'єднання «Рівні можливості», №13, березень 2017. м. Київ, - 13 с.
3. Окінавська хартія глобального інформаційного суспільства. - URL:http://zakon.rada.gov.ua/laws/show/998_163/print
4. Приєднання України до Гаазької конвенції про захист дітей мінімізує ризики комерційних та кримінальних усиновлень. - URL: <https://www.kmu.gov.ua/ua/news/minyust-priyednannya-ukrayini-do-gaazkoyi-konvenciyi-pro-zahist-ditej-minimizuye-riziki-komercijnih-ta-kriminalnih-usinovlen>, 15 березня 2018 р.
5. Про прийняття за основу проекту Закону України про внесення змін до деяких законодавчих актів України щодо захисту прав дітей на безпечний інформаційний простір : постанова Верховної Ради України від 02.10.2012 р. № 5300-VI. - URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45128 .
6. Проект Закону про внесення змін до деяких законодавчих актів України щодо захисту суспільної моралі та традиційних сімейних цінностей № 8442 від 07.06.2018. - URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=64163
7. Сопілко І.А. Особливості тлумачення окремих термінів інформаційного права / Ірина Сопілко // Юридична Україна. – 2013. – № 12. – С. 27–31;

8. Sexual exploitation and prostitution and its impact on gender equality / European Parliament resolution of 26 February 2014 on sexual exploitation and prostitution and its impact on gender equality (2013/2103(INI)). - URL:<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0162>

*Тихонюк О. В., ст. викладач
ФСП КПІ ім. Ігоря Сікорського*

ВИПАДКИ ПОРУШЕННЯ ПРАВА НА ІНФОРМАЦІЮ ПІД ЧАС ЗДІЙСНЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ

Стаття 43 Конституції України проголошує принцип свободи праці — вільне розпорядження людиною своєю здатністю до праці, можливість вільно заробляти собі на життя (при цьому обов'язковість працювати — відсутня).

Чинне законодавство про працю України наголошує, що *працівник має право* реалізувати свої здібності до продуктивної і творчої праці шляхом укладання трудового договору (контракту) з роботодавцем (ч. 2 ст. 21 КЗпП України), а *роботодавець, у свою чергу, не має права* вимагати від працівника виконання роботи, не обумовленої трудовим договором (ст. 31 КЗпП України), а згідно зі статтею 32 КЗпП України під *переведення на іншу роботу* можна провести будь-яку вимогу виконувати роботу, не обумовлену при укладанні трудового договору (контракту), тобто, *будь-яка зміна трудової функції працівника вважатиметься переведенням на іншу роботу*. Але така зміна можлива лише за згодою працівника.

Поширеними *випадками* порушення роботодавцями прав найманих працівників під час *випробування* можна вважати наступні:

1) людину приймають до штату працюючих «з гідною заробітною платою», а насправді – зараховують на мізерну оплату праці, не повідомляючи про це самого працівника. Через декілька тижнів його звільняють, виплачують частку з цієї заробітної платні. У судовому порядку винні дії роботодавця неможливо довести, винуватим в цій ситуації залишається найманий працівник;

2) людину приймають на роботу «з гідною заробітною платою», але «забувають» попередити про випробувальний термін. Забирають трудову книжку та копії інших необхідних документів. Працівник сумлінно виконує свої обов'язки декілька тижнів, після чого його звільняють, повертають трудову книжку без запису про прийняття на роботу. Заробітну плату не виплачують, оскільки людину взагалі не оформляли на дане підприємство, установу, організацію (далі — ПУО). У судовому порядку винні дії роботодавця довести дуже складно, необхідні суттєві докази: або фото робочого місця скривдженого працівника, або фото цього працівника з іншими працівниками на даному ПУО, або колеги - свідки, які погодяться підтвердити наведені докази;

3) людину приймають на роботу, укладають з нею контракт на один місяць із зазначеною мінімальною заробітною платою, а їй «ніби офіційно» пропонують заробітну плату «у конверті». Через місяць працівника звільняють з виплатою йому зазначеної у контракті мінімальної заробітної плати. У судовому порядку провину роботодавця довести неможливо;

4) встановлення *більшого строку* випробування (внесення до Типового трудового договору положення про встановлення випробування при прийнятті на роботу *усім* без винятку *працівникам* строком на 4 або 6 місяців), що суперечить чинному законодавству України про працю, а саме частині 1 та 2 статті 27 КЗпП України, за яким тривалість випробування не може перевищувати одного місяця для *робітників* і, як правило, трьох місяців для *працівників*;

5) прийняття на роботу з випробувальним терміном осіб, яким, згідно частини 3 статті 26 КЗпП України, *заборонено* його встановлювати;

6) встановлення випробування при *переведенні* працівника з однієї посади на іншу або до іншого структурного підрозділу (випробування встановлюється тільки при *прийнятті* на роботу);

7) згідно частини 2 статті 26 КЗпП України на працівників на весь час випробування поширюється законодавство про працю, але жодна зі статей чинного Кодексу законів про працю України *не містить* норм щодо оплати праці при проходженні випробування, а тому роботодавець або встановлює заробітну плату на час випробування у розмірі прожиткового мінімуму, або взагалі відмовляється оплатити працівникові виконувану роботу за весь час випробувального терміну.

Підсумовуючи вищенаведене, можна зробити наступні *висновки*:

1) «*переведенням*» вважається доручення працівникові роботи, що не відповідає його спеціальності, кваліфікації чи посаді, не визначеній трудовим договором;

2) згода працівника на *переведення* потрібна, навіть якщо працівника підвищують у посаді або інша робота краще оплачується;

3) у разі *переведення* працівник має право на передбачені законодавством обов'язкові додаткові виплати у разі змін щодо обсягу чи характеру своїх обов'язків, розміру заробітної плати, тощо;

4) у разі *переведення* на іншу роботу і зміні істотних умов праці працівник має право на передбачені законодавством обов'язкові додаткові виплати, тільки якщо змінюється система та розмір оплати праці, пільги, режим роботи, встановлюється або скасовується неповний робочий час, сполучення професій, змінюються розряди і найменування посади або будь-які інші істотні умови праці;

5) у разі *тимчасового переведення* у зв'язку з *виробничою необхідністю* працівник має право на передбачені законодавством обов'язкові додаткові виплати, тільки під час переведення на нижче оплачувану роботу (зберігається його попередній середній заробіток упродовж двох тижнів з дня переведення); працівник *може бути переведеним* на строк до одного місяця на іншу роботу, не

обумовлену трудовим договором, без його згоди, якщо вона йому не протипоказана за станом здоров'я;

б) *простій у роботі*, тобто, її зупинення, *можливий* у разі відсутності організаційних або технічних умов, необхідних для її виконання; або через невідворотну силу чи інші обставини; працівник *може бути переведений* з урахуванням спеціальності і кваліфікації на іншу роботу на тому ж ПУО, але в тій самій місцевості на строк до одного місяця; відмова працівника від *переведення* у разі *простою* не є порушенням трудових обов'язків;

7) законодавством забороняється переводити працівника на іншу роботу під час його відсутності з поважних причин (хвороба, відпустка, тощо);

8) під час *переміщення*, умови праці та трудова функція залишаються без змін і без згоди працівника (ч. 2 ст. 32); але роботодавець *не має права* переміщати працівника на роботу, протипоказану йому за станом здоров'я;

9) *випробування під час працевлаштування на роботу має двоякий характер, тобто, дає можливість реалізувати право на працю і водночас використовує працю людини, як дешеву робочу силу, заради збагачення роботодавця; а тому можна стверджувати, що законодавча база щодо регулювання інституту випробування вимагає значного доопрацювання та доповнення.*

Список використаних джерел:

1. Конституція України від 28.06.1996. –URL: <http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>.

2. Кодекс законів про працю України від 10.12.1971.–URL: <http://zakon2.rada.gov.ua/laws/show/322-08>.

*Даниленко Н. П., студент
ФСП КПІ ім. Ігоря Сік орського
Науковий керівник:
Фурашев В. М., к.т.н., с.н.с., доцент
КПІ ім. Ігоря Сік орського*

ПОНЯТТЯ, СУТНІСТЬ ТА ПРАВОВА ЗАБЕЗПЕЧЕНІСТЬ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ У СУЧАСНИХ УМОВАХ

Питання забезпечення інформаційного суверенітету в часи постійного зростаючої ролі інформатизації у життєзабезпечення суспільства нині є чи не найголовнішою темою з питань безпеки, на всіх рівнях, у більшості розвинених країн світу. Це обумовлено, в першу чергу, загрозами, які, на жаль, є прихованими від національного законодавства.

Розглядаючи, з точки зору, питання поняття інформаційного суверенітету у сучасності, слід зазначити, що інформаційна безпека в національному законодавстві закріплена на найвищому рівні, тобто в Конституції України - “захист суверенітету і територіальної цілісності України, забезпечення її

економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу” [1].

І якщо проаналізувати вищезазначене, то можна прийти до висновку, що інформаційна безпека розглядається на одному рівні з такими невід’ємними атрибутами державності як суверенітет і територіальна цілісність.

Звісно, крім Конституції України є більш чітке та виокремлене поняття, а саме: “Інформаційний суверенітет держави - здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави” [2].

Однак, на відміну від законодавчого, чітко визначеного поняття, до сутності інформаційного суверенітету, для більшості політиків та простих громадян у його розумінні лежить величезна прірва.

Складність трактування сутності інформаційного суверенітету, в першу чергу, полягає в складності відмежування шляхів реалізації захисту інформаційного суверенітету держави від порушення тих чи інших прав громадян.

Яскравим прикладом проблематики розмежування шляхів реалізації та порушення прав є заборона так званих “інформаційно-токсичних” сайтів, коли з одного боку ця дія покликана виключно з питань національної інформаційної безпеки та викликана в першу чергу національними інтересами, а з іншого боку, в свою чергу, постає проблематика роз’яснення населенню, що насамперед це є не утиск прав та свобод громадян на спілкування та інформацію, а саме державний захист громадян від негативного впливу того чи іншого сайту.

Найчастіше ця проблематика проявляється в країнах з поширеним серед населення правовим нігілізмом чи низьким рівнем, або взагалі відсутністю національної ідеї.

Та національне питання не єдиний аспект проблематики розмежування, адже на міжнародній арені взагалі неможливо уникнути критики та не зустріти супротив проти тих чи інших дій, які стосуються насамперед національних інтересів, не кажучи вже про те, що навіть союзники можуть розкритикувати такі кроки посиляючись на утиск прав і свобод громадян та зменшенням рівня демократії в країні.

Тож проаналізувавши вищезазначене можна прийти до висновку, що дотримання межі та балансу в питанні шляхів реалізації є досить непростим завданням.

Однак, це стосується не лише заборон “токсичних” сайтів, через те що це лиш один із шляхів реалізації, інші варіанти зазвичай зустрічають ще більший опір від правозахисників, до таких заборон можна віднести:

– заборона певних телевізійних каналів, які прямо чи опосередковано здійснюють пропагандистську діяльність на користь чужої країни чи провокують сепаратистські настрої;

- заборона певних газет, які теж прямо чи опосередковано створені задля розмиття національної єдності та ідеї;
- та інших способів чи засобів впливу на соціум, які є загрозою для інформаційного суверенітету держави.
- Як вже зазначалось, цілі та завдання захисту інформаційного суверенітету полягають у:
 - здійсненні контролю та регулювання потоків інформації з-поза меж держави;
 - захисту національного інформаційного простору від негативного впливу сусідніх країн;
 - гарантування національної безпеки держави.

Є досить не чіткими шляхи реалізації, тобто такими, які дають змогу по різному трактувати їх кожному по своєму, цим самим ускладнюючи головну задачу інформаційного суверенітету - державну та національну інформаційну незалежність.

Також проблематика постає в тій частині, де йдеться про національну ідею та національний інтерес, адже ці питання тісно пов'язані, а отже існування порізну не можливо. Але відсутність чіткого їх визначення та закріплення в національному законодавстві взагалі провокує трактування цих понять, задля зручного виправдання тих чи інших дій пов'язаних зі шляхами реалізації чи навіть самими завданнями та цілями інформаційного суверенітету.

Нормативно-правова забезпеченість інформаційного суверенітету є “камнем спотикання”, як в національному законодавстві кожної країни, так і в міжнародному праві.

Проте, по відношенню до цього питання та його нормативно-правовому забезпеченню в Україні, дослідивши законотворчий шлях, можна сформулювати думку про те, що забезпеченість інформаційного суверенітету є питанням навіть більш розмитим ніж шляхи його реалізації.

Вперше визначення “інформаційний суверенітет України” було закріплено в статті 53 Закону України “Про Інформацію” від 02.10.1992 де зазначалось, що “основою інформаційного суверенітету України є національні інформаційні ресурси.

До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення.

Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами” [3].

Також в статті 54 Закону України “Про інформацію” зазначаються гарантії забезпечення інформаційного суверенітету - “виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету; створенням національних систем інформації; встановленням режиму доступу інших держав до інформаційних ресурсів України; використанням

інформаційних ресурсів на основі рівноправного співробітництва з іншими державами” [3].

Але, ці дві статті зникають при редакції Закону від 06.01.2011.

Через що єдиним до розуміння сутності, а точніше єдиними поняттями інформаційного суверенітету України є ті, що знаходяться в проектах Закону України “Про інформаційний суверенітет та інформаційну безпеку України”, представлені народним депутатом Лук’яненком Л.Г. трактуванні “права держави на формування і здійснення національної інформаційної політики відповідно до Конституції і законодавства України, міжнародного права в національному інформаційному просторі України” [4], а також народним депутатом Чижом І.С. – “невід’ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку і здійсненні національної інформаційної політики відповідно до Конституції та чинного законодавства України, міжнародного права в національному просторі України” [5].

На даний час поняття “інформаційний суверенітет держави” законодавче визначене Законом України “Про національну програму інформатизації” - “інформаційний суверенітет держави - здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави” [2].

Отже, якщо підсумувати все вище викладене можна прийти до такого висновку:

– національне законодавство України в сфері забезпечення інформаційного суверенітету держави хоч і закріплена державна політика, але вона є досить не чіткою та фрагментарною;

– в час зростання кількості та видів загроз інформаційному суверенітету держави питання формування та тлумачення поняття інформаційного суверенітету є не менш важливим ніж його нормативно-правове забезпечення, адже без нього неможливе коректне встановлення шляхів реалізації захисту того ж національного інформаційного суверенітету.

Список використаних джерел:

1. Конституція України. –URL: <http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#n4215>
2. Закон України “Про національну програму інформатизації”. – URL: <http://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80>
3. Закон України “Про інформацію”. –URL: <http://zakon.rada.gov.ua/laws/show/2657-12/ed20110106#o360>
4. Проект Закону України “Про інформаційний суверенітет та інформаційну безпеку України”. – URL: <http://uacm.kharkov.ua/ukr/index.shtml?ulaws/usuvetr.htm>

Проект Закону України “Про інформаційний суверенітет та інформаційну безпеку України”. –URL:
http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6670

*Николаєнко Г. В., аспірант
НДІІП НАПрН України*

ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ МЕЖ ДЕРЖАВНОГО СЕКТОРУ В СТАТИСТИЦІ УКРАЇНИ

Проблема визначення меж державного сектору в економічній системі країни має системний характер, оскільки це тягне за собою значні структурні зрушення у макропоказниках, що відображають зокрема стан державних фінансів. Приміром, величина боргу державного сектору економіки буде змінюватись залежно від величини останнього, оскільки врахування активів і зобов'язань фондів соціального страхування чи місцевих органів влади значно вплине на структуру та величину сектору.

Звернемося до підходів, що використовуються в ЄС. Європейська система рахунків (національних і регіональних) 1995 року (ЄСР 95) у структурі сектору державного управління виділяє ті самі чотири елементи, що і СНР та СДФ 2001, а саме: центральний уряд (centralgovernment), регіональні органи влади (stategovernment), органи місцевого управління (localgovernment), фонди соціального забезпечення (socialsecurityfunds). На жаль, у ЄСР 95 відсутнє єдине визначення державного боргу, хоча там містяться загальні підходи до його оцінки. Пунктом 7.01 Директиви 2223 від 25 червня 1996 р. передбачено, що – статті активів і зобов'язань записані в балансовому звіті повинні бути оцінені за ринковими цінами на дату балансу [1].

Тобто зобов'язання сектору державного управління, що подаються у балансовому звіті за обліковий період, повинні бути оцінені за ринковими цінами на дату балансу. З огляду на це, державний борг повинен дорівнювати сумі всіх зобов'язань сектору державного управління, а саме: готівки та депозитів, цінних паперів, крім акцій, фінансових деривативів, позик, іншої кредиторської заборгованості, тощо [2, с. 197]. Водночас, згідно з СФД 2001, «валова боргова позиція» сектору державного управління не включає зобов'язань з похідних фінансових інструментам, тобто є певні розбіжності між цими стандартами [3].

Проте Стаття 2 Протоколу № 20 «Про процедуру надмірного дефіциту» Договору про заснування ЄС [4] дає чітке визначення державного боргу (governmentdebt): борг –це непогашена загальна номінальна величина валового боргу на кінець року, що консолідована між та в середині підсекторів сектору державного управління. Слід також відмітити, що у випадку оцінки державного боргу як суми номінальної вартості зобов'язань до його величини не можуть бути

включені похідні фінансові інструменти, оскільки вони не мають номінальної вартості, як інші боргові інструменти.

Аналіз показує, що як у системі СДФ 2001, так і в ЄСР 95 визначені принципи оцінки величини державного боргу, в т.ч. законодавчими актами (в ЄС). Незважаючи на метод оцінки (ринкова чи номінальна), державним боргом є загальна сума зобов'язань сектору державного управління.

Виникає запитання: на якій основі визначається величина державного боргу України, його структура, метод оцінки та ступінь консолідації зобов'язань державного сектору України? У статті 2 Бюджетного кодексу України дано визначення державного боргу, а саме: «загальна сума заборгованості держави, яка складається з усіх випущених і непогашених боргових зобов'язань держави, включаючи боргові зобов'язання держави, що вступають в дію в результаті виданих гарантій за кредитами, або зобов'язань, що виникають на підставі законодавства або договору» [5]. Причому боргові зобов'язання держави можуть утворитись тільки внаслідок державного запозичення.

Визначення, подане у Бюджетному кодексі України, значно звужує величину державного боргу, оскільки передбачає, що державним боргом є виключно зобов'язання держави – тобто центрального уряду (centralgovernment). Крім того, для віднесення зобов'язання було віднесено до державного боргу воно повинно утворитися внаслідок запозичення чи вступу в силу державних гарантій. А це не відповідає підходам, визначеним в СДФ 2001 і ЄСР 95.

Визначення, подане в Бюджетному кодексі, не враховує зобов'язання інших підсекторів сектору державного управління, а саме: боргів регіональних органів влади, органів місцевого управління, фондів соціального забезпечення. Так, влада м. Києва успішно провела ряд емісій муніципальних облігацій, у тому числі й єврооблігацій. Борг міста, відповідно до принципів СДФ 2001 і ЄСР 95, відноситься до державного боргу, а згідно з законодавством України не є державним боргом. Тобто для приведення у відповідність із міжнародними стандартами статистики державних фінансів, щодо визначення величини державного боргу, необхідно в першу чергу внести зміни до Бюджетного кодексу України, що також тягне за собою внесення змін до бюджетної класифікації та інших змін у нормативно-правових актах.

Для керівних органів ЄС достовірне та точне визначення величини державного боргу країни-члена ЄС є дуже важливим, оскільки стаття 104 Договору про заснування ЄС та Протокол № 20 визначають вимоги до величини державного боргу та дефіциту, зокрема відношення державного боргу до ВВП має бути меншим за 60%, а державний дефіцит не повинен перевищувати 3% ВВП.

Проте, як показує аналіз, методика розрахунку величини державного боргу України є іншою порівняно з методикою, затвердженою законодавством ЄС та ЄСР 95, а це в свою чергу призводить до заниження цього показника для України.

Список використаних джерел:

1. Council Regulation (EC) № 2223/96 of 25 June 1996 on the European system of national and regional accounts in the Community // *Official Journal*. - 30.11.1996. - L 310. - P. 1-469.
2. ESA95 Manual on government deficit and debt. — Luxemburg, Eurostat, 2002. — 243 p.
3. Government Finance Statistics Manual. - Washington : International Monetary Fund, 2001. - 199 p.
4. Protocol № 20 on the excessive deficit procedure / Annexed to the Treaty establishing the European Community (Maastricht consolidated version) // *Official Journal C 224*. - 31.08.1992. - P. 79.
5. Бюджетний кодекс України. URL:<http://zakon.rada.gov.ua/laws/show/2456-17>.

Фабрикантов М. І., студент
ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Пашов Р. І., к.ф.н., ст. викладач
ФСП КПІ ім. Ігоря Сікорського

ПРАКТИКА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ РЕЗУЛЬТАТИВНІСТЮ ДЕРЖАВНОЇ СЛУЖБИ

Останнім часом результати спеціальних наукових досліджень пропагують думку, що суспільний розвиток в першу чергу залежить від стану розвитку та функціонування державних інститутів, їх націленості на результат та якісні перетворення. Ефективність економіки, якість управління, характер і зміст соціальних комунікацій, рівень розвитку людського потенціалу знаходяться в складній взаємозалежності та вимагають постійної модернізації відповідно до викликів епохи. Тому, застосування методики управління, орієнтованого на результат, допомагає визначити і підвищити ефективність державного управління і, як наслідок, забезпечити сталий розвиток суспільства та всіх його сфер.

В основі методики управління, орієнтованого на результат, лежить практика використання показників, що дозволяють простежити досягнення результатів по відношенню до поставлених цілей з урахуванням наявних ресурсів і визначити якість досягнутих результатів. Особливість даної методики полягає в тому, що предметом моніторингу мають бути не самі дії владних структур, не стільки продукт діяльності, скільки кількісні і якісні результати цієї діяльності. Варто відзначити, що при оцінюванні роботи державних службовців, зокрема, та структур, загалом, – думка населення є одним з головних критеріїв, що дозволяють оцінити досягнутий результат. Особливо важливим даний фактор постає при реалізації соціальних проектів, коли у населення ще не склалося враження про якість тієї чи іншої пропонованої послуги. При визначенні

показника результативності необхідно оцінити, наскільки глибоко за допомогою даного показника можна проаналізувати ситуацію, відшукати причини і шляхи вирішення проблем, що виникли.

Важливим етапом реалізації методики управління, орієнтованого на результат, є процес моніторингу результативності. Тут можна виділити три моменти: збір інформації про досягнуті результати; оцінка і аналіз отриманих результатів шляхом зіставлення з плановими значеннями; надання звітності особам, які приймають рішення, для оцінки ефективності та внесення необхідних коригувань

Управління за результатами включає в себе ряд внутрішньо взаємопов'язаних напрямків, які охоплюють практично всі аспекти державного управління: відповідальну фінансову політику, бюджетування за результатами, оптимізацію організаційних структур, залучення кваліфікованих кадрів, впровадження конкурентних засад при наданні державних послуг.

Тим не менше, використання методики управління, орієнтованого на результат, дуже актуально в теперішніх умовах процесу децентралізації. Інтерес до нього зростає, причому ініціаторами частіше виступають не тільки аналітичні центри, спеціалізовані консультанти, некомерційні організації, а й провідні фахівці органів місцевого самоврядування, зацікавлені в незалежній і об'єктивній експертизі своїх управлінських рішень. Розглядаючи оціночну діяльність в контексті роботи державної служби та її соціально-економічного розвитку, можна зробити висновок, що цей інтерес став наслідком розширення проектного та програмного підходу в роботі на місцевому рівні, прагнення підвищити її ефективність, впровадити нові методичні розробки. Багато в чому зростання популярності оціночних інструментів на місцях пояснюється поступовим підвищенням кваліфікації державних кадрів. Це виражається як у вдосконаленні їх професійних знань, так і в певній зміні менталітету. Все більше число державних працівників, в тому числі і в невеликих локальних утвореннях, демонструють системний підхід до розвитку місцевої економіки і соціальної сфери. Поширення методики управління, орієнтованого на результат, безсумнівно, повинно сприяти більш високому рівню розвитку державної служби в нашій країні.

Таким чином, ефективне застосування принципів управління за результатами передбачає наявність, з одного боку, ефективного розвитку економічних процесів в регіоні, з іншого – належним чином вибудованої інформаційної системи управління, яка забезпечувала б відповідальних осіб на всіх рівнях ієрархії управління інформацією про розвиток регіону в цілях оцінки його ефективності і створення подальших управлінських рішень. На сьогоднішній день в Україні не розроблена методологія, яка використовується при управлінні за результатами, яка ґрунтувалася б на чіткій моделі соціально-економічного розвитку, орієнтованої на результат з комплексом показників. Це є основною перешкодою на шляху створення інформаційної системи управління країною і, відповідно, впровадження принципів управління за результатами. Проте,

позитивні зрушення не можна не помітити, тому чітке реформування адміністративної сфери та впровадження новітніх моделей управління дає можливість для досягнення високого рівня державного управління в Україні.

Розділ 7 *РОЗВИТОК ІНФОРМАЦІЙНОГО ПРАВА ЯК НАУКИ В
КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ТА ЄВРОАТЛАНТИЧНОЇ
ІНТЕГРАЦІЇ УКРАЇНИ*

*Костенко О. В., аспірант
НДШІП НАПрН України*

**ШЛЯХИ ПРАВОГО РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ
ПОСЛУГ В ЄВРОПЕЙСЬКОМУ СОЮЗІ**

Бурхливий розвиток інформаційних технологій, який людство переживає останніми роками, створив нові суспільні відносини. Це, в свою чергу, дало підґрунтя для нових правових, економічних, політичних, духовних, професійних та інших відносин, що суттєво зменшило соціально-демографічні, соціально-групові, соціально професійні та інші бар'єри між суб'єктами правовідносин. Фактично відбулася революційна цифровізація людства, в наслідок якої кожен громадянин отримав можливість користуватися інформаційними технологіями і ресурсами. Тривалий період більшість інформаційних даних створювалися, використовувалися, зберігалися та знищувалися знеособлено.

Виходячи з вищезазначеного, актуальним на сьогодні є питання ідентифікації суб'єкта в інформаційно-технологічному просторі. Воно вирішується за допомогою використання електронних підписів та електронних довірчих послуг. Однак неврегульованість співіснування різних правових систем та різна кваліфікація базових дефініцій в сфері електронних довірчих послуг та цифрового підпису в законодавствах різних країн, а також невизначеність правового регулювання визнання іноземних електронних довірчих послуг, та транскордонного визнання сертифікатів електронних підписів наразі є актуальною проблемою.

Як свідчить світова практика, створення або урегулювання правових норм для вирішення проблеми транскордонного визнання електронних довірчих послуг та електронних підписів може відбуватися за можливими правовими режимами:

- заснованими на міжнародних угодах (конвенціях) та/або на прямо застосовуваних міжнародних нормах;
- заснованих на комерційних угодах та/або загальній торговельній практиці;
- без спеціального міжнародного регулювання.

На міжнародному рівні роботи з правової стандартизації в галузі електронного обміну даними, торгівлі та електронного підпису здійснюються одночасно різними інституціями. Наразі суттєвого прогресу досягнуто саме Європейським Союзом.

Європейським парламентом та Радою Європи було прийнято «Регламент (ЄС) №910/2014 Європейського парламенту та Ради Європи щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС» (далі – Регламент, eIDAS) [1]. Наразі він є базовим нормативно-правовим документом, який створено як регуляторний акт, що впорядковує суспільні відносини, які розвиваються паралельно процесові удосконалення інфраструктури відкритого ключа ЄС. В даному випадку eIDAS є прикладом нормативно-правового акту для суміщеної системи, що ґрунтується на стандартах Міжнародної організації зі стандартизації (ISO) та національних законодавствах країнах-членах Європейського Союзу.

Регламент встановлює нові вимоги до забезпечення надійності електронних довірчих послуг між приватними організаціями, громадянами та державними органами в ЄС.

Однією із ключових правових проблем впровадження Регламенту стала складність реалізації електронної ідентифікації як елемента електронних довірчих послуг. Вирішення цієї проблеми покладено на проект STORK (Secure identity across borders linked), метою якого є створення та впровадження єдиної загальноєвропейської системи електронної ідентифікації. Проект анонсувало 19 партнерів з 11 країн, однак згодом число партнерів збільшилася до 58.

Перша частина проекту STORK 1.0 складалась з 5 пілотних проектів: SaferChat (безпечний чат в транскордонному контексті), Student Mobility (студентська мобільність, online доступ до європейських університетів), Delivery (електронна доставка повідомлень громадянин-держава), Change of Address (зміна адреси, переміщення іноземців) та ECAS integration (European Commission Authentication Service — інтеграція сервісів європейської служби аутентифікації).

Наступна частина, STORK 2.0, реалізує чотири пілотні електронні послуги, орієнтовані на наступні стратегічні напрямки: e-Banking, e-Health, e-Learning та e-Government for Business.

E-Banking. Дана послуга надає можливість фізичним та юридичним особам вільно користуватися послугами іноземних банків через їхні web-сервіси (відкривати банківські рахунки, робити фінансові операції).

E-Health. Даний сервіс дозволить не тільки лікарям отримувати доступ до інформації про пацієнта, що зберігається на стороні країни пацієнта, але й самому пацієнту отримувати дані зі свого облікового запису. Використання E-Health дозволить зменшити вартість та підвищити якість послуг з охорони здоров'я за рахунок залучення інформаційних технологій при направленні на лікування в іншу країну.

E-Learning. Воно дозволяє будувати сервіси на основі загальної платформи, за допомогою яких громадяни, компанії та державні структури можуть взаємодіяти між собою:

- створити транскордонні послуги, засновані на обміні атрибутів, що засвідчують особу (для електронного навчання та опитувань громадської думки).
- полегшити використання загальнодержавної інформації користувачами, державними і приватними організаціями;
- показана можливість інтеграції інших існуючих послуг щодо перевірки будь-яких сертифікатів шляхом «зарахування в публічні реєстри» або «One-stop shop».

На сьогоднішній день: проведено огляд і детальний аналіз суспільних інфраструктур електронної ідентифікації для довірчих послуг в кожній країні-члені ЄС; зроблено аналіз правових норм, включаючи ключові поняття, процедуру покладання на фізичних та юридичних осіб правових повноважень з використанням електронних засобів, в тому числі електронного підпису; виявлено правове проблемне питання захисту даних, в тому числі персональних; запропоновано QAA модель (Quality Authentication Assurance - забезпечення якісної аутентифікації) по досягненню допустимих рівнів якості для різних рішень електронної ідентифікації.

В рамках проекту проаналізовані основні юридичні ризики в питаннях вирішення спорів, захисту даних, відповідальності, гарантій рівня обслуговування, надання повноважень тощо. Ці правові розбіжності потім будуть порівнюватися з існуючими національними законодавствами та Регламентом. Проблемні питання планується розв'язати шляхом пошуку та внесення відповідних правових норм до національного законодавства законотворчим органом кожної з країн-учасниць в кожному конкретному випадку. Питання транскордонного використання повноважень означає, що повноваження, надані особі в країні А, повинні мати силу і застосовуватися в країні В. Іншими словами, країна В повинна визнавати формат і законність повноважень, наданих у країні А. Це відбувається у разі, якщо обидві країни пов'язані міжнародним договором або законодавством ЄС.

Фактично Європейський Союз наполегливо і поступово здійснює формування електронних довірчих послуг, які користуються попитом і популярністю у населення, визначає тестовий перелік довірчих послуг, що генеруються органами державної влади та місцевого самоврядування з метою впорядкування національних нормативних баз до єдиного типового формату, але з урахуванням особливостей національних юрисдикцій. Проект STORK — це елемент модернізації правової та технічної нормативної бази, що сприятиме регулюванню використання країнами-членами ЄС електронних довірчих послуг та електронних підписів.

Список використаних джерел:

1. Regulation (eu) № 910/2014 of the european parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.—URL: <https://eur->

*Пасічник В. В., аспірант
ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Бевз С. І., к.ю.н., доцент
ФСП КПІ ім. Ігоря Сікорського*

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕКОНОМІЧНОЇ КОНКУРЕНЦІЇ В СФЕРІ ЗОВНІШНЬОЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

Інформаційне забезпечення захисту економічної конкуренції в сфері зовнішньоекономічної діяльності є необхідною умовою для здійснення Міністерством економічного розвитку і торгівлі України (надалі – Міністерство) та Міжвідомчою комісією з міжнародної торгівлі (надалі – Міжвідомча комісія) адміністративно-процесуальної діяльності з ефективного захисту суб'єктів господарської діяльності України від неправомірних, протиправних дій іноземних суб'єктів господарської діяльності як на території України, так і за її межами.

Особливо важливе значення інформаційне забезпечення в цій сфері має при прийнятті Міжвідомчою комісією правових актів індивідуальної дії щодо застосування певних заходів торговельного захисту. Адже прийняття в зовнішньоекономічній діяльності будь-якого адміністративно-правового акту потребує наявності певних інформаційних ресурсів й налагодженої між заявниками, відповідним органом виконавчої влади в Україні та Міністерством, Міжвідомчою комісією ефективною інформаційною комунікації. Саме тому питання забезпечення Міністерства, Міжвідомчої комісії повною та достовірною інформацією для ефективного здійснення захисту суб'єктів господарської діяльності України від проявів недобросовісної конкуренції в сфері зовнішньоекономічної діяльності є досить актуальним.

Частина 1 ст. 5 Закону України «Про застосування спеціальних заходів щодо імпорту в Україну» визначає у разі, якщо тенденція зростання обсягів імпорту в Україну може викликати необхідність застосування передбачених цим Законом заходів, центральний орган виконавчої влади, що забезпечує формування та реалізує державну податкову і митну політику, відповідний орган виконавчої влади в Україні інформує про це Міністерство. Міністерство може за власною ініціативою зібрати таку інформацію [1]. Вважаємо за доцільне закріплення на законодавчому рівні можливості інформування та забезпечення Міністерства своєчасною, повною та достовірною інформацією відповідним органом виконавчої влади в Україні. Адже інформування Міністерства про факти зростання імпорту в Україну, що заподіює значну шкоду або загрожує

заподіянням значної шкоди національному товаровиробнику, надасть можливість Міністерству швидкого реагування та завчасного початку проведення спеціального розслідування.

Крім закріплення на законодавчому рівні можливості інформування Міністерства про факти зростання імпорту в Україну, дане Міністерство має право збирати таку інформацію самостійно – за власною ініціативою. Міністерство вправі також вимагати від органів виконавчої влади в Україні під час проведення спеціального розслідування надання необхідної інформації для ефективного здійснення адміністративно-процесуальної діяльності – проведення спеціального розслідування. Зібрання всієї необхідної інформації надає можливість Міністерству підготувати повний достовірний звіт про результати спеціального розслідування та подати на розгляд Міжвідомчої комісії, яка в подальшому може прийняти рішення про застосування спеціальних заходів. Зазначене підтверджується тим, що на підставі наданої/зібраної Міністерством інформації та досліджуваної Міжвідомчою комісією в 2018 році було прийняте рішення про застосування спеціальних заходів щодо імпорту в Україну кислоти сірчаної та олеуму незалежно від країни походження та експорту.

Щодо інформування заявниками – суб'єктом господарської діяльності Міністерства про наявність факту демпінгового імпорту в Україну та з метою запобігання шкоді, заявники вправі повідомити про це Міністерство шляхом подання відповідної скарги. Відомості, які повинні міститися в скарзі, наведені в ч. 4 ст. 12 Закону України «Про захист національного товаровиробника від демпінгового імпорту» [2]. Зазначимо, що Міністерство не наділене можливістю за власною ініціативою здійснювати збір інформації щодо наявності на митній території України демпінгу до початку порушення антидемпінгової процедури. Це пояснюється тим, що обов'язковою умовою порушення зазначеної процедури є наявність скарги національного товаровиробника. Міністерство вправі лише надіслати експортерам, імпортерам, іншим сторонам антидемпінгового розслідування, яких вважає за доцільне залучити до участі в антидемпінговому розслідуванні, або компетентним органам країни експорту запитальники з метою отримання необхідної інформації та вимагати від заінтересованих сторін надання інформації, необхідної для проведення антидемпінгового розслідування. В 2018 році на підставі дослідженої Міністерством та Міжвідомчою комісією інформації Міжвідомчою комісією було прийнято такі адміністративно-правові акти про застосування заходів торговельного захисту: а) про зміну антидемпінгових заходів щодо імпорту в Україну нітрату амонію (аміачної селітри) походженням з Російської Федерації; б) про застосування остаточних антидемпінгових заходів щодо імпорту в Україну карбамідо-формальдегідної продукції походженням з Російської Федерації.

Як вбачається з вищевикладеного в основу інформаційного забезпечення захисту економічної конкуренції в сфері зовнішньоекономічної діяльності покладена категорія «інформація». Під якою слід розуміти 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 [3].

Як вказує О.В. Харенко розширений перелік форм, вигляду та носіїв збереження відомостей, що закріплені законодавцем у даній нормі, є ознакою превентивного засобу попередження колізій у застосуванні терміну у правових відносинах. Також таке визначення можна розуміти як приклад того, що поняття «інформація» доцільно розглядати через форми її подання, серед яких розрізняють – але не обмежуються – символічну, текстову, графічну, числову, звукову та комбіновану форми, де дорожні знаки, книги, документи, преса, ілюстрації, фотографії, формули, звукові записи, пояснення осіб, консультації, висловлювання, повідомлення, публічні виступи, кінофільми, відеофільми тощо – способи подачі інформації [4, с. 121].

Враховуючи вищевикладене, зазначимо, що під інформаційним забезпеченням захисту економічної конкуренції в сфері зовнішньоекономічної діяльності визначається сукупність прийомів та способів, спрямованих на отримання, збирання, аналізу, дослідження Міністерством необхідної інформації для здійснення ефективної адміністративно-процедурної діяльності (спеціального розслідування, антидемпінгової процедури, антидемпінгового розслідування) та прийняття Міжвідомчою комісією рішень щодо застосування певних заходів торговельного захисту.

Список використаних джерел:

1. Закон України «Про застосування спеціальних заходів щодо імпорту в Україну» N 332-XIV від 22 грудня 1998 року. URL: <http://zakon.rada.gov.ua/laws/show/332-14>.

2. Закон України «Про захист національного товаровиробника від демпінгово імпорту» N 330-XIV від 22 грудня 1998 року. URL: <http://zakon.rada.gov.ua/laws/show/330-14>.

3. Закон України «Про захист економічної конкуренції» N 2210-III від 11 січня 2001 року. URL: <http://zakon.rada.gov.ua/laws/show/2210-14>.

4. Харенко О.В. Поняття «інформація» в юридичній науці та законодавстві України // Часопис Київського університету права. № 3, 2014. - С. 119-124.

Наукове видання

ІНФОРМАЦІЙНЕ ПРАВО: СУЧАСНІ ВИКЛИКИ І НАПРЯМИ РОЗВИТКУ

Матеріали першої науково-практичної конференції 18 жовтня 2018 року

(Українською та російською мовами)

В авторській редакції
Комп'ютерна верстка авторська

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Перемоги, 37,
м. Київ, 03056

Підп. до друку 23.11.2018. Формат 60×841 /16. Папір офс. Гарнітура Times.
Спосіб друку – ризографічний. Ум. друк. арк. 11,39. Обл.-вид. арк. 18,94. Наклад 100 пр.
Зам. № 18-135.

КПІ ім. Ігоря Сікорського, Видавництво «Політехніка»,
вул. Політехнічна, 14, корп. 15 м.
Київ, 03056 тел.
(044) 204-81-78