



Комітет Верховної Ради України з питань цифрової трансформації

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

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет соціології і права**

Інтернет речей: проблеми правового регулювання та впровадження

**Матеріали III науково-практичної конференції
21 листопада 2019 р.
м. Київ**

**Київ
КПІ ім. Ігоря Сікорського
2019**

- I-73 **Інтернет речей: проблеми правового регулювання та впровадження :**
Матеріали III наук.-практ. конф., 21 лист. 2019 р., м. Київ. / Упоряд. : В. М. Фурашев,
С. О. Дорогих, С. Ю. Петряєв. – Київ : КІП ім. Ігоря Сікорського, Вид-во
«Політехніка», 2019. – 180 с.
ISBN 978-966-622-977-2

Матеріали конференції присвячені розгляду питань упровадження та використання технологій Інтернету речей у різних сферах суспільної діяльності; правових аспектів ризиків та бар'єрів щодо впровадження технологій Інтернету речей; проблем правового регулювання та юридичної відповідальності в умовах застосування технологій Інтернету речей, а також питань інноваційного застосування ІКТ в юридичній діяльності та проблем вдосконалення законодавства з питань інформатизації, телекомунікації, користування радіочастотним ресурсом, захисту персональних даних, інфраструктурної безпеки, кібербезпеки тощо.

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

Доповіді учасників конференції можуть бути корисними для спеціалістів у сферах правотворення, правозастосування та правоохоронної діяльності, фахівців різних галузей права, науково-педагогічних працівників та здобувачів вищої освіти.

УДК 34:004](06)

Матеріали подано в авторській редакції

Упорядники: В. М. Фурашев, С. О. Дорогих, С. Ю. Петряєв

Оформлення обкладинки:

Лабораторія технічної естетики та дизайну ФСП КІП ім. Ігоря Сікорського
designlab.kpi.ua@gmail.com

Д. В. Балашов (balashov.dim@gmail.com)

Рекомендовано до друку:

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

Протокол № 9 від 05.12.2019 р.

Вченою радою факультету соціології і права

*Національного технічного університету України «Київський політехнічний інститут
імені Ігоря Сікорського». Протокол № 4 від 25.11.2019 р.*

ISBN 978-966-622-977-2

© Верховна Рада України, 2019

© Науково-дослідний інститут інформатики
і права НАПрН України, 2019

© КІП ім. Ігоря Сікорського (ФСП), 2019

© Колектив авторів, 2019

Наукове видання

Інтернет речей: проблеми правового регулювання та впровадження

Матеріали III науково-практичної конференції
21 листопада 2019 р.,
м. Київ

*В авторській редакції
Комп'ютерна верстка упорядників*

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

Темплан 2019, поз. 3-3-011

Підп. до друку 27.12.2019. Формат 60×84^{1/16}. Папір офс. Гарнітура Times.
Спосіб друку – ризографічний. Ум. друк. арк. 10,46. Обл.-вид. арк. 17,40. Наклад 90 пр.
Зам. № 19-158.

КПІ ім. Ігоря Сікорського, Видавництво «Політехніка»,
вул. Політехнічна, 14, корп. 15
м. Київ, 03056
тел. (044) 204-81-78

ЗМІСТ

Баранов О. А., Інтернет речей і право: погляд у майбутнє	7
Мельниченко А. А., Майбутнє освіти в епоху штучного інтелекту та Інтернету речей.....	13
Ткачук Т., Інтернет-речі: від фантастики минулого до реалій сьогодення.....	15
Жиляєв І., Деякі проблеми правового регулювання діяльності науковців на ринку новітніх технологій.....	19
Харитонов Є., Харитонova О., Правовідносини та штучний інтелект: «суб'єктивізація» об'єкту.....	23
Коломієць Т., Проблеми правового регулювання розвитку штучного інтелекту	27
Дранник В., Застосування Інтернету речей у різних сферах життєдіяльності людства.....	30
Нашинець-Наумова А., Інтернет речей: реалії сьогодення.....	31
Антузінська К., Реалізація масових та критичних IoT-проектів (екосистем технологій Інтернету речей): правовове регулювання у перспективі.....	34
Доронін І., Самоорганізація як регулятор	39
Каздобіна Ю., Права людини та інтернет речей: виклики державного регулювання.....	42
Гребенюк М., Проблеми правового регулювання застосування технологій IoT.....	47
Мисливий В., Правове регулювання безпілотного автотранспорту.....	49
Жиляєв І., Фурашев В., Проблеми національного законодавчого регулювання новітніх ІКТ (на прикладі Інтернету речей)	54

<i>Забара І.,</i>	
До питання визначення проблематики міжнародно-правової відповідальності за правопорушення при використанні новітніх інформаційно-комунікаційних технологій.....	58
<i>Гордієнко С.,</i>	
Бути, чи не бути збалансованому розвитку людського капіталу в Україні?.....	61
<i>Головко О.,</i>	
Загрози правам людини: окремі аспекти використання технологій IoT.....	65
<i>Мошко М., Прозоров А.,</i>	
Забезпечення прав і свобод людини і громадянина в умовах використання технологій IoT	69
<i>Телька А., Безкоровайна Ю.,</i>	
Технології Інтернет речей на захист і права на приватність.....	72
<i>Зуєв В., Антонець К.,</i>	
Бенчмаркінгова природа впровадження технологій Інтернету речей у соціальній роботі.....	74
<i>Некрутенко В.,</i>	
Privacy of Things: соціально-правові питання захисту персональних даних у сфері Інтернету Речей.....	78
<i>Костенко І. В.,</i> Система загроз та ризиків конфіденційності персональних даних при застосуванні технологій Інтернет речей.....	82
<i>Коваль В.,</i>	
Правові умови захисту персональних даних на господарюючих суб'єктах, які здійснюють господарську діяльність в мережі Інтернет.....	84
<i>Некіт К.,</i>	
Персональні дані як валюта: трансформації цифрової доби.....	88
<i>Скаржинський В.,</i>	
Специфіка захисту персональних даних в умовах розвитку інтернету речей.....	93
<i>Крилова Ю.,</i>	
Проблеми правового регулювання захисту персональних даних в контексті Інтернет речей	98
<i>Ворушило С.,</i>	
Управління мережею інтернет в контексті національної та міжнародної безпеки.....	101

Шрамко С., Використання Інтернету речей (IoT) у забезпеченні громадської безпеки: постановка проблеми.....	105
Гоц О., Інформаційна безпека і сучасність.....	107
Гуртовенко С., Поняття та класифікація викликів і загроз інформаційної безпеки особи.....	112
Гречана А., Сучасні тенденції кіберзлочинності в Україні.....	115
Коркач Д. В., Ткаченко Д. Д., Кібербезпека локальних мереж підприємств.....	118
Благодарний А., До питання вдосконалення стратегічних комунікацій в діяльності правоохоронних органів України.....	121
Кунєв Ю., Славка А., Об'єкт і предмет інформаційного права.....	124
Бортник Р., Новицька Н.Б., Проблеми використання технології блокчейн в інформаційному праві.....	128
Процишен М., Електронна комерція з точки зору телекомунікаційного права.....	131
Рєпіна Є., Устименко О., Правовий статус криптовалюти у світі.....	135
Текєджанова К., Проблеми правового регулювання криптовалют в Україні.....	138
Маньгора В., Правове регулювання електронних господарських договорів	140
Високос В., Комп'ютерна програма як об'єкт інтелектуальної власності	143
Кривобок І., Досвід США щодо правової охорони дизайну одягу як результату інтелектуальної діяльності.....	146
Шарудило Д., Правовий статус суб'єктів авторського права на твори архітектури	151
Третьякова П., Ознаки театральної постановки як об'єкта авторського права.....	156

**ТЕЗИ ВИСТУПІВ СТУДЕНТІВ НТУУ «КПІ ім. ІГОРЯ
СІКОРСЬКОГО» НА ДРУГОМУ УКРАЇНСЬКОМУ
МОЛОДІЖНОМУ ФОРУМІ З УПРАВЛІННЯ ІНТЕРНЕТОМ**

Сазонова К.,	
Соціальні мережі: кіберзалежність чи комунікація майбутнього?....	159
Мнишенко М.,	
Права людини та розширення ролі інтернету, як засобу маніпуляції суспільством	163
Єрмак Я.,	
Доступ до інтернету в селах, селищах, смт	164
Климчук М.,	
Шахрайство в глобальній мережі Інтернет	166
Фарадж Д.,	
Негативний вплив інтернету на підростаюче покоління	168
Натяжний Я.,	
Штучний інтелект: проблеми регулювання	170
Олексенко М.,	
Кібербезпека в країнах Європейського Союзу	173
Крюкова Є.,	
Електромобіль та інформаційна безпека	176

ІНТЕРНЕТ РЕЧЕЙ І ПРАВО: ПОГЛЯД У МАЙБУТНЄ

Історія цивілізації знає декілька технологічних (промислових) революцій, які за різною класифікацією мають різну назву. Але всі вони мають одну загальну рису: технологічні революції - це відгук на концептуальний соціальний запит. Одним з фундаментальних результатів 4-ї технологічної революції є процес широкого застосування Інтернету речей (Internet of things, IoT).

На який же соціальний запит IoT є відповіддю? Процес застосування технологій IoT, що динамічно набирає силу у багатьох країнах, – це відповідь на стрімке погіршення на планеті стану справ з ресурсами чистого повітря, вуглеводів, корисних копалин, лісів, чистої прісної води; родючих земель тощо. Спостерігається нарощування проблем у перенасичених мегаполісах, перевантаженість інфраструктурних об'єктів, загрожуюче зростання кількості автомобілів тощо. Відбувається глобальне потепління, багато країн потерпають від глобальної нестачі продовольства. Тому експерти доходять до висновку, що людство, яке постійно прораховувалось при прийнятті рішень, майже стоїть на порозі глобальної катастрофи тому, що вже вичерпало всі можливі ліміти на свої помилки.

Чому саме сьогодні ми маємо такий результат? Базовою причиною, є те, що останні 1,5-2 століття процес прийняття рішень характеризується наступним: необхідністю враховувати великі обсяги інформації (даних) про навколишнє середовище, про велику кількість суб'єктів та об'єктів, які є дотичними до процесів відносно яких приймається рішення, яке ж до того здебільше потрібно приймати в режимі максимально наближеному режиму реального часу. В наслідок певних фізіологічних та когнітивних обмежень людина на в змозі в таких умовах приймати обґрунтовані рішення, які б були хоча б раціональними, не кажучи вже про їх оптимальність.

Технології IoT дозволяють забезпечити умови щодо прийняття та виконання рішень приймаються в режимі реального часу на основі збору і обробки величезної кількості даних, ідентифікації всіх об'єктів та суб'єктів, що беруть участь в процесах відносно яких приймається рішення, та застосування спеціальних математичних алгоритмів, зокрема, алгоритмів штучного інтелекту.

Будемо застосовувати наступне визначення: Інтернет речей – це сукупність взаємодіючих технічних систем і комплексів, що складаються з

мікропроцесорів, сенсорів, пристроїв, систем передачі даних, локальних і / або розподілених обчислювальних ресурсів і програмних засобів, зокрема, програм штучного інтелекту, призначених для реалізації суспільних відносин, в тому числі, пов'язаних з наданням послуг і проведенням робіт при безпосередній участі або без участі суб'єктів (юридичних або фізичних осіб) на основі використання великих даних і мережі Інтернет [1].

В світі багато країн прийняли на найвищому рівні національні стратегії або концепції щодо розвитку та впровадженню технологій IoT. Оскільки штучний інтелект (ШІ) вважається базовою умовою застосування технологій IoT, тому протягом останніх 1,5 – 2 років біля 20 держав світу мають затверджені національні стратегії розвитку штучного інтелекту. Майже 10 з цих держав в якості мети стратегій визначили наступне: стати державою № 1 у світі у розвитку штучного інтелекту [2]. Це свідчить про те, що розвитку ШІ відводиться надзвичайно важлива роль у майбутньому людської цивілізації.

В той же час, можемо констатувати, що існують певні бар'єри та ризики на шляху розвитку технологій Інтернету речей. До основних системних бар'єрів слід віднести наступне: відсутність державної стратегії та лідерів змін, недостатнє розуміння цінностей IP політичним істеблішментом країни, керівниками галузей та бізнес-структур. Крім того, існує ще певна низка бар'єрів та ризиків: політичні, техніко-технологічні, правового регулювання, освітянські та мотиваційні, фінансово-економічні, правового регулювання, безпекові, конфіденційності, сумісності, стандартизації. Кожен з перелічених видів бар'єрів потребує ретельного дослідження для формування програми заходів щодо їх подолання.

Наприклад, щодо техніко-технологічного бар'єру, то пояснення його наявності наступне. Один із базових технологічних принципів – це те, що будь-які технології, що забезпечать надання послуги або виконання роботи комфортніше, дешевше, швидше, якісніше, безпечніше мають бути імплементовані до IoT. Саме це стає причиною фундаментальної техніко-технологічної відмінності, яка полягає в тому, що архітектура комплексів та систем IoT є транскордонна, багатовимірна, складна, багатозв'язна, багатофункціональна, яка адаптивно змінюється та самостійно перелаштовується.

В частині безпекових проблем слід звернути увагу на основний принцип функціонування технологій IP – це забезпечення надійності, стійкості і якості здійснення тієї чи іншої людської діяльності. А це означає визначенні та забезпечення інфраструктурної безпеки (надійність, стійкість, резервування тощо), технологічної та кібернетичної безпеки. Особливість інфраструктури систем та комплексів IoT обумовлює наявність проблеми забезпечення

безперервної та багаторівневої безпеки, інтеграції і взаємодії систем безпеки. Все потребує створення та функціонування спеціального менеджменту безпеки.

В сфері законодавства один з основних принципів – правове регулювання має сприяти розвитку та застосуванню технологій IoT в інтересах людей. Але дослідження проблем правового регулювання потребує знання соціальної моделі суспільства, моделі яка в необхідному обсязі описує мету, зміст та особливості реалізації певних груп суспільних відносин. Саме з визначенням соціальної моделі суспільства виникає проблема, яка має незвичайний характер.

Україна, як і всі держави світу, перебуває на порозі кардинального технологічного стрибка (наступні 30-50 р.), який відбудеться завдяки застосуванню досягнень у сфері технологій Інтернету речей, штучного інтелекту, нано- і біо- технологій, генетики, робототехніки тощо. Особливість сучасного технологічного стрибка в тому, що він може призвести до стрімкого формування і розвитку нових за змістом і формою суспільних відносин у різних сферах життєдіяльності людини, суспільства, держави. Тобто сьогодні ми не можемо з певним рівнем впевненості уявити яке ж суспільство, які ж суспільні відносини будуть через 30-50 років.

Крім того, потрібно зауважити наступне. Протягом наступних десяти років у всіх сферах суспільної активності відбудуться безпрецедентні технологічні зміни, лева частка з яких буде обов'язково базуватись на використанні інформаційно-комп'ютерних технологіях (ІКТ). Тобто використання ІКТ буде умовою реалізації всіх суспільних відносин. Таким чином, правове забезпечення всіх правовідносин буде обов'язково включати норми інформаційного права.

Традиційно система права (правових норм) здебільше формувалась після вивчення усталеної практики здійснення суспільних відносин, тобто після їх ретроспективного аналізу, виявлення закономірностей їх реалізації та подальшої фіксації за допомогою законодавства. При цьому терміни формування законодавства змінювались: до кінця XIX сторіччя – це сотні років, іноді десятки років; XX сторіччя – це десятки років, іноді декілька років; XXI сторіччя – це декілька років и менше.

Для XXI століття в умовах технологічного стрибка умови формування досить кардинально змінюються. Виникає нагальна потреба у визначенні правового регулювання нових видів суспільних відносин, які або тільки почали з'являтися, або будуть з'являтися в майбутньому. Бажано запобігти ситуації правової сінгулярності, тобто коли внаслідок трансформації суспільства з'являться нові за змістом і формою суспільні відносини, але для

яких ще не буде сформовано законодавство. З огляду на масштабність та на високу динаміку появи нових суспільних відносин, існують великі ризики виникнення правового, а, значить, і суспільного хаосу, що має потенційну небезпеку для всього людства.

Таким чином, доходимо до висновку про те, що настав час змінювати парадигму: переходити від ретроспективного методу до прогностичного методу формування системи права. Це означає, що за результатами міждисциплінарних досліджень має бути побудована прогностична модель суспільства (суспільних відносин) майбутнього. А вже на базі такої прогностичної моделі суспільства мають будуватись прогностичні правові моделі регулювання: адміністративних, цивільних, інформаційних відносин тощо; встановлення юридичної відповідальності; телекомунікацій та використання спектра; забезпечення конкуренції; використання штучного інтелекту та роботів; застосування технологій блокчейну та криптовалют використання смарт контрактів; захисту інтелектуальної власності; захисту приватності; забезпечення безпеки і конфіденційності тощо.

При цьому потрібно враховувати концептуальну правову проблему майбутнього. Традиційна правова доктрина стверджує, що правові норми регулюють суспільні відносини між людьми. Але на сучасному етапі правова наука не готова надати відповідь про те, яким чином будуть регулюватись суспільні відносини, що пов'язані з роботами із штучним інтелектом. Те, що проблема визначення правового регулювання суспільних відносин в умовах використання ШІ не є надуманою або фантастичною, свідчать надзвичайно активні дії багатьох держав щодо створення національних стратегій, концепцій та програм розвитку ШІ, а також надзвичайно великі бюджети транснаціональних корпорацій для науково-дослідних робіт з розвитку ШІ.

Шість національних стратегій (Китай, Південна Корея, Японія, США, Велика Британія, Євросоюз) мають окремі розділи щодо вирішення правових проблем, пов'язаних з розвитком та застосуванням систем з ШІ. Так в Резолюції Європейського Парламенту поставлено завдання Єврокомісії щодо необхідності проведення оцінки впливу на майбутнє цивільне законодавство створення в довгостроковій перспективі особливого юридичного статусу для роботів, наприклад, для найскладніших автономних роботів (роботів з ШІ) [3]. Але, те, що майже 3 роки тому вважалось далекою перспективою, сьогодні вже може бути оцінено середньостроковою перспективою.

Запропонуємо наступну гіпотезу: якщо когнітивні функції (КФ) робота з ШІ є еквівалентними КФ фізичної особи, то робот з ШІ може бути визнано правовим еквівалентом фізичної особи [4]. В такому випадку: **штучний інтелект** – це певна сукупність методів, способів, технологій і засобів, в тому

числі, апаратних, та комп'ютерних програм, які реалізують одну, кілька або всі когнітивні функції (КФ), які є еквівалентними когнітивним функціям людини.

З метою пошуку можливостей застосувати при визначенні правового регулювання суспільних відносин, пов'язаних із ШІ, всіх напрацювань та здобутки традиційних правових систем світу пропонуємо вдосконалені редакції таких категорій права як:

юридична догма – це будь-який елемент системи права або окремі її положення, що приймаються за істину без доказів, дослідного обґрунтування і практичної перевірки, а лише на основі включення їх в правові доктрини або законодавство;

юридична фікція – це юридична догма, яка дозволяє давати правову характеристику суб'єктам, об'єктам та/або змісту правовідносин на засадах правової аналогії (правової еквівалентності) з іншими змістовно не пов'язаними елементами системи права, та яка використовується суворо в рамках вичерпно визначених правових умов та обмежень її застосування.

Використовуючи надані дефініції категорій сформулюємо відповідні категорії в інтересах цивільного права [5]:

юридична догма: Система Інтернету речей із штучним інтелектом, яка самостійно виконує частину функцій людини в процесі надання послуг або проведення робіт, є суб'єктом права.

юридична фікція – Система Інтернету речей із штучним інтелектом як суб'єкт права, може розглядатися в якості представника в розумінні ст. 237 ЦКУ, який зобов'язаний або має право вчиняти правочини від імені її власника (розпорядника), якого вона (система) представляє.

Визнання обґрунтованості справедливості запропонованої гіпотези дозволить вирішити правові проблеми, пов'язані з роботами із ШІ в рамках традиційної системи права, з використанням всього багатовікового досвіду її функціонування, шляхом формування теоретико-методологічних основ та розроблення практичних рекомендацій зі створення відповідної системи правового забезпечення.

Таким чином, можна в цілому визначити майбутні напрями наукових досліджень:

1. Визначення теоретико-методологічних основ та практичних рекомендацій щодо засад правового регулювання суспільних відносин в умовах «взаємодії»:

- людина – робот, робот – робот - за ініціативою людини;
- робот – людина, робот – робот - за ініціативою роботу.

2. Вдосконалення всієї системи правового регулювання в умовах прийняття рішень (проявів «волевиявлення») роботами із штучним інтелектом.

3. Проведення теоретико-методологічних досліджень щодо визначення прогностичних (майбутніх) правових моделей при реалізації суспільних відносин в умовах застосування ІР із ШІ у цивільному, інформаційному (комп'ютерні технології, телекомунікації, використання радіочастотного ресурсу тощо), морському, авіаційному, медичному, кримінальному, адміністративному, сімейному праві тощо.

4. Проведення теоретико-методологічних досліджень щодо визначення прогностичних (майбутніх) правових моделей при реалізації суспільних відносин в умовах застосування технологій ІР із ШІ у промисловості, сільському господарстві, банківській сфері, енергетиці, медицині, освіті, державному управлінні, ретейлі, збройних силах тощо.

5. Проведення правових досліджень з метою забезпечення в умовах застосування технологій ІР із ШІ: лібералізації та конкуренції на певних ринках; захисту прав споживачів; визначення відповідальності; безпеки, зокрема кібербезпеки; захисту приватності (захисту персональних даних); захисту інтелектуальної власності та авторського права тощо.

Список використаних джерел:

1. Баранов О.А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія/ О.А. Баранов; НДІП НАПрН України – К.: Видавничий дім «АртЕк». – 2018. – 344 с.

2. Баранов О. А. Правові аспекти національних стратегій розвитку штучного інтелекту. Юридична Україна. – 2019. - № 7. – С. 21-38.

3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics - Strasbourg European Parliament 16 February 2017 <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect>

4. Баранов О.А. Інтернет речей (ІоТ): робот с штучним інтелектом як суб'єкт правовідносин. Юридична Україна. – 2018. – № 5-6. – С. 75–95.

5. Баранов О.А. Інтернет речей (ІоТ): регулювання надання послуг роботами зі штучним інтелектом / О.А Баранов // Інформація і право. – 2018. – № 4. – С. 46-70.

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

МАЙБУТНЄ ОСВІТИ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНТЕРНЕТУ РЕЧЕЙ

Нещодавно в Україні друком вийшла праця професора Массачусетського технологічного інституту Макса Тегмарка «Життя 3.0. Доба штучного інтелекту» (в США видання побачило світ у 2017 році), який доволі ґрунтовно і в цікавій формі рефлексує щодо перспектив розвитку штучного інтелекту, загроз його поширення в режимі всезагальності тощо. Автор вказує, що «ніхто достеменно не знає, яким буде суперуспішний субстрат для обчислювальних технологій. Але ми точно знаємо, що ще близько не підійшли до меж, накладених законами фізики» [1, С. 88]. Тобто, можемо зробити висновок, що штучний інтелект, а відтак і феномен Інтернету речей, насправді знаходяться ще відносно на початковій стадії свого розвитку і розкриття всіх можливостей і меж застосування людству ще належить дізнатися. Останнім часом, починають з'являтися публікації про «зрощення» штучного інтелекту та Інтернету речей. Так, Бенджамін Джокела (Benjamin Jokela) вважає цілком логічною появу гібрида «Інтернету речей» і штучного інтелекту, який отримав назву AIoT (AI + IoT). Він зазначає, що «штучний інтелект вже став нормою в нашому світі, і, оскільки його роль в «Інтернеті речей» стає більш важливішою, нам потрібно шукати «розумні» рішення, які полегшать їх злиття. Крім того, штучний інтелект скоро буде готовий витіснити людину-оператора з багатьох сфер діяльності, що ще сильніше підкреслює необхідність в надійних системах, здатних впоратися з будь-якою відповідною цій екосистемі проблемою» [2, с. 72]

З огляду на це, постає правомірне питання щодо перспектив правового регулювання суспільних відносин, які будуть опосередковані цілою системою технологічних, інформаційно-комунікаційних артефактів. Більше того, одним з ключових питань є питання щодо зміни характеру діяльності самої людини, а також умов її трудової діяльності. Адже, не секрет, що повсюдне розповсюдження технологій штучного інтелекту може призвести до суттєвого вивільнення робочих місць, зміною становища людини у виробничому процесі. Сучасна юридична наука, напевно, не готова відповісти яким чином здійснюватиметься захист права на працю, коли об'єктивним фактором стане, переважаюча ефективність виконання трудових завдань системами штучного інтелекту. Чи готовий світ до появи нової хвилі луддитів?... Більше того, згадуваний нами, Макс Тегмарк доволі серйозно розмірковує не тільки над вивільненням працівників-операторів, а й вказує про перспективи участі

штучного інтелекту у судочинстві, обґрунтовуючи це тим, що «робосудді могли б також виключити з процесу людську упередженість, яка радше випадкова, ніж умисна; судді-люди не можуть опанувати всіх фахових знань, необхідних для кожної можливої справи (від заплутаних патентних суперечок до загадкових убивств, які не розкрити без найновітніших досягнень судової експертизи), то робосудді майбутнього можуть мати в принципі безмежну пам'ять і здатність до навчання..» [1]

Щоб уникнути проблем зі зміною стратифікаційної структури у сторону появи більшої кількості безробітних, варто звернути увагу на систему освіти, яка має забезпечувати спромоги людини на універсалізацію своєї діяльності. Звичайно, така система освіти повинна формуватися в режимі всезгальності, що в межах сучасної суспільно-історичної ситуації, практично неможливо, а відтак – залишаються перспективи поглиблення нерівностей у різних їх формах.

Вже сьогодні стає зрозумілим, що значна кількість сучасних закладів вищої освіти готує «непотрібних» в майбутньому фахівців, тобто тих, чийі знання і вміння будуть доволі успішно замінені системами, пов'язаними зі штучним інтелектом. Саме тому модернізація системи освіти повинна здійснюватися не з огляду на формування нових вузьких компетентностей, а на те, щоб за словами Е.В. Ільєнкова змогти створити можливості «людині повернути втрачену їм владу над світом машин, щоб перетворити людину в розумного і сильного володаря, і господаря всього створеного нею грандіозного, хитромудрого і могутнього механізму сучасного машинного виробництва, щоб людину зробити розумнішою і сильнішою, ніж машина» [3].

Список використаних джерел:

1. Тегмарк М. Життя 3.0. Доба штучного інтелекту / пер. з англ. Зорина Корабліна. К.: Наш формат. 2019. 432 с.
2. Джокела Б. Слияние искусственного интеллекта и «Интернета вещей». Control engineering Россия. 2019. №2 (80). – С.70-72.
3. Ильенков Э. Об идолах и идеалах. 2-е изд. К.: «Час-Крок», 2006. - с. 312.

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

*Ткачук Т., д.ю.н., доцент, заступник зав.
кафедри організації захисту інформації з
обмеженим доступом Навчально-
наукового інституту інформаційної
безпеки Національної академії СБУ*

ІНТРЕНЕТ-РЕЧІ: ВІД ФАНТАСТИКИ МИНУЛОГО ДО РЕАЛІЙ СЬОГОДЕННЯ

Переваги використання технологій штучного інтелекту очевидні, тому не дивно, що IoT з кожним роком набирає обертів і буде мати позитивну тенденцію. Пристрої, гаджети і розумні системи при цьому покликані не замінити спеціалістів, а полегшити і оптимізувати їх роботу. Так, спеціалісти Tractica прогнозують, що поставки клінічних і неклінічних підключених натільних датчиків досягнуть 92,1 млн одиниць в 2022 році (для порівняння: 2,4 млн одиниць було в 2016 році) [1].

Термін IoT (анг. «Internet of Things», скор. – IoT) вперше було сформульовано у 1999 році засновником дослідницького центру Auto-ID Center в Массачусетському технологічному інституті Кевіном Ештоном [2].

Проте, історія IoT має свій футурологічний аспект, зокрема у творах письменників фантастів. Так, у 1950-ті роки Рей Бредбері створив кілька творів, в яких напрочуд точно передбачив технології та тренди, що з'явилися в майбутньому. З кожним роком все більше винаходів, описаних в його книгах, втілюються в життя. Ось кілька з них.

1. Віртуальна реальність. В оповіданні «Вельд» Р. Бредбері описує кімнату з ефектом присутності. Вона може створювати зображення, звуки і запахи, а також, судячи з подій сюжету, ще й впливати на матеріальні об'єкти.

2. Безпілотні автомобілі. В оповіданні «Пішохід» фігурують автомобілі, які їздять самі по собі, а також вміють вести з людьми діалог.

3. Bluetooth-навушники. У романі «451 градус за Фаренгейтом» описані радіопередатчіки-«черепашки», які щільно прилягають до вух і відтворюють звук без проводів. Понад 50 років пішло в людства, аби втілити передбачення Бредбері в життя — у 2016 році Apple представила AirPods.

4. Розумний годинник і стільниковий зв'язок. В оповіданні «Вбивця» 1953 року фантаст передбачив появу пристроїв, які дозволять розмовляти один з одним на відстані без проводів. В його уяві це були радіобраслети – невеликі девайси у вигляді годинника з вбудованим мікрофоном і динаміком. Виходить, Бредбері передбачав відразу дві технології: мобільний зв'язок і розумні годинник. Наприклад, дзвінки можна здійснювати з AppleWatch – точно так, як описано в книзі.

5. *Розумний будинок*. У кількох оповіданнях Р. Бредбері зустрічаються розумні будинки. Вони вміють розуміти голосові команди, готувати їжу, прибирати, прати, навіть мити і одягати власників. У 1999-му році Disney випустила фільм, в якому сім'я заїжджає в «будинок майбутнього», яким керував віртуальний асистент Пет.

Рей Бредбері зміг передбачити багато винаходів і тренди майбутнього. Але головний посыл практично всіх його творів – що розвиток технологій перетворить людей у бездушні біомашини – поки, на щастя, не був втілений в життя. Хай-тек, скоріше, допомагає вирішувати проблеми людства, ніж створює їх.

Серед інших письменників, які змогли досить точно зазирнути у майбутнє поправу одна вважає Жюль Верна, який у 1865 році написав книгу «Із Землі на Місяць», в якій йшла розповідь про першу подорож людей на Місяць. Письменник не лише передбачив сам факт польоту людини на Місяць, у його книзі безліч інших точних передбачень. Цікаво те, що між книгою Жуля Верна та польотом людини на Місяць пройшло 104 роки!

Попри очевидні переваги практичного застосування IoT на сучасному етапі суспільного розвитку, актуалізується і зворотна сторона даних процесів – кібербезпека. За оцінкою компанії Hewlett-Packard (2015 рік), більше 70% пристроїв, що входять в IoT, мають уразливості, у 60% з них - небезпечний web-інтерфейс. При цьому більшість з них мають у своєму розпорядженні доступом до таких даних своїх власників, як адреса, e-mail і навіть банківський рахунок [3].

Часто це пов'язано з тим, що виробники, прагнучи знизити свої витрати, радикально економлять на забезпеченні безпеки. У свою чергу, фірми-постачальники дешевих відеокамер практично ігнорують включення в свої продукти засобів захисту, оскільки, за їхніми оцінками, для більшості користувачів камер низька вартість набагато важливіше. 9 січня 2017 року Федеральна торгова комісія США навіть подала позов проти D-Link через неякісний захист веб-камер і роутерів [4].

У 2016 році значного розголосу набула інформація про успішний злом інсулінової помпи, який здійснив на прикладі власного пристрою хакер, який страждає діабетом. Він отримав доступ через незахищений Wi-Fi канал [5].

У своїй новій книзі під назвою «ClickHeretoKillEverybody» («Натисніть сюди, щоб убити всіх»), співробітник центру BerkmanKleinCenterfor Internet andSociety в Гарварді, член ради Фонду ElectronicFrontierFoundation, головний фахівець з технологій у компанії IBM Resilient, яка допомагає іншим кампаніям підготуватися до потенційних кіберзагроз Брюс Шнайер стверджує,

що уряди повинні змусити компанії, що займаються розробкою гаджетів, які виходять в Інтернет, поставити безпеку на перше, а не на останнє місце [6].

Ці та ряд інших важливих проблем кібербезпеки IoT слугували підставою випуску Технічним комітетом Європейського інституту телекомунікаційних стандартів (ETSI) з кібербезпеки стандарту кібербезпеки в Інтернет речей TS 103 645 [7]. Документ встановлює базовий рівень безпеки для споживчих товарів, підключених до Інтернету, і закладає основу для майбутніх схем сертифікації IoT.

TS 103 645 вимагає від розробників відмовитися від використання універсальних паролів за замовчуванням, які стали джерелом багатьох проблем безпеки. Він також передбачає дотримання політики розкриття вразливостей, щоб дозволити дослідникам безпеки і іншим особам повідомляти про проблеми. Крім того, стандарт дозволить забезпечити дотримання норм Загального регламенту щодо захисту даних (GeneralDataProtectionRegulation, GDPR) IoT-пристроями і сервісами, що зберігають і обробляють персональні дані користувачів.

Крім того, на основі TS 103 645 розробники планують впровадити схеми сертифікації, які допоможуть захистити особисті дані користувачів.

Одна з важливих функцій стандарту - скоротити кількість паролів, які використовуються за замовчуванням. Саме стандартні паролі є однією з головних причин загроз кібербезпеки IoT-сфери. TS 103 645 також передбачає політику розкриття вразливостей: це простимулює користувачів повідомляти про проблеми з функціонуванням пристроїв.

Застосування цього стандарту дозволить також повноцінно дотримуватися норм Загального регламенту щодо захисту даних (GDPR) - спеціальної постанови ЄС, спрямованого на захист і уніфікацію персональних даних всіх громадян Європейського союзу. У свою чергу використання GDPR допоможе захистити персональну інформацію користувачів та підвести єдину нормативну базу під весь сектор IoT і IT-технологій.

Відповідний суб'єкт, такий, як постачальник послуг або виробник пристрою, зобов'язаний забезпечити обробку персональних даних відповідно до чинного законодавства про захист персональних даних (таким, наприклад, як європейський GDPR), а також відповідно до чинного законодавства і нормативних вимог до питань безпеки.

Так, згаданий стандарт, у частині захисту персональних даних, крім іншого, передбачає:

Положення 4.8-1. Виробники пристроїв і постачальники послуг зобов'язані надавати споживачам чітку і прозору інформацію про те, як, ким і

з якою метою використовуються їхні персональні дані. Це також відноситься до третіх сторін, які можуть бути залучені, включаючи рекламодавців.

Положення 4.8-2. Якщо особисті дані обробляються на основі згоди споживачів, ця згода має бути отримана належним чином.

Положення 4.8-3. Споживачам, які дали згоду на обробку своїх персональних даних, повинна бути надана можливість відкликати згоду в будь-який час.

Отримання згоди «належним чином» (in a valid way) як правило передбачає надання споживачам, у цьому випадку – пацієнтам, вільного, очевидного і явного вибору (*причому за замовчуванням вважається, що такої згоди немає – варіант opt-in*) щодо використання їх персональних даних для певної мети третіми особами.

Пацієнти очікують, що їм будуть надані засоби для захисту недоторканності їх приватного життя, за допомогою належного налаштування функціональних можливостей пристроїв і послуг IoT, які використовуються у процесі надання їм медичних послуг.

Розробка стандарту кібербезпеки є важливим кроком для правової нормалізації всієї сфери IoT, у тому числі й у сфері медицини. На сьогоднішній день персональні дані користувачів IoT-пристроїв залишаються незахищеними, тоді як сама сфера застосування подібних пристроїв зростає.

Список використаних джерел :

1. How IoT enhances medicine. M-Health Conference Tallinn. URL: <https://tallinn.mhealth.events/article/iot-v-meditsine-kak-internet-veshchey-sovershenstvuet-sferu-zdravoohraneniya-97414>
2. Kevin Ashton That 'Internet of Things' Thing. RFID Journal. URL: <https://www.rfidjournal.com/articles/view?4986>
3. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. News Advisory. URL: <https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676>
4. Federal trade commission d-link corporation and D-link systems, INC. Case 3:17-cv-00039 URL: https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf
5. Johnson&Johnson says insulin pump 'could be hacked' BBC NEWS. 4 October 2016. URL: <https://www.bbc.com/news/business-37551633>
6. Bruce Schneier Click Here to Kill Everybody Security and Survival in a Hyper-connected World. September 2018 W. W. Norton & Company. 288 Pages URL: https://www.schneier.com/books/click_here/
7. CYBER; Cyber Security for Consumer Internet of Things. ETSI TS 103 645 V1.1.1 (2019-02) URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

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

ДЕЯКІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ НАУКОВЦІВ НА РИНКУ НОВІТНІХ ТЕХНОЛОГІЙ

На засіданні Комітету ВРУ з питань науки, освіти та інновацій 6 листопада 2019 р. при розгляді стану реалізації Закону України «Про наукову і науково-технічну діяльність» однією з проблем, які перешкоджають сучасному розвитку науки, діяльності наукових установ та вчених було визначено загрозливу ситуацію, що склалася із набуттям 20.07.2019 р. чинності змін до постанов КМУ: від 27.12.2001 р. № 1756 “Про державну реєстрацію авторського права і договорів, які стосуються права автора на твір” та від 23.12.2004 р. № 1716 “Про затвердження Порядку сплати зборів за дії, пов’язані з охороною прав на об’єкти інтелектуальної власності”. Затверджено нові розміри обов’язкових зборів за дії, пов’язані із державною реєстрацією об’єктів авторського права (АП) та об’єктів інтелектуальної власності (ІВ), а також із реєстрацію дій щодо зміни прав на зазначені об’єкти (продаж¹). Таким чином, суттєво збільшуються витрати науковців та наукових закладів як на реєстрацію, так й на продаж (передачу прав власності) зазначених об’єктів. Особливе занепокоєння висловлювалось щодо нового фінансового навантаження на науковців, які мають сплачувати ці витрати із своїх власних доходів.

Так, новий розмір збору державної реєстрації авторського права і договорів, які стосуються права автора на твір (в неоподатковуваних мінімумах доходів громадян, НМДГ)², для заявника – фізичної особи становив: державна реєстрація об’єктів АП – 15 (ставка збору з 27.12.2001 по 20.07.2019 дорівнювала 3,25 НМДГ), тобто збільшено більш ніж в 4,6 рази); державна реєстрація договорів, що засвідчує передачу (відчуження) майнового права або передачу права на використання твору (права на твір)³ – 30 (відповідно = 4,25

¹ Продаж результатів робіт (послуг) включає, зокрема, надання права на користування товарами за договорами оперативного лізингу (оренди), продажу, передачі права відповідно до авторських або ліцензійних договорів, а також інші способи передачі об’єктів авторського права, патентів, знаків для товарів і послуг, інших об’єктів права інтелектуальної, у тому числі промислової власності [4].

² Неоподатковуваний мінімум доходів громадян в 2019 р. дорівнював 960,5 грн. (складає 1/2 прожиткового мінімуму для працездатних осіб).

³ Зокрема таких об’єктів АП, як монографії, підручники та комп’ютерні програми – але сьогодні комп’ютерні програми в Україні реєструються не часто.

НМДГ та 7 разів); зміна до Держреєстру свідоцтв реєстрації АП – 3 (0,5 та 6 разів); Зміна до Держреєстру договорів права на твір – 3 (0,25 та 12 разів). [1].

Нові розміри зборів за права на об'єкти ІВ: винаходи (В) та корисні моделі (КМ) для заявника – фізичної особи збільшились за 9 років (з 21.09.2011 по 20.07.2019) у 2 рази (за деякими діями у 3-4 рази): 1) за подання заявки⁴ з 800 грн. до: на В = 1600 грн.; КМ = 2400 грн.; 2) за проведення експертизи заявки на В, формула якого має один незалежний пункт до 6000 грн., за кожний додатковий пункт по 6000 грн.; 3) за публікацію про видачу патенту з 200 грн. до: В = 400; КМ= 600; 4) за опублікування відомостей про передачу права власності на винахід (корисну модель) з 600 до 2400 грн.; 4) річний збір⁵ за підтримання чинності патенту на В за кожний рік дії патенту починаючи від дати подання заявки: 1-ий, 2-ий з 300 грн. до 600; 3-ий з 400 до 800; 4-ий з 500 до 1000; ... 25-ий з 3800 до 30400 грн. тощо [2]. Також за видачу патенту на винахід, корисну модель, промисловий зразок для резидентів України справляється державне мито у розмірі одного неоподаткованого мінімуму доходів громадян [3].

Стан ринку⁶ ІВ України. Кількість заявок від національних заявників на об'єкти промислової власності за 9 місяців 2019 року порівняно з відповідним періодом 2015 року змінилась: на винаходи з 1647 до 1749 (106,2%), з них поданими резидентами – фізичними особами з 857 до 750 (87,5%). Кількість зареєстрованих на резидентів – фізичних осіб винаходів, відповідно за ці періоди: з 348 до 325 (93,4%), корисних моделей з 2103 до 1858 (88,3%) [5].

У жовтні 2019 р.: 1) прийнято заявок на винаходи: 281 (88,6% від жовтня 2018), на корисні моделі: 418 (57,3%); 2) прийнято рішень 188 (79%) 783 (101%); 3) зареєстровано 160 (77%) 581 (66,5%).

Україна в патентних рейтингах ВОІС займала достатньо скромне місце: у 2012 р. 23-є місце (за Індонезією, перед Аргентиною) кількість патентів всього

⁴ При поданні в електронному виді діє 20% знижка від ставки збору.

⁵ Річний збір запроваджується з моменту подання заявки. Враховуючи, що середній строк розгляду заявок на винаходи в цілому збільшився з 25,2 місяців у 2015 році до 28,3 місяців у 2019 році, заявники ще на стадії експертизи заявки додатково у середньому сплачуватимуть за новою ставкою майже 1,4 тис. грн. [5]. Іноді експертиза затягується. Так, заявку на патент на винахід № 84387 було подано 09.03.2000, рішення було прийнято 27.10.2008. Експертиза проводилась протягом майже 103 місяців, за час яких заявник мав сплачувати щорічно збір за підтримку дії патенту. Див. ІДС "Відомості про патенти України на винаходи (корисні моделі), які визнані недійсними, та патенти, які втратили чинність". URL:

https://base.uipv.org/searchInvRevoke/search.php?action=setparams&qp=claims_per_page=10;ch_0=on;ch_4=on;qe0=84387;qe4=<>%2024.10.2000;

⁶ Ринок товарів (робіт, послуг) – сфера обігу товарів (робіт, послуг), що визначається виходячи з можливості покупця (продавця) без значних додаткових витрат придбати (реалізувати) товар (роботи, послуги) на найближчій для покупця (продавця) території [4].

- 5253, з них на резидентів – 2649; нерезидентів – 2604; у 2018 – 27-ме (за В'єтнамом, перед Польщею) заявок 4047, з них резидентами – 2283, нерезидентами – 1764.

Варто зазначити, що є значні складнощі із інформацією щодо економічного обороту об'єктів АП та прав ІВ⁷.

Стан справ на українському ринку вимагає проведення термінових та виважених реформ, орієнтованих у першу чергу на стимулювання резидентів – науковців, закладів вищої освіти та наукових установ реєструвати свої права на об'єкти АП та ІВ, активізацію включення зазначених об'єктів в економічну діяльність. Приваблює в цьому сенсі досвід США з інтенсифікації «включення» в ринковий оборот об'єктів ІВ, який розпочато майже 30 років тому, що реалізований в чотирьох взаємопов'язаних змінах: 1) прийняття Закону Бей-Доула (Bayh-Dole Act), який дозволив університетам і іншим дослідницьким центрам займатися комерціалізацією інновацій, створених за рахунок публічних коштів; 2) поступовим розширенням меж патентоспроможності (зокрема, по відношенню до комп'ютерних програм); 3) фінансуванню Патентного відомства США за рахунок зборів з заявників, що активізувало та прискорило патентування (навіть при неочевидності новизни і корисності); 4) прийняттям судами більш жорстких рішень щодо порушників прав ІВ.

Резюме

1. Введення нових (підвищених) державних ставок зборів на об'єкти як АП, так й ІВ та їх “роздрібнення” з уточненою деталізацією оплати за кожен вид дій призводить до суттєвого збільшення вартості легалізації та підтримання (передачі) прав на ці об'єкти.

2. Нормативними актами не встановлено з яких джерел фінансування науковці (фізичні особи) та неприбуткові організації – заклади освіти / наукові установи (юридичні особи) мають сплачувати дії за легалізацію та підтримку (передачу) прав як на об'єкти АП, так й на об'єкти ІВ.

3. Національний ринок об'єктів АП та ІВ розбалансовується. За більш менш стабільним обсягом надходжень стоїть зменшення кількості об'єктів ІВ. Україна в перспективі може мати проблеми із присутністю на глобальному ринку інтелектуальної власності.

4. Стан державної безпеки у сфері ІВ знижується також за рахунок нового правового ризику: можна подавати міжнародну заявку на винаходи відповідно

⁷ Так, в офіційній інформації Укрпатенту щодо надходження від зборів за відповідними кодами на 26.11.2019 дані про надходження грошей від зборів за опублікування відомостей про передачу права власності відсутні. (Див.: URL: <https://ukrpatent.org/uk/payment>).

до Договору про патентну кооперацію (РСТ) без оформлення національної відповідної заявки. (протиріччя із ст. 37 ЗУ «Про охорону прав на винаходи і корисні моделі»).

5. Фактично дії на національному ринку інтелектуальної власності, пов'язані із реєстрацією та продажем комп'ютерних програм⁸, а також реєстрацією продажу (передачі прав власності) об'єктів ІВ недостатньо фіксовані, вони часто відбуваються за механізмами недосконалого тіньового ринку.

6. Органам державної влади задля реалізації завдань соціально-економічного розвитку країни, що мають також реалізовуватися через діяльність з розробки та продажу об'єктів АП та об'єктів ІВ доцільно розглянути правомірність та економічну доцільність збільшення ставок зборів, а також розробити відповідні заходи із стимулювання діяльності науковців та неприбуткових організацій, закладів освіти і наукових установ.

Список використаних джерел:

1. Про державну реєстрацію авторського права і договорів, які стосуються права автора на твір : Постанова Кабінету Міністрів України від 27.12.2001 р. № 1756 (Редакція від 14.11.2019) <https://zakon.rada.gov.ua/laws/show/1756-2001-п> (Дата звернення: 25.11.2019).

2. Порядок сплати зборів за дії, пов'язані з охороною прав на об'єкти інтелектуальної власності : Постанова Кабінету Міністрів України від 23.12.2004 р. № 1716 (Редакція від 14.11.2019) URL: <https://zakon.rada.gov.ua/laws/show/1716-2004-п#n13> (Дата звернення: 25.11.2019).

3. Про державне мито : Декрет Кабінету Міністрів України від 21.01.1993 р. №7-93 (Редакція від 26.09.2019) URL: <https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=7-93&p=1218034688041545> (Дата звернення: 25.11.2019).

4. Податковий кодекс України від 02.12.2010 № 2755-VI (Редакція від 20.10.2019) URL: <https://zakon.rada.gov.ua/laws/show/2755-17> (Дата звернення: 25.11.2019).

5. Промислова власність у цифрах. Показники діяльності у сфері промислової власності за 9 місяців 2019 року. К. ДП «Український інститут інтелектуальної власності». 2019. URL: <https://ukrpatent.org/atachs/promvlasnist-9m-2019.pdf> (Дата звернення: 25.11.2019).

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

⁸ Так, констатувалось, що «за останні 5 років в Україні зареєстровано лише 4,5 тисячі комп'ютерних програм і 235 баз даних, хоча створюється їх на декілька порядків більше». Див.: Рекомендації парламентських слухань на тему: "Створення в Україні сприятливих умов для розвитку індустрії програмного забезпечення" : Постанова Верховної Ради України від 15.03.2012 р. № 4538-VI URL: <https://zakon.rada.gov.ua/laws/show/4538-17> (Дата звернення: 25.11.2019).

Харитонов Є., д.ю.н., професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «Одеська юридична академія»,

Харитонova О., д.ю.н., професор, член-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності та корпоративного права НУ «Одеська юридична академія»

ПРАВОВІДНОСИНИ ТА ШТУЧНИЙ ІНТЕЛЕКТ: «СУБ'ЄКТИВІЗАЦІЯ» ОБ'ЄКТУ

Інтернет речей займає усе більш помітне місце в людському суспільстві, що робить нагальним завдання правового регулювання відносин у відповідній сфері. Актуальність вирішення цих питань останнім часом посилюється зростанням реальності припущення, що роботи можуть бути як об'єктом, так і суб'єктом суспільних відносин взагалі [1]. Так, науковці вже розробили робота, що без попередньої підготовки конструює уявлення про себе самого. Він самостійно вивчає, яку має форму і як може рухатися – як і новонароджена дитина. Ця здатність самопізнання дає змогу машині гнучкіше прилаштовуватися до нових завдань і до пошкоджень. Це може бути першим кроком до справжньої самосвідомості, пишуть учені у журналі «Science Robotics» [2].

Хоча, на нашу думку, таке припущення, поки що більшою мірою пов'язане футурологічними моделям розвитку ІТ, про що йшлося у нашому виступі на торішній конференції, присвяченій Інтернету речей, однак це не означає заперечення доцільності розгляду проблеми правосуб'єктності штучного інтелекту, як такої.

Отже, для початку аргументуємо свою позицію у цьому питанні. Передусім, ми виходимо з того, що при сучасному рівні знань вплив на інформаційне поле з метою його впорядкування реально можливий лише у частині його біологічного (людського) субстрату. І обґрунтованого спростування цієї реальності та доказів зворотного поки що зустрічати не доводилося. Це дає нам підстави для висновку, що Інтернет речей це, усе ж таки, поки що об'єкт, але не суб'єкт правовідносин.

Разом із тим, при сприятливих умовах розвитку людства проблема визнання Штучного інтелекту суб'єктом права вже в недалекому майбутньому може постати на повний зріст. Тому маємо бути готовими до такого перебігу подій, аби не залагоджувати згадану проблему потім похапцем. У кожному разі вже зараз має бути встановлена принципова можливість і методологічне

підґрунтя «суб'єктивізації» Штучного інтелекту, тобто визнання за ним властивостей суб'єкта (квазі-суб'єкта) правовідносин.

Як на нашу думку, така можливість може бути обґрунтована шляхом звернення до доробку правознавців Стародавнього Риму, котрим довелося вирішувати подібну проблему – залучення рабів (які були об'єктами правовідносин) до участі у цивільному обігу в якості його «квазі-суб'єктів».

Вирішувалася зазначена проблема за допомогою різноманітних юридико-технічних прийомів, які дозволяли вирішувати колізії розуміння рабів як об'єктів права з одночасним фактичним визнанням за ними здатності створювати певні права і обов'язки для їхніх хазяїв.

Методологічним підґрунтям вирішення згаданих колізій було природне право. Зокрема, застосовуючи такий підхід, Ульпіан запропонував рішення, що докорінно змінювало межі визначення суб'єктів права: «Раб не може бути з точки зору цивільного права стороною у договірному зобов'язанні, однак у природно-правовому аспекті він може і зобов'язувати, і зобов'язуватись» (Д.44.7.14).

Тут варто згадати, що згідно з положеннями цивільного права раби були позбавлені правоздатності: вони мають статус «знаряддя, що говорить». Раби не можуть мати власність. Не можуть вони також мати сім'ю. Зв'язок раба з рабинєю (*contubernium*), як, між іншим, з будь-якою жінкою, не визнавався шлюбом і не породжував правових наслідків. Діти, народжені рабинєю, не підпадали під батьківську владу. Раб, як річ, міг стати об'єктом будь-якого права (права власності, права застави, особистих сервітутів тощо), предметом будь-якої приватноправової угоди (купівлі-продажу, міни, майнового найму), цивільного спору. Якщо йому завдано каліцтво чи інше ушкодження, з позовом до кривдника міг звернутися не сам раб, а його хазяїн, як власник речі. Коли раба виганяли з дому чи від нього відмовлявся володар, це не означало виникнення у нього свободи: раба, як і будь-яку річ, викинуто на вулицю, міг підібрати будь-хто.

Разом із тим, у добу класичного римського права існує важлива тенденція поступового залучення рабів до участі у цивільному обігу.

По-перше, рабство не розглядається римськими юристами як специфічний римський інститут - і за своєю сутністю, і за правовим режимом. Як зазначає Гай, «влада над рабами - є інститут **juris gentium**, бо взагалі у народів ми можемо помітити, що господарі мають над рабами право життя і смерті і що все, що набувається рабом, набувається хазяїном» (Інституції. I.52).

Ще більш цікавий наступний фрагмент: «але у наш час нікому з підданих римського народу не дозволяється жорстоко поводитись зі своїми

рабами без законної причини. За наказом імператора Антоніна той, хто безпідставно вб'є свого раба, підлягає не меншій відповідальності, ніж той, хто вбив чужого раба. І навіть надмірна суворість господарів обмежується наказом того ж імператора. Бо Антонін...написав: у випадку коли б жорстокість господарів видалася нестерпною, їх треба примушувати продати своїх рабів в інші руки. І те, й інше є справедливим, позаяк ми не повинні зловживати належним нам правом» (Інституції. I.53).

Особливо прикметною у цих фрагментах є перевірка становища рабів нормами природного права та справедливості. Не ідеалізуючи ні римських законодавців, ні юриспруденцію в їх ставленні до рабства, варто усе ж підкреслити послідовність тенденції застосування критеріїв - у даному випадку принципу справедливості при регулюванні різноманітних інститутів, в тому числі і цього.

По-друге, не менш важливий момент, на який варто звернути увагу, це поступова зміна приватноправового становища рабів (без змін у їх публічно-правовому статусі): хоч вони і надалі не вважалися суб'єктами права, але поступово з практичних міркувань були фактично залучені до участі у цивільному обігу як його суб'єкти. Для цього були використані такі засоби як надання рабам пекулію, а також преторські позови за договорами, що вони здійснювали.

Сутність рабського пекулію полягала у наданні господарем рабу майна, яке враховувалось окремо від іншого, що належало цьому хазяїну (Д.15.1.5.4). Рабський пекулій був цікавим і неодноримірним явищем. З одного боку, він був засобом підвищення зацікавленості раба у результатах власної праці - врешті решт на користь його ж хазяїну, котрий кожної митті міг забрати назад своє майно. З іншого боку, пекулій став ефективним засобом залучення рабів до торгового обігу, оскільки наявність у нього відокремленого майна природно підштовхувала до укладення договорів, набуття нового майна тощо. Необхідність створення гарантій для третіх осіб, які вступали в договори з рабами, котрі мали пекулій, призвела до того, що претори почали давати позови до хазяїна, який надав пекулій. Юридична діяльність раба, зумовлена пекулієм, суворо регламентувалася. Звичайно, все набуте рабом при управлінні пекулієм автоматично ставало власністю його хазяїна. Проте і зобов'язання, що впливали з пекулія, також покладалися на хазяїна раба. Відповідальність рабовласника у цих випадках обмежувалась сумою пекулія (Д.15.1.41). Якщо раб укладав договір, що не впливав з пекулія, його хазяїн за таким договором відповідальності не ніс.

Стосовно пекулію допускалося виникнення правовідносин між рабом та його хазяїном. Так, якщо пекулій був торговим майном, то хазяїн з його

вимогами до раба опинявся в «одній команді» зі сторонніми кредиторами. Більш того, раб також мав право на позов проти свого хазяїна, якщо той проводив розрахунки з ним неправильно (Д.15.1.9.6).

Іншим видом юридико-технічних засобів залучення рабів у цивільний обіг, з визнанням за ними цивільної нібито правоздатності, були преторські позови.

Зміст та характер таких позовів зазвичай залежав від роду діяльності раба: 1. Actio institoria претор надавав у тих випадках, коли хазяїн призначав раба керуючим своїм підприємством—торговим або іншим. Оскільки хазяїн доручав рабу вести свої справи, на нього лягала відповідальність за дії раба у повному обсязі (Д.14.3.1); 2. За договорами, укладеними рабом - капітаном судна, надавався позов - actio exercitoria (Д.14.1.1); 3. Actio quodjussu міг бути наданий тоді, коли раб укладав договір на підставі попередньої домовленості свого хазяїна з третьою особою. І в цьому випадку хазяїн відповідав у повному обсязі (Д.15.4.1.1); 4. За actio deinremverso хазяїн відповідав у межах отриманого майна за договорами раба, в наслідок яких це майно перейшло до нього (Д.12.6.13-14); 5. Крім того, хазяїн відповідав за шкоду, заподіяну його рабом іншій особі.

Таким чином, спектр участі рабів у цивільному обігу був достатньо широким, що дозволяє говорити про існування у них деякої реальної, хоч і обмеженої, правосуб'єктності у галузі приватного права.

Думаємо, що з використанням такого алгоритму може відбуватися й поступове залучення штучного інтелекту до участі у цивільному обігу і в інформаційному та пост інформаційному суспільствах.

Список використаних джерел:

1. Баранов О.А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. URL: <http://aphd.ua/publication-249/>

2. Робот усвідомлює себе. Nadja Podbregar. Roboter erkennt sich selbst scinexx, 31.01.2019 Robert Kwiatkowski, HodLipsonTask-agnostic self-modeling machines Science Robotics, vol. 4, Issue 26, eaau9354, 30.01.2019. Зреферувала С. К. 02.02.2019. <https://zbruc.eu/node/86643>

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

*Коломієць Т. В., студентка ФСП КІП
ім. Ігоря Сікорського
Науковий керівник: Фурашев В. М.,
доцент кафедри ІППІВ, к.т.н., с.н.с.*

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

Починаючи з кінця минулого століття інформаційно-комунікаційні технології все більше інтегруються в соціальне буття всього людства, знаходять своє застосування в усіх сферах суспільного життя. Стрімкий розвиток новітніх технологій поставив перед юристами ХХІ століття багато завдань з правового регулювання суспільних відносин, що виникають та відбуваються з використанням великих обсягів даних (англ. big data), машинного навчання (англ. machine learning), інструментів віртуальної та доповненої реальності (англ. VR/AR), інтернету речей (англ. IoT), робототехніки (англ. robotics) та зі створенням штучного інтелекту.

Зараз в літературі можна знайти багато різноманітних визначень штучного інтелекту, проте якщо проаналізувати їх, можна прийти до висновку, що під штучним інтелектом розуміється певна сукупність технологій, способів чи засобів, які реалізують когнітивні функції людини.

Якщо розглянути поняття штучного інтелекту детальніше, можна зрозуміти, що цей термін використовують відразу в декількох розуміннях: слабкий штучний інтелект, сильний штучний інтелект і штучний суперінтелект:

- «слабкий штучний інтелект» (англ. Weak Artificial Intelligence, WAI), «вузький штучний інтелект» або «обмежений штучний інтелект» (англ. Artificial Narrow Intelligence, NAI) [1, 4, 6] - це штучний інтелект, орієнтований на вирішення одного чи декількох завдань, які виконує або може виконувати людина. Останнім часом слабкий штучний інтелект все частіше називають прикладним штучний інтелект (англ. Applied Artificial Intelligence, AAI);
- «сильний штучний інтелект» (англ. Strong artificial intelligence, ASI, термін запропонував філософ Джон Сирл (John Searle), Каліфорнійський університет, Берклі, 1980 р. [2]), загальний штучний інтелект (англ. Artificial General Intelligence, AGI) - це штучний інтелект, орієнтований на вирішення всіх завдань, які виконує або може виконувати людина;
- «штучний суперінтелект» (англ. Artificial Superintelligence, ASI, термін запропонував філософ Нік Бострем (Nick Bostrom), Оксфордський інститут майбутнього людства, 1998 р.) - це інтелект, який набагато розумніший, ніж

кращий людський інтелект практично в кожній області, включаючи наукову творчість, загальну мудрість і соціальні навички [5].

На даному етапі можна помітити одне з питань правового регулювання розвитку штучного інтелекту, яке може стати проблемою, а саме стурбованість деяких науковців щодо доцільності заборони чи певного обмеження розвитку штучного інтелекту. Деякі вчені наполягають на забороні досліджень штучного інтелекту або на повному контролі за поширенням технології, спираючись на небезпечність некерованого розвитку штучного інтелекту. Проте, в цьому питанні я погоджуюсь з М.В. Карчевським, який зазначає, що заборона досліджень в сфері штучного інтелекту принципово не може стати дієвою. З розвитком інформаційних технологій дана діяльність ставатиме ще доступнішою, а отримані зразки зброї – ще більш небезпечними. В таких умовах законодавча заборона розробки автономної зброї приведе до ситуації, коли органи безпеки та правопорядку будуть оснащені на порядок гірше ніж злочинці, терористичні організації тощо [8]. Адже для нормальної заборони розвитку штучного інтелекту на законодавчому рівні необхідно мати важелі впливу, засоби державного примусу, за допомогою яких можна було б контролювати розвиток штучного інтелекту, що, в сучасних реаліях, є неможливим.

Варто зауважити, що власне штучний інтелект, без виконавчих механізмів, пристроїв, що виконують функції просторового переміщення, різних сенсорів і т.д., не може реалізувати когнітивні функції людини. Саме тому використання штучного інтелекту часто здійснюється в об'єднанні з технічними системами, які оснащені виконавчими пристроями і сенсорами. Таке об'єднання має назву «робот». Термін «робот» також можна розглядати в декількох значеннях. Так, О.А. Баранов запропонував наступні дефініції даного терміну:

- простий робот (simple robot) – інтеграція прикладного ШІ і технічної системи, що дозволяє реалізовувати одну або кілька когнітивних функцій людини в процесі здійснення конкретного виду діяльності, пов'язаної, як правило, з однорідними об'єктами, що мають матеріальний або нематеріальний зміст;
- робот-андроїд (robot android) – інтеграція загального ШІ і технічної системи, що дозволяє реалізовувати безліч когнітивних функцій в процесі здійснення будь-якого виду діяльності без участі людини, пов'язаної з різними об'єктами, що мають матеріальний або нематеріальний зміст;
- андроїд (android) – інтеграція супер ШІ і технічної системи, що дозволяє реалізувати повну множину когнітивних функцій в процесі здійснення будь-якої раніше відомої або невідомої діяльності без участі людини, пов'язаної з

різними відомими або раніше невідомими об'єктами, що мають матеріальний або нематеріальний зміст [7].

Прості роботи вже давно використовуються в сільськогосподарській діяльності під час збирання врожаю, в машинобудуванні та обробці матеріалів та в інших сферах людської діяльності, популярності набирають побутові роботи, які призначені для допомоги людині в повсякденному житті.

Появу андроїдів експерти прогнозують ближче до середини XXI століття, в Парламенті Євросоюзу зазначають, що настання нової епохи в розвитку людства, коли з'являться все більш складні роботи, боти, андроїди та інші прояви штучного інтелекту, стане каталізатором нової індустріальної революції, яка, ймовірно, не залишить жодного прошарку суспільства незацепленим, а отже, для законодавчої влади життєве важливим є вираховування юридичних та етичних наслідків [3].

Основна дискусія в сфері правового регулювання роботів відбувається саме навколо питання про віднесення роботів зі штучним інтелектом до суб'єктів чи до об'єктів правовідносин. Зрозуміло, для того, щоб визнати роботу суб'єктом правовідносин необхідно довести наявність в нього правосуб'єктності, що була б еквівалентна правосуб'єктності фізичної особи. Вирішення цього питання безумовно змінить правові системи світу, проте які саме зміни варто очікувати, на сьогодні можна лише припускати.

Отже, розвиток штучного інтелекту неможливо зупинити, ця технологія постійно розвивається провідними вченими, тому є необхідність правового регулювання суспільних відносин, що здійснюються з використанням штучного інтелекту, необхідно бути готовими до зміни правової системи, появи нових суб'єктів права чи розширення поняття об'єкта права.

Список використаних джерел:

1. Agnese Smith. Artificial intelligence. 2015. URL: <http://nationalmagazine.ca/Articles/Fall-Issue-2015/Artificial-intelligence.aspx>
2. B.J. Copeland. Artificial intelligence (AI). January 12, 2017. URL: <https://www.britannica.com/technology/artificial-intelligence>
3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>
4. Gary Lea. The Struggle To Define What Artificial Intelligence Actually Means. September 3, 2015. URL: <https://www.popsoci.com/why-we-need-legal-definition-artificial-intelligence>
5. Nick Bostrom. How long before superintelligence? Oxford Future of Humanity Institute. University of Oxford. Originally published in Int. Jour. of Future Studies, 1998, vol. 2. URL: <https://nickbostrom.com/superintelligence.html>

6. Tim Urban. The AI Revolution: The Road to Superintelligence. January 22, 2015. URL: <https://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html>

7. Баранов О.А. ІНТЕРНЕТ РЕЧЕЙ І ШТУЧНИЙ ІНТЕЛЕКТ: ВИТОКИ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ [Електронний ресурс] // ІТ ПРАВО: ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ (ДРУГА МІЖНАРОДНА ЩОРІЧНА КОНФЕРЕНЦІЯ). – 2017. – URL: <http://aphd.ua/publication-377/>.

8. Карчевський М. В. Основні проблеми правового регулювання соціалізації штучного інтелекту [Електронний ресурс] / М. В. Карчевський // ІТ ПРАВО: ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ (ДРУГА МІЖНАРОДНА ЩОРІЧНА КОНФЕРЕНЦІЯ). – 2017. – URL: <http://aphd.ua/publication-369/>

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

*Дранник В., викладач кафедри
філософії ФСП КПП ім. Ігоря
Сікорського*

ЗАСТОСУВАННЯ ІНТЕРНЕТУ РЕЧЕЙ У РІЗНИХ СФЕРАХ ЖИТТЄДІЯЛЬНОСТІ ЛЮДСТВА

Сьогодні Інтернет речей займає доволі високі позиції в життєдіяльності людства. Можливо, що в недалекому майбутньому він повністю охопить всі сфери життя людини настільки, що вже буде важко без цього уявити своє існування.

Інтернет речей це найоптимальніша «взаємодія» між людиною та приладами. Він може застосовуватися в різних сферах життєдіяльності людства: в промисловості, в охороні здоров'я, у виробництві, в сільському господарстві, в логістиці, в торгівлі, в машинобудуванні, в енергетиці, а найголовніше, в своєму будинку - система «розумний дім».

Плюси застосування Інтернету речей в тому, що він спрощує життя людей, створює максимальний комфорт і економію всіх ресурсів. Людина отримує більше вільного часу, який вона може приділяти своїм улюбленим справам, хобі, саморозвитку, самовдосконаленню тощо. Також, якщо машину надійно запрограмувати, то вона зробить все оптимально, вірно і раціонально, без помилок, що притаманні людині, адже машина охоплює найменші деталі, які можуть вислизнути від людського погляду.

Але, є й зворотний бік медалі. Навіщо людині витрачати час на саморозвиток і самовдосконалення, якщо вже не буде потреби це десь застосовувати, бо це вже буде прерогатива технології Інтернету речей? Але, немає межі досконалості. Одне впливає з іншого. Людство розвивається і тим самим розробляє нові засоби і сфери прояву Інтернету речей.

Таким чином, треба працювати над новими ідеями щодо використання технологій Інтернету речей, підвищувати рівень обізнаності населення щодо питання його застосування в різних сферах життєдіяльності людства, а також приділяти увагу розробці технологій захисту і безпеки людини в сфері Інтернету речей.

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

*Нашинець-Наумова А., д.ю.н.,
доцент, заступник декана
Київського університету імені
Бориса Грінченка*

ІНТЕРНЕТ РЕЧЕЙ: РЕАЛІЇ СЬОГОДЕННЯ

Інтернет речей – одна з найпопулярніших концепцій в сучасній футурології. Більш того, одна з тих небагатьох, що вже перестають бути концепціями і втілюються в життя. Історично Інтернет речей (The Internet of Things, IoT) розглядається одночасно як технічний і культурний феномен, його історія бере свій початок з 9 жовтня 1832 року, коли видатний російський дипломат і вчений Павло Львович Шилінг продемонстрував у своїй квартирі в будинку на Марсовому полі в Санкт-Петербурзі першу діючу модель електромагнітного телеграфу. З цього моменту почалася передача даних з використанням електричної енергії [1, с. 73].

У 1926 р. Нікола Тесла в інтерв'ю для журналу «Collier's» сказав: «Коли бездротові технології досягнуть справжнього розвитку, вся Земля перетвориться в єдиний величезний мозок, всі речі стануть частиною єдиного цілого і доступ до цього мозку людина буде мати за допомогою приладу, схожого на сучасний телефон, кожен зможе носити його в кишені» [2]. Важко повірити, що ці слова були вимовлені 90 років тому.

У 1990 р. випускник МІТ, один з батьків протоколу TCP / IP, Джон Ромки створив першу в світі інтернет-річ. Він підключив до мережі свій тостер [3]. Інженер зумів, приєднавши кухонного помічника до Всесвітньої павутини, включити і вимкнути його віддалено. Просто так, заради забави, не підозрюючи, що його експеримент стане спусковим механізмом, який викличе «ефект лавини» і почне формувати нову реальність [4]. У наступні роки концепція поступово розвивалася та набувала теоретичну базу і практичний зміст.

У 1999 р. Кевіном Ештоном був запропонований термін «Інтернет речей» (The Internet of Things). В цьому ж році був створений Центр автоматичної ідентифікації (AutoID Center), що займається радіочастотною

ідентифікацією (RFID) і сенсорними технологіями, завдяки якому ця концепція і отримала широке поширення. У 2008-2009 рр. відбувся перехід від «Інтернету людей» до «Інтернету речей», тобто кількість підключених до мережі предметів перевищило кількість людей [3]. В даний час існує можливість ідентифікувати обладнання, предмети побуту та віртуальні об'єкти (наприклад, цифрові фотографії) в такий само спосіб, як і окремих користувачів в Інтернеті. Таким чином, речі можуть бути інтегровані в широкую мережу взаємозв'язків, в якій вони взаємодіють один з одним або з людьми. По суті, речі в світі IoT знаходяться тепер на одному рівні з людьми. У звіті Міжнародного союзу електрозв'язку (МСЕ) за 2015 р. «Вимір інформаційного суспільства» IoT визначається як «глобальна інфраструктура інформаційного общества, лежащая в основе динамично развивающейся сети физических объектов или устройств, имеющих IP-адрес для возможности установления соединения с Интернетом, а также связь, имеющая место между такими объектами и системами, что делает возможным их применение на основе Интернета» [5]. Число об'єктів, які можуть бути частиною IoT, значно перевищує кількість людей. Число підключених до Інтернет пристроїв на початок поточного року становила 8 млрд, тобто 6,58 пристроїв на одну людину з числа інтернет-користувачів. За оцінками різних дослідницьких організацій, до 2021 р. число пристроїв, з'єднаних IoT, складе від 26 до 100 млрд [5]. До таких речей належать, наприклад, пристрої рухомого зв'язку, лічильники на паркувальних місцях, термостати, кардіомонітори, кардіостимулятори тощо.

Найбільш важливими відмінностями Інтернету речей від існуючого Інтернету людей є [6]:

1. акцентування на речах, а не на людині;
2. істотне збільшення числа підключених об'єктів;
3. істотне зменшення розмірів об'єктів та невисокі швидкості передачі даних;
4. акцентування на зчитуванні інформації, а не на комунікаціях;
5. необхідність створення нової інфраструктури і альтернативних стандартів.

Інтернет речей ґрунтується на трьох базових принципах:

1. поширення комунікаційної інфраструктури
2. глобальна ідентифікація кожного об'єкта
3. можливість об'єкта відправляти і отримувати дані за допомогою персональної мережі або Інтернету.

Дану концепцію пов'язують, як правило, з розвитком двох технологій: радіочастотної ідентифікації і бездротових сенсорних мереж. IoT знаходить застосування в будь-якій галузі економіки, в різнопрофільних процесах і повсякденному житті. Його цінність в основному полягає в створенні, обробці

та аналізі нових даних. У всьому світі в результаті роботи мільярдів пристроїв з'являються великі обсяги даних. Частка даних, створених людиною, таких як текстова інформація і дані соціальних медіа, в загальній структурі великих обсягів даних постійно скорочується у зв'язку з тим, що багато пристроїв в сфері IoT генерують в машинні дані, обмінюючись ними з іншими пристроями, і все це відбувається без втручання людини [5].

Передбачається, що в майбутньому «речі» стануть активними учасниками бізнесу, інформаційних і соціальних процесів, де вони зможуть взаємодіяти і спілкуватися між собою, обмінюючись інформацією про навколишнє середовище, реагуючи і впливаючи на процеси, що відбуваються в навколишньому світі, без втручання людини. Іншими словами Інтернет речей можна розглядати як мережу мереж, в якій невеликі менші зв'язані мережі утворюють більші. IoT дозволяє створювати комбінацію з інтелектуальних пристроїв (наприклад, різного роду засоби дистанційного збору даних і роботи), об'єднаних гетерогенними мережами зв'язку і людей-операторів. Спільно вони можуть створювати системи для роботи в середовищах, незручних або недоступних для людини: космос, великі глибини, ядерні установки, трубопроводи тощо. Об'єднання різних речей в поєднанні з творчими можливостями приносить якісно нові результати. Інтернет речей не тільки знаходить застосування в різних галузях економіки, науки, виробництва, різнопрофільних процесах і повсякденному житті, але і надає нові потужні можливості для розвитку глобальної науки і міжнародної кооперації.

Та чи так все райдужно, як виглядає? Швидкими темпами розвиваючи згадані технології, водночас підносимо до нечуваного рівня свою вразливість і відкритість для кібернападів і зламів. Темпи зростання Інтернету речей значно випереджають розвиток галузі кібербезпеки. Розробляючи технології, про безпеку часто думають в останню чергу. І це дійсно так! Для ілюстрації найгірших сценаріїв того, що може статися через хакерські атаки в Інтернеті речей, керівник «Exlab» Саша Майнраз наводить приклад кардіостимуляторів: «Усі говорять про переваги приєднання до хмари. Але водночас передбачається, що хмара цілком захищена... Багато хто говорить про кардіостимулятори, приєднані до хмари. Справді, тут є перевага – якщо щось буде негаразд із вашим серцевим ритмом, ви отримаєте автоматичний сигнал тривоги. Та що як терорист чи й просто дурна дитина задля розваги вирішить дати сигнал тривоги всім кардіостимуляторам в Америці?» [7, с. 20].

Незабаром усі прив'язані до мережі речі, що оточують нас, зможуть бути використанні як платформа для хакерської атаки. Можливо, складно уявити,

що об'єктом нападу може стати ваш телефон або холодильник. Та насправді такі речі вже відбуваються.

Таким чином, зазначимо, що приєднання побутовий речей до інтернету відкриває багато захопливих можливостей, але водночас несе й чималі загрози. Підкреслимо, що істотне здешевлення технічних засобів та швидка їх поширеність дозволить технологіям IoT увійти не тільки в наше повсякденне життя, але і внести істотні зміни в міжнародний простір. Інтернет речей – це новий етап розвитку Інтернету, який значно розширює можливості збору, аналізу і розподілу даних, які людина може перетворити в інформацію і в знання.

Список використаних джерел:

1. Махровский О. Рождение электросвязи в России // Век качества. 2013. № 1. С. 72–76.
2. Черняк Л. Интернет вещей: новые вызовы и новые технологии. 2013. URL: <http://www.osp.ru/os/2013/04/13035551>
3. Пилипенко Н. Интернет вещей – а что это? 2012. URL: <https://geektimes.ru/post/149593>
4. Саруханова О. «Интернет вещей» – это уже не выдумка из научной фантастики // Аргументы и факты в Беларуси. 2016. № 21.
5. Международный союз электросвязи. Измерение информационного общества. Отчет за 2015 год. URL: [https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR 2015-ES-R.pdf](https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR%2015-ES-R.pdf)
6. Интернет вещей и межмашинные коммуникации. Обзор ситуации в мире. 2013. URL: http://www.json.ru/poleznye_materialy/free_market_watches/analytics/internet_vewej_i_mezhmashinnye_kommunikacii_obzor_situacii_v_rossii_i_mire
7. Ткачук Т. Интернет речей та кібербезпека: аналіз можливостей та загроз // Бизнес и безопасность. 2018. №6. С. 17-23.

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

*Антузіньська К., студентка Київського
національного університету імені Тараса
Шевченка*

РЕАЛІЗАЦІЯ МАСОВИХ ТА КРИТИЧНИХ ІОТ-ПРОЕКТІВ (ЕКОСИСТЕМ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ): ПРАВОВОВЕ РЕГУЛЮВАННЯ У ПЕРСПЕКТИВІ

Світ врятує не просто краса, а краса Інтернету речей! Для забезпечення безпечного існування цієї краси необхідно створити якісне правове регулювання.

У широкому застосуванні технологій Інтернету речей (надалі - «IoT», «IP») вбачається величезний потенціал значного підвищення ефективності

практично будь-якого виду людської діяльності. Технології Інтернету речей кардинально змінюють бізнес-ландшафт і стратегії розвитку підприємств, трансформують особисті та соціальні аспекти життя, трансформують цілі галузі та існуючий ІТ-ландшафт. Застосування технологій IoT успішно проявили себе вже у таких галузях, як енергетика, транспорт, охорона здоров'я, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, промисловість, військово-оборонний комплекс, агро-сектор, що у сукупності складає критичну інфраструктуру України.

ІР вже сьогодні фактично створює безліч нових продуктів і призводить до появи нових високотехнологічних компаній на ринку. Консультанти IDC припускають, що апаратне забезпечення стане найбільшою технологічною категорією, стартуючи з 2018 року: основні витрати підуть на модулі і давачі – більше 200 млрд.дол., з яких частина буде спрямована на інфраструктуру і безпеку. Послуги стануть другою за величиною технологічною категорією, за якою крокують програмне забезпечення та можливості підключення [1].

Наразі, всі **IoT-проекти (IoT-екосистеми)** умовно можна поділити на дві групи в залежності від типу комунікації пристроїв: **масові (Massive MTC) і критичні (Critical MTC)**. Перед кожним типом стоять свої завдання, і кожен з них має свої вимоги до мережі [2].

Масові IoT-проекти як рішення передбачають передачу невеликого об'єму даних від величезної кількості сенсорів, де один сервер приймає багато запитів від великої кількості пристроїв, обробляє їх та аналізує. Ці рішення характеризуються некритичністю гарантованої передачі-отримання інформації. Якщо один раз з якої-небудь причини інформацію з лічильника не отримано, дані будуть оновлені під час наступного сеансу передачі [3]. Якщо говорити більш образно, ціна помилки в масовій IoT-екосистемі є не такою значною і немає таких серйозних наслідків, як в критичній IoT-екосистемі. Для реалізації масових проектів потрібно, щоб пристрої були дешевими та споживали мало енергії. Частково такі проекти можуть бути реалізовані на основі GSM-мереж, але більшість з них побудовано на основі інфраструктури LTE [4].

Пропоную до розгляду **декілька прикладів масових IoT-проектів**, їхніх переваг для споживачів та впливу Інтернету речей на загальне сприйняття звичних процесів:

1) Власна екосистема Xiaomi. Прикладом є концепція **Smart Home від Xiaomi**: чайник закипить, щойно ви прокинетеся; очищувач повітря працюватиме, коли ви будете з'являтися біля нього; робот-пилосос зробить усю роботу, поки вас немає вдома; світло працюватиме, лише коли хтось є у

кімнаті, відстежуючи це датчиками руху. Набір компонентів такого розумного дому включає в себе хаб для підключення пристроїв (центр керування – комутатор), датчик руху; розумну розетку; датчик відкриття вікон/дверей; бездротову кнопку, датчику - аналізатору забрудненості повітря, датчик диму, датчик газу, камеру, нічник, який зафіксує в неосвітленій кімнаті рух, тощо [5].

2) FOODGER як менеджер «розумного» споживання їжі. Користувач відразу зможе бачити інформацію в режимі он-лайн про кількість продуктів у нього в холодильнику і приймати рішення, чи варто купувати той чи інший товар. Всі продукти, які необхідно докупити, вже будуть вказані єдиними списком у програмі. Окрім цього, програма сама знаходить рецепти під наявну кількість продуктів і пропонує їх користувачу. Якщо для якогось рецепту не вистачає декілька інгредієнтів, то програма запропонує їх придбати і автоматично додасть у список покупок. Коли користувач повертається додому, FOODGER попереджає завчасно про відсутність певних продуктів та пропонує по дорозі завітати до магазину [6].

3) Гаджет PetCube українського розробника, що дозволяє власникам домашніх тварин стежити на відстані за своїми улюбленцями. Це невеликий алюмінієвий куб, вагою у 589 грамів, у який вмонтовані ширококутна камера, динамік, мікрофон та лазерна указка. Гаджет підключається до Wi-Fi, саме цим дозволяючи господарю, незалежно від місця його перебування, перевірити, що робить вихованець удома. Керувати Petcube можна зі смартфона через мобільний додаток для IOS та Android. Цікава розробка українців дає господарю неймовірні можливості, дозволяючи погратися із улюбленцем на відстані за допомогою лазерної указки або зателефонувати йому [7].

Критичні IoT-проекти (або комунікації машинного типу з критичною місією, тс МТС) характеризуються своєю значимістю, адже при їх реалізації від роботи мережі залежить безпека життя користувача. Їхнє завдання — оперативно передавати інформацію через надійну стійку мережу. Характеристиками критичної машинної комунікації є низька затримка передачі сигналу (менш ніж 5 мілісекунд) та висока надійність, висока надійність для пристроїв різного рівня, підтримка недорогого та розширеного покриття, мобільність, тощо. Критичні IoT-рішення поки що існують у вигляді прототипів або тестових зразків, оскільки для їх реалізації потрібні мережі наступного покоління – 5G [8].

Критичні IoT-екосистеми застосовуються в роботі об'єктів критичної інфраструктури, зокрема, підприємствами та установами (незалежно від форми власності) таких галузей, як енергетика, промисловість, транспорт,

банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [9]. Критичні IoT-проекти починають відігравати центральну роль в промислових екосистемах Інтернету речей та мають потенціал для створення високодохідних підприємств, включаючи інтелектуальні транспортні системи, служби громадської безпеки та високоякісні додатки, тощо.

Пропоную до розгляду декілька прикладів критичних IoT-проектів:

1) Медичні пристрої, які прикріплені до пацієнта, виконують найважливішу функцію постійного надання автоматизованої допомоги щодо збереження життя, підтримки життєдіяльності організму людини. Ці медичні пристрої можуть бути імплантовані в організм пацієнта або прикріплені до пацієнта ззовні. Всі пристрої, які підключені до одного пацієнта, називаються персональними медичними пристроями (ПМД). Ці пристрої стають все більш поширеними, і їхній ринок прогнозується до 17 мільярдів доларів до 2019 року. В свою чергу, BSN (Network Sensor Network) – це мережа спеціального призначення, призначена для автономної роботи для підключення до різних медичних датчиків та імплантатів, розташованих всередині та ззовні людського тіла. Застосування цього механізму включає моніторинг фізіологічних даних людини, відстеження та моніторинг пацієнтів всередині лікарні, облік лікарських засобів у лікарнях, облік лікарських засобів інвазійно, тощо. Наприклад, інженери Caltech, Huntington Medical Research Institute і USC продемонстрували, що камера на смартфон і не інвазійно може надавати детальну інформацію про здоров'я людського серця. Замість 45-хвилинного ультразвукового сканування, тепер це можна зробити за 1-2 хвилини просто тримаючи телефон на шиї в певному місці [10, стр. 30].

2) Промисловий Інтернет речей. Прикладом може бути обладнання заводу Philips з виробництва бритв в Нідерландах, яке працює в неосвітленому приміщенні, де встановлені 128 роботів. Весь персонал заводу складається з дев'яти працівників [11]. Другим прикладом є використання роботизованих бурових установок, які зроблять видобуток нафти і газу більш рентабельним і дозволять різко збільшити відсоток вилучення вуглеводів з родовищ [12, с. 65].

3) Смарт-мережі. Головна ідея смарт-мереж полягає в підключенні електричних

генераторів і споживачів до однієї великої мережі, таким чином, що її можна

буде контролювати більш ефективно і надійно. Використовується велика кількість датчиків на вітряки і поліпшується якість обробки одержуваної з них інформації; сенсори на нових турбінах збирають в три - п'ять разів більше

корисної інформації, ніж раніше; збирається інформація про роботу трансформаторів, запобігаючи їх виходу з ладу і аварії на мережах; аналізуються важливі показники, що дозволяє управляти споживанням енергії, скорочуючи витрати споживачів і оптимізуючи навантаження на мережі, що, відповідно, відбивається на тарифах і на витратах кінцевих споживачів [13, с. 62].

Оскільки критичні IoT-проекти стосуються елементів національної критично важливої інфраструктури (наприклад, дамб, мостів та елементів електромережі), питання правового регулювання та безпеки реалізації таких критичних IoT-проектів є надзвичайно важливим на національному рівні.

Висновки:

Отже, сучасна модель правового регулювання щодо застосування технології IP в масових IoT-та критичних IoT-проектах має ґрунтуватися на нормативній базі, програмно-стратегічних документах, напрацьованому досвіді та найкращих прикладах правового регулювання аналогічного інституту в зарубіжних країнах.

Особливу увагу необхідно звернути на реалізацію критичних IoT-проектів. Оскільки критичні IoT-проекти потребують гарантій швидкого оновлення системи для їхньої ефективної роботи, адаптації до змінних умов життя, захисту від будь-яких виникаючих загроз; для критичних IoT-проектів будь-яка затримка сигналу є надзвичайно критичною; необхідна абсолютна надійність мережі; масштабні збої та критичні поломки на виробництвах, у застосування матимуть серйозні наслідки для великої кількості людей; найменша дизфункція може призвести до травм та/або загибелі людей, необхідно жорстко врегулювати на законодавчому та технічно-нормативному рівнях питання стандартів виробництва складових апаратного забезпечення та розробки алгоритмів, безпеки, стандартизації, стійкості архітектури до атак, конфіденційності, автентифікації даних, контролю доступу, захисту прав споживачів, тощо.

Список використаної літератури:

1. IoT: все, що потрібно знати про інтернет речей і про майбутнє сучасної цивілізації: інноваційний інтегратор Еверест / Юлія Долгоп'ятова. – 2018. – URL: <https://www.everest.ua/ai-platform/analytics/iot-vse-shho-potribno-znati-pro-internet-reczej-i-pro-majbutne-suchasnoi-civilizacii/>

2. Лекторій. Що таке інтернет речей і навіщо він потрібен?: НВ / Олексій Бондарєв. – 2017. – URL: <https://techno.nv.ua/ukr/popscience/lektorij-shcho-take-internet-reczej-i-navishcho-vin-potriben-1326653.html>

2.
2.

2. Система розумного дому від Xiaomi: чи є сенс купувати зараз?: KTC Блог. – URL: https://ktc.ua/blog/sistema_rozumnogo_domu_vid_xiaomi_chi_je_sens_kupuvati.html

3. Як працює FOODGER — IoT-проект для «розумного» споживання їжі: blog.imena.ua / Катерина Прогнімак. – 2016. URL: <https://www.imena.ua/blog/foodger-talk/>

4. Відтепер гратися з улюбленцем можна буде незалежно від відстані.: ТСН.ua – 2015. – URL: https://tsn.ua/nauka_it/petcube-ukrayinskiy-startap-yakiy-vraziv-svit-infografika-521171.html

5. Розумні міста, домівки й машини: навіщо нам інтернет речей: Beet Root Academy Блог. – URL: <https://beetroot.academy/uk/blog/rozumni-mista-domivki-j-mashini-navishho-nam-internet-rechey/>

6. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету міністрів України № 563 від 23 серпня 2016 р. / Офіційний сайт Верховної Ради України. URL: <https://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF/paran17>

7. О.А. Баранов, Інтернет речей: теоретико-методологічні основи правового регулювання. Т.1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія/ О.А. Баранов; НДПП НАПрН України – К.: Видавничий дім «АртЕк». – 2018. – 344 с.

8. Трекер для станка: когда в Россию придет промышленный интернет вещей: Forbes / Василь Чуранов. – 2017. – URL: <http://www.forbes.ru/tehnologii/337091-treker-dlya-stanka-kogda-v-rossiyu-pridet-promyshlenny-internet-veshchey>

9. О.А. Баранов, Інтернет речей: теоретико-методологічні основи правового регулювання. Т.1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія/ О.А. Баранов; НДПП НАПрН України – К.: Видавничий дім «АртЕк». – 2018. – 344 с.

9.

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

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

САМООРГАНІЗАЦІЯ ЯК РЕГУЛЯТОР

Цифрова епоха, що є складовою епохи інформаційної, знаменує істотні трансформаційні зміни у суспільстві, його регуляції та перспективах подальшого розвитку. У загальному вигляді під цифровою епохою можливо розглядати такий етап розвитку людства, що характеризується наступними основними рисами:

- лавиноподібне розповсюдження соціальних комунікацій, що побудовані на глобальних комп'ютерних мережах (на відміну від традиційних об'єднань людей та подібних соціальних інститутів);

- скасування паперу та інших подібних («твердих» та «індивідуальних») технологій зберігання інформації як інформаційної основи;

- максимальне пришвидшення обміну інформації, а також пов'язані з цим явища – штучний інтелект, пряма комунікація між технічними пристроями з обмеженим втручанням людини, розвиток новітніх інформаційних технологій у різних сферах, який зумовлюється самими технологіями.

На прикладі першої складової можливо прослідити принаймні 25-річний період розвитку комунікацій за напрямками: - електронні публічні дошки - форуми - спеціалізовані сервіси комунікацій - відкриті групи месенджерів. Функціонування практично усіх напрямів відбувається одночасно.

Друга складова характеризує відмову від традиційних протягом сторіч технологій зберігання, накопичення та розповсюдженні інформації за допомогою матеріальних носіїв (від пергаментних сувоїв до флеш-накопичувачів) на користь повністю електронних засобів зберігання інформації (хмарні, GRID та блокчейн-технології).

Третя складова є найбільш динамічною оскільки наразі неможливо передбачити яка саме технологія (віртуальної реальності, штучного інтелекту, Інтернету речей або розподіленого реєстру) ознаменує собою повний перехід до цифрової епохи, але уже зараз можливо стверджувати про його неминучість.

Який основний виклик для права - регулятора в умовах, що постають?

Проблеми, що традиційно визначені як правові, насправді є похідними або ж надто теоретичними. У даному випадку більшість із них можуть бути вирішені засобами традиційного права. Так, наприклад, цивільна відповідальність власника джерела підвищеної небезпеки – автомобіля не залежить від його конструкції. Тому автомобіль з автопілотом у цивільному праві мало відрізняється від звичайного.

Інша річ – це вплив технологій на ситуації безпосередньо правового регулювання. Мова йде про здатність програмного коду стати правом (поряд з іншими джерелами права), як це передбачав наприкінці 1990-х років Лоуренс Лессіг [1, р. 16].

У такому разі вирішуються наступні проблеми сучасного права:

- 1) Примус, суб'єкт примусу, підстава примусу, сила примусу та межа примусу. Ці питання втрачають сенс. У випадку, коли код регулює відносини примус забезпечується технологічно.

2) Тлумачення права відмирає. Застосування норми забезпечується технологічно, а отже немає потреби у правовій позиції як такій.

3) Юридичний факт визначається технологічно. За таких умов немає потреби у засобах засвідчення. Вірогідно, що першою юридичною професією, яка відійде у минуле, стане професія нотаріуса.

4) Юридичні докази втрачають сенс. Немає потреби у визначенні їх допустимості, сукупності та сили. Технологія забезпечує існування факту. Його доведення також здійснюється автоматично.

Але така думка є занадто глобальною. На рівні сучасної законотворчості криза права та криза нормотворчості особливо помітна. Так звані «криптовалюти» демонструють здатність вислизати з-під регуляції, а тому державам лишається отримати лише податок з тих осіб, що їх мають, або обмінюють на інші цінності. Пропозиції розробити законодавчий акт для штучного інтелекту натикаються на питання забезпечення примусу щодо суб'єктів законодавчого акту. На більш прагматичному рівні можливо спостерігати поступову юридизацію документів стратегічного планування, що традиційно знаходились поза межами права. Проблема легальності у мережі Інтернет знаходить парадоксальну відповідь в Ульріха Бека, який свого часу зазначив наступне:

«Світова економіка діє транслегально, тобто ні нелегально, ні легально» [2, с. 120].

Зрозуміло, що сучасні юристи мріють про відповідні правові технології, такий собі «legaltech», який би забезпечив технологічний примус над сутностями кіберпростору [3, с. 11].

Щодо майбутнього права загалом Т.Я. Хабрієва виокремила можливі варіанти:

- 1) право трансформується в інший соціальний регулятор;
- 2) право збереже власні субстанціональні ознаки і буде співіснувати із кодом;
- 3) з'явиться нова нормативна система, що матиме власне місце у системі соціальних норм [3, с. 18].

Такі варіанти розвитку подій можливо додати четвертим варіантом – коли люди відмовляться від регулятора на користь технічних засобів. Така «технічна утопія» є можливою. Але усталеність права, як регулятора у суспільстві не дасть змоги зробити це принаймні сьогодні та у найближчій перспективі.

На рівні побудови квазі-права мережевих форумів можливо спостерігати виникнення та становлення системи регулятора шляхом від визначення правил до розвинутою системи їх застосування. Але така самоорганізація забезпечується доволі простим примусом – владою модератора. У випадку

коли модератором стає програма, а її серцевиною – код можливо стверджувати, що технічна утопія стала реальністю.

Водночас право як феномен залишається. Чи здатне право само організовуватися у такому випадку?

В.Ю. Скоробогатов у своєму дослідженні, присвяченому проблематиці самоорганізації правових систем, прийшов до парадоксальних висновків – сама правова система має здатність до саморегулювання, як здатність зберігати власну цілісність. Ця трансформація зумовлена сучасними явищами (інформатизацією та глобалізацією), і полягає у тому, що право із засобу регулювання перетворюється на засіб саморегулювання. Але визначивши фактор саморегуляції дослідник не вважає, що право «відмирає», навпаки його трансформована роль лише підвищується [4, с. 148-151].

З такою точкою зору можливо погодитись, якщо визнати, що право є системою. У такому разі система дійсно здатна саморегулюватись. Принаймні код має бути зумовленим волею. А воля - виходити від суспільного сприйняття.

Тому найбільш перспективним у пізнанні пост-права, або «наступного права» є дослідження процесу самоорганізації, прикладів такої самоорганізації і сприйняття права саме як системи.

Список використаних джерел:

1. Lessig L. The Laws of Cyberspace// Taiwan NET Conference. Taipei. April, 3. 1998. URL: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf
2. Бек У. Влада і контрвлада у добу глобалізації. Київ: Ніка-Центр, 2011. 408 с.
3. Хабриева Т.Я. Право перед вызовами цифровой реальности. Доклад// Журнал российского права. 2018. № 9 (261), С. 5-16.
4. Скоробогатов В.Ю. Саморегулирование как свойство правовой системы: дисс. ... канд. юрид. наук. Москва, 2013. 186 с.

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

Каздобіна Ю., магістр політології та міжнародних відносин, Голова ГО «Українська фундація безпекових студій»

ПРАВА ЛЮДИНИ ТА ІНТЕРНЕТ РЕЧЕЙ: ВИКЛИКИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ

Інтернет речей з нами вже сьогодні. Звичний мобільний телефон не є просто телефоном: він приєднаний до інтернету, має велику кількість сенсорів та датчиків, через які збирає та передає все більше даних про нас

компанії, яка його виробила; платформам, на яких ми зареєстровані в якості користувачів; виробникам мобільних застосунків, якими ми користуємося.

Коли говоримо про інтернет речей, говоримо про приєднані до мережі речі, які мають адресу у мережі, мають здатність збирати, обробляти та передавати інформацію, та робити певні дії, виходячи з аналізу цих даних. Разом з тим, вони не мають власного наміру [2]. Це є новим явищем, яке вимагає осмислення його впливу на суспільні відносини та захист прав людини зокрема.

Міжнародні підходи

Починаючи з 2012 року на рівні ООН та інших міжнародних організацій йдеться про необхідність захищати права людини в мережі. Хотілося б зупинитися на ключових моментах декількох резолюцій. Починаючи з 2012 року Комісія з питань прав людини у Женеві приймає Резолюцію про просування, захист та реалізацію прав людини в Інтернеті. В ній вперше йшлося про те, що права людини, які захищені *оф-лайн*, мають бути захищені і *он-лайн*. Її остання версія від 2018 року, стверджує, що *компанії* так само мають захищати права людини, як і держави.

В зв'язку з тим, що збір персональних даних загрожує праву людини на приватність, «**Право на приватність у цифрову епоху**» стало ще однією важливою резолюцією ООН, ухваленою Генеральною Асамблеєю 18 грудня 2013 року. Остання версія резолюції, ухвалена 2017 року вперше підкреслює, що: "Держави повинні гарантувати, що будь-яке втручання у право на приватне життя відповідає принципам законності, необхідності та пропорційності".

Легальність – мають бути записані у законі та наперед відомі;

Необхідність – найбільш розмитий з критеріїв. Причини мають бути важливими та достатніми. Непропорційне обмеження ніколи не може бути визнано необхідним;

Пропорційність. пропонуване обмеження має бути «найменшим обмежувальним засобом» для досягнення відповідної мети.

Разом з тим, «**Доповідь ООН щодо епохи цифрової взаємозалежності**» визнає: «У багатьох випадках далеко не очевидно, як закони та договори про права людини, складені в пре-цифрову еру, повинні застосовуватися в епоху цифрових технологій». Причиною цього, серед іншого, є розмиття суверенітету держав та їх монополії на застосування легітимного насильства у віртуальному просторі.

Право на приватність та інші права, що опиняються під загрозою

Право на приватність визначено в ст. 12 Загальної декларації прав людини: «Ніхто не може зазнавати безпідставного втручання у його особисте і

сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію».

В контексті порушення права на приватність, зазвичай говорять про порушення ще двох прав людини – право на свободу висловлення (ст. 19) та право мирних зборів (ст. 20). Людина, яка знає, що за нею можуть слідкувати, скоріш за все буде обережніша з висловлюваннями та буде брати менш активну участь у громадському житті.

Виходячи з відомих на сьогодні випадків використання великих даних та взаємозв'язків, що виникають в мережі, до цього списку також можна додати свободу пересування (ст. 13), право володіти майном (ст. 17), право на демократію (ст. 21), а, також, різні форми дискримінації, які виникають в результаті застосування моделей, що спираються на великі дані.

Прикладом обмеження свободи пересування може слугувати Китай, де запровадження системи соціальних рейтингів, призвело до того, що люди, занесені в чорний список, не можуть купувати квитки на транспорт [6].

Право володіти майном включає в себе право насолоджуватися або розпоряджатися ним в рамках закону. Прикладом його порушення може стати ситуація з Apple, яка в 2016 році через оновлення програмного забезпечення ненавмисно заблокувала велику кількість телефонів, які ремонтували не в авторизованих сервісах компанії [4]. Це було непередбачуваним наслідком, але поставило питання, то хто ж має право розпоряджатися цим майном? Чи люди, які заплатили чималі гроші, мають право обирати, де вони будуть ремонтувати свої пристрої?

Подібна ситуація відбулась з електронними книжками, коли в 2009 році з електронних пристроїв для читання Kindle без відома їх господарів зникли раніше завантажені книжки Орвела [3]. Проблема виникла через те, що видавець, який розмістив їх на платформі, не мав права інтелектуальної власності на них. Амазон прибрав книгу з платформи та з пристроїв користувачів та повернув їм гроші. Але чи мав він право це робити без згоди власника?

Найконкретнішим у цьому контексті є «право на демократію». Згідно Загальної декларації прав людини «Кожна людина має право брати участь в управлінні своєю країною безпосередньо або через вільно обраних представників». Також, «Воля народу повинна бути основою влади уряду; ця воля повинна виявлятися у періодичних і нефальсифікованих виборах».

Як відомо, збір персональної інформації про користувачів інтернету з подальшим використанням результатів її аналізу для таргетування осіб та груп осіб відповідно до їх вподобань та психологічних особливостей є розповсюдженою практикою. Можливість знати, де людина фізично

знаходиться у певний момент часу використовується деякими компаніями для того, щоб вчасно надсилати пропозиції з метою вплинути на її вибір при покупці [7].

Використання великих даних для впливу на економічний вибір користувача вважається менш контраверсійним, хоча питання, наскільки це позбавляє людину права вільного вибору вже йдуть. У політичній площині ситуація з Cambridge Analytica та використанням персональних даних користувачів для просування певних політичних сил, поставила питання щодо втручання у вибори. І хоча йдеться про загрозу демократії загалом, варто відзначити, що така загроза стає можливою через обмеження свободи вибору конкретного виборця та фальсифікацію загального результату виборів, як кумулятивний ефект від безпосереднього таргетованого інформаційно-психологічного впливу на користувачів інтернету. Такий вплив відбувається через маніпулювання інформаційними потоками та рішеннями, що, на думку автора, є порушенням права людини на вільний вибір своїх представників.

Питання дискримінації при використанні даних для автоматизації прийняття рішень у своїй книзі «Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy» (Зброя математичного ураження: як великі дані збільшують нерівність та загрожують демократії) [1] досліджує математик Кеті О'Ніл. Вона аналізує американський досвід застосування алгоритмів, що аналізують великі дані, для прийняття рішень.

За її висновком, кореляції між змінними та петлі зворотного зв'язку, які виникають при застосуванні статистичних моделей, призводять до дискримінації. Вона наводить приклади автоматизації прийняття рішень судовою гілкою влади, в результаті чого вірогідність винуватості людини вважається більшою тільки через місце її проживання, та приклади вибору місця для патрулювання, коли більше патрулювання в одному місці призводить до фіксації більшої кількості порушень, і, в свою чергу, веде до збільшення патрулювання. Також, вона піднімає питання використання моделей в кредитуванні. Якщо рейтинг особи впав, її проценти зростають і їй стає ще важче вибратися з боргової ями без жодної надії очистити свою історію. Моделі також не є об'єктивними. Вони відображують упередження тих, хто їх складав. В результаті, дискримінація за якоюсь ознакою стає більш масштабною, адже автоматизація прийняття рішень призводить до більшої кількості рішень.

Виклики для держави

На сьогодні основні принципи захисту прав людини в цифрову епоху задекларовано, але їх імплементація стикається з багатьма перешкодами. Перше - це питання юрисдикції. Хоча запровадження системи IP адрес та

геолокації змінило інтернет, і він більше не є світом без кордонів, ці кордони є прозорими, для тих, хто хоче їх порушувати. Держави часто не мають можливості контролювати трафік, по-перше, через те, що інструменти контролю та самі мережі, на яких їх може бути встановлено, знаходяться у приватних руках. По-друге, через відсутність технічної можливості блокувати певну діяльність.

Так, наприклад, держава технічно не може завадити встановленню на мобільному телефоні громадянина України додатку, виданого російським банком для проведення платежів он-лайн. Встановлення ж цього додатку дає доступ його розробнику до приватних даних користувача, які зберігаються в його телефоні, або виробляються його телефоном у процесі користування, що призводить до порушення його права на приватність, а в разі виникнення кумулятивного ефекту може навіть становити загрозу національній безпеці.

Також, держава часто не має доступу до алгоритмів, які використовуються для обробки даних, якщо це робиться приватними компаніями. Ці алгоритми часто є комерційною таємницею, але їх застосування може призводити до навмисної або ненавмисної дискримінації.

В Україні захист прав людини в мережі ускладняється недостатнім усвідомленням проблем, пов'язаних з порушенням права на приватність, та недовірою громадян до правоохоронної системи. Загрозу становить не розповсюдження певної технологія, та не можливості, які вона надає. Проблема в тому, хто і для чого користується зібраними даними, та хто відповідає за їх збереження. На сьогодні спільного розуміння викликів та можливих відповідей на них нема.

Отже, на сьогодні проблема порушення прав людини он-лайн потребує більш широкого висвітлення, вивчення та пошуку як юридичних, так і технічних рішень. Також, її розв'язання потребує діалогу та побудови довіри між технічною спільнотою та державою, тому що у держави є право встановлювати правила, а у технічної спільноти є інструменти для того, щоб їх запроваджувати. Надважливе питання, яке треба обговорювати в процесі – це як контролювати застосування технологій комерційними та державними гравцями.

Список використаних джерел:

1. O'Neil, C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown, September 2016. 272 pages
2. Bunz, M., Meikle, G. The Internet of Things (Digital Media and Society). Polity, 2017. 149 pages
3. Загальна декларація прав людини : Організація об'єднаних націй, 10 грудня 1948 р. URL: https://zakon.rada.gov.ua/laws/main/995_015

4. Stone, Brad “Amazon Erases Orwell Books From Kindle”, July 17, 2009 URL: <https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html>
5. Breen, Marcia “Error 53: Latest iOS Update May Brick Your Phone If You Did This” February 5, 2016. URL: <https://www.nbcnews.com/tech/tech-news/latest-ios-update-will-brick-your-phone-if-you-had-n512326>
6. Zhong, Rui “In China, social credit is just a more invasive form of social media” 31 October, 2019. URL: <https://codastory.com/authoritarian-tech/china-socialcredit/?fbclid=IwAR2DlFd99A7i1J6K6VjDATZ8fj1ywreMEvBSnlAen6S6U0o2Svn8L5UxNGM>
7. Matsakis, Luise “How the West Got China's Social Credit System Wrong” 29 July, 2019. URL: <https://www.wired.com/story/china-social-credit-score-system/>
8. Hill, Thomas “How to Target Customers With Location-Based Marketing” 26 June 2018. URL: <https://business.tutsplus.com/tutorials/how-to-target-customers-with-location-based-marketing--cms-21507>

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

*Гребенюк М., к.ю.н., доцент,
керівник Міжвідомчого науково-
дослідного центру з проблем
боротьби з організованою
злочинністю при РНБО України*

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІОТ

В епоху масового використання можливостей Інтернету, постійного розширення цільової аудиторії користувачів виникає нагальна потреба в захисті прав та інтересів фізичних і юридичних осіб, держави, суспільства з метою недопущення кібератак, злочинних посягань у кіберпросторі (кіберзлочинів), розповсюдження в глобальній всесвітній мережі зараженого програмного забезпечення, вірусів, спамів, ботів тощо. Завдяки широкому використанню Інтернет-технологій у сфері суспільного життя дискусії з приводу розуміння змісту правового регулювання суспільних відносин у цій сфері, в тому числі в Україні, тривають.

В останні роки в перспективах розвитку Інтернет-сфери набуває активного поширення словосполучення «Інтернет речей». Як зазначається, поняття «Інтернет речей» (скорочено ІР, англ. – Internet of Things (IoT)) розглядається як «мережа різних об'єктів, що розширюється, – від промислових пристроїв до споживацьких товарів, які можуть обмінюватися інформацією і виконувати свої завдання, поки людина працює, спить або займається спортом. Інтернет речей складається з мільйонів датчиків і різних пристроїв, що генерують безперервні потоки даних, які можна

використовувати для поліпшення як життя взагалі, так і для підвищення ефективності бізнесу зокрема».

До основних проблем Інтернету речей можна віднести інформаційну безпеку і захист персональних даних. Технології IP значно посилюють ризики порушення конфіденційності персональних даних унаслідок того, що вони передбачають накопичення, циркулювання і використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання таких даних та забезпечення їх захисту від несанкціонованого використання [1, с. 90,85]. Вказане навіть призвело до появи нової галузі права – права Інтернету речей. Невипадково світові експерти стверджують, що Інтернет речей є однією з найперспективніших технологій останніх років. Складний комплекс взаємодії та взаємозалежності в системі об'єкт-суб'єктних взаємовідносин в інформаційному просторі також обумовлює необхідність вироблення та реалізації послідовної державної інформаційної політики, спрямованої, з одного боку, на захист законних прав і свобод особи в царині інформації, а з іншого – на забезпечення дотримання впорядкованих і законодавчо визначених правил і норм функціонування інших учасників інформаційних відносин [2, с. 15].

Виходячи із викладеного, Є.П. Литвинов визначає інноваційну галузь – Інтернет-право, розуміючи його як сукупність юридичних норм, які вивчають всесвітній кіберпростір та його особливості [3, с.158]. На переконання Л. Мудриєвської, з метою впорядкування правових основ використання глобальної мережі, необхідно прийняти окремий законодавчий акт «Про Інтернет», де не тільки були б визначені термінологічні засади діяльності, але й Інтернет розглядався б як багатоманітне явище, а саме як форма діяльності, засіб комунікації, спосіб суспільного життя і свідомості [4, с. 71].

Основними об'єктами, з приводу яких виникають суспільні відносини в кіберпросторі, є: 1) програмно-технічні комплекси, інформаційні системи, інформаційно-телекомунікаційні технології як засіб формування інформаційної інфраструктури, засоби зв'язку і телекомунікацій, що забезпечують здійснення інформаційних процесів (апаратна безпека, безпека додатків та серверів зв'язку); 2) інформація, інформаційні ресурси, інформаційні продукти, інформаційні послуги (контентна безпека); 3) доменні імена; 4) інформаційні права і свободи; 5) інтереси особи, суспільства, держави в кіберпросторі. Узагальнюючи викладене, можна виокремити дві основні групи відносин, які пов'язані з Інтернетом: безпосередньо з мережею Інтернет як телекомунікаційною мережею; з використанням мережі Інтернет, Інтернет-технологій для реалізації різних видів діяльності.

Тобто проблеми правового регулювання Інтернету і зокрема застосування технологій IoT доцільно розділити на дві великі групи: технічне регулювання, пов'язане з визначенням основних принципів функціонування; регулювання відносин, що виникають при використанні мережі Інтернет у діяльності фізичних та юридичних осіб. Враховуючи викладене, доцільно активізувати питання щодо розробки та схвалення світовою спільнотою на міжнародному рівні Декларації цифрових прав людини як фундаментального міжнародного документа сучасності, в якому важливе місце має відводитися саме впровадженню сучасних Інтернет технологій з метою їх використання у різних видах діяльності, включаючи Інтернет речей.

Список використаних джерел:

1. Баранов О.А. Захист персональних даних в сфері Інтернет речей / О.А. Баранов, В.М. Брижко // Інформація і право. – 2016. – №2 (17). – С. 85- 91;
2. Розлуцька А.Б. Людина як об'єкт і суб'єкт інформаційної політики: автореф. дис ... канд. політ. наук: 23.00.01 "Теорія та історія політичної науки" / А.Б. Розлуцька. – Нац пед. ун-т ім. М. П. Драгоманова. – Київ, 2012. – 16 с.;
3. Литвинов Є.П. Місце Інтернет-права в системі права та в системі юридичних наук / Є.П. Литвинов // Адміністративне право і процес. – 2013. – № 4(6). – С. 155–162;
4. Мудриєвська Л.М. Правове регулювання діяльності Інтернету та його значення у формуванні інформаційного суспільства в Україні / Л.М. Мудриєвська // Актуальні проблеми вітчизняної юриспруденції. –2013. Вип. №4. – С.63 – 71.

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

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

ПРАВОВЕ РЕГУЛЮВАННЯ БЕЗПІЛОТНОГО АВТОТРАНСПОРТУ

Науково-технічний прогрес втілює у життя донедавна футурологічні уявлення людства, одним з яких є впровадження штучного інтелекту у сферу експлуатації автомобільного транспорту. Феномен «безпілотного автотранспорту» дозволить знизити вплив «людського фактору» на функціонування автомобільного транспорту, адже прогнози аналітиків розвитку ринку найбільш потужних світових автомобільних концернів Tesla, General Motors, Google, Apple (США), Nissan, Toyota (Японія), Volkswagen (ФРН), Volvo (Швеція) й інших показують, що до 2020 року кількість безпілотних автомобілів у світі досягне 150 тисяч, а до 2035 року кількість робочарів зросте до 21 мільйона і почнеться ера безпілотного транспорту [1].

Враховуючи, що у сфері дорожнього руху будуть взаємодіяти різні види автомобільного транспорту, з огляду на повноту їх експлуатації як безпілотних (самокерованих) транспортних засобів, у США запропонована така їх класифікація: 1-й рівень – водій повинен бути готовий у будь-який момент взяти керування на себе (можуть бути присутніми такі автоматизовані системи, як круїз-контроль (ACC, Adaptive Cruise Control), автоматична паркувальна система і система попередження про схід зі смуги (LKA, Lane Keeping Assistance); 2-й рівень – водій повинен реагувати, якщо система не змогла впоратися самотійно, система управляє прискоренням, гальмуванням і керуванням, система може бути відключена; 3-й рівень – водій може не контролювати машину на дорогах з «передбачуваним» рухом (наприклад автобани), але бути готовим взяти управління; 4-й рівень – аналогічно 3-му рівню, але вже не вимагає уваги водія; 5-й рівень – з боку людини потрібно лише старт системи та вказівка пункту призначення [2]. Наведена класифікація показує, що до безпілотних автотransпортних засобів, оснащених відповідним обладнанням, слід відносити автомобілі, здатні функціонувати без контролю людини, починаючи із 3-го по 5-тий рівень. Також є очевидним, що безпілотні автомобілі не зразу опанують сферу дорожнього руху, а отже протягом певного часу людина буде залишатися причетною до безпосереднього керування транспортним засобом залежно від повноти його експлуатації системою штучного інтелекту.

Фахівці вважають, що впровадження штучного інтелекту в експлуатацію автомобільного транспорту забезпечить його значні економічні та соціальні переваги, зокрема такі, як безоплатність і безперервність діяльності, заощадження ресурсів рухомого складу під час експлуатації, беззастережне дотримання маршрутів і режимів руху, відсутність потреб убезпечення соціального захисту та інших гарантій, необхідних для водія-людини (екіпажу) тощо.

Поряд з цим, впровадження штучного інтелекту, позбавленого багатьох небезпечних властивостей людини, вплив на які у сучасних умовах у сфері дорожнього руху вдається майже вичерпаним, може забезпечити суттєве запобігання у дорожній інфраструктурі протиправним та помилковим діям людини, що слугуватиме докорінному зниженню аварійності у світі.

Сьогодні впровадження безпілотного автотранспорту відбувається цивілізованим шляхом під контролем органів державної та місцевої влади, самокеровані автомобілі перебувають у стані активних експериментальних досліджень та випробувань в обмеженій та врегульованій сфері дорожнього руху під контролем водія-людини та інших фахівців. Разом з цим, технічне обладнання, програмне забезпечення та інші технологічні складові

безпілотників швидко прогресують, що одночасно обумовлює необхідність вирішення багатьох питань їх функціонування. Тим більше, що сьогодні суспільство не задовольняє некерований підхід до розвитку нового феномену, адже воно вимагає негайного впровадження запобіжників від можливих негативних наслідків експлуатації безпілотного автотранспорту.

Очевидно, що в таких умовах зростає роль та значення правового регулювання безпілотного автомобільного транспорту, адже сьогодні функціонування автомобільного транспорту, що донедавна розглядалося як непорушна тріада «водій – автомобіль – дорога», значно ускладнюється за рахунок таких компонентів, як: «водій (людина) – водій (штучний інтелект) – безпілотний автомобіль – розумна дорога – правове середовище». Останній елемент – «правове середовище» [3, с. 94] – означає, що безпечне функціонування автомобільного транспорту неможливе без правового врегулювання національним законодавством, нормами міжнародного права, а також нормативно-правовими актами, що визначають соціальні, організаційні, управлінські, технічні, правові та інші засади дорожнього руху та його безпеки, спрямовані на захист життя та здоров'я людей, охорону власності та довкілля.

Безумовно, що просування у цьому напрямку, у першу чергу, залежить від державної політики, свідченням чому є положення постанови Кабінету Міністрів України «Деякі питання визначення середньострокових пріоритетних напрямів інноваційної діяльності галузевого рівня на 2017-2021 роки», якими серед інших заходів передбачено розвиток та впровадження систем штучного інтелекту, у тому числі: нових інтелектуальних технологій транспорту (безпілотні автомобільні засоби), а також інших технологій і систем у різних сферах життєдіяльності та безпеки держави [4]. Реалізації заходів щодо забезпечення розвитку штучного інтелекту має також сприяти діяльність новоствореного Міністерства цифрової трансформації України [5].

Разом з цим, необхідно відзначити, що на сьогодні в законодавстві України відсутнє поняття штучного інтелекту, вже не кажучи про правову регламентацію його функціонування, що, на наш погляд, вимагає прийняття «Концепції створення, впровадження та напрямків розвитку штучного інтелекту в Україні» та розробки на її основі відповідних державних цільових програм.

Аналіз досвіду найбільш розвинутих країн світу, в яких здійснені суттєві кроки у напрямку впровадження системних елементів штучного інтелекту у функціонування безпілотного автомобільного транспорту, що характеризується новітніми технічними і безпековими технологіями, показує необхідність вжиття комплексу заходів, пов'язаних з правовим регулюванням

стандартів виготовлення, сертифікації, ліцензування, маркування, обліку, випробування, серійного виробництва, тестування, реєстрації, експлуатації та утилізації безпілотного автотранспорту.

При цьому йдеться про необхідність удосконалення цивільного, господарського, адміністративного, кримінального та інших галузей чинного національного законодавства, що буде стосуватися питань функціонування безпілотного автомобільного транспорту.

Зокрема необхідні зміни у цивільному законодавстві України, яке регулює основи життєдіяльності суспільства та передбачає відповідальність за завдання шкоди джерелами підвищеної небезпеки, до яких має відношення функціонування безпілотного автотранспорту. Серйозного вдосконалення вимагатиме сфера соціального страхування, правові норми якої повинні забезпечити зняття виробничих, експлуатаційних, безпекових та інших ризиків, пов'язаних з особливостями безпілотного автотранспорту.

Суттєвих змін та доповнень вимагатимуть закони України «Про транспорт» (1994), «Про автомобільний транспорт» (2001), «Про дорожній рух» (1993), «Про міський електричний транспорт» (2004), «Про автомобільні дороги» (2005) та інші закони, а також «Правила дорожнього руху» і чисельні підзаконні нормативні акти.

При цьому йдеться як про додатковий понятійний апарат спеціальних термінів, так і особливості безпеки руху та експлуатації безпілотних транспортних засобів. Необхідно мати на увазі нові вимоги, що постають до «розумної дорожньої транспортної інфраструктури», з якою повинні взаємодіяти самокеровані автомобілі, що у свою чергу вимагає вдосконалення дорожніх знаків, розмітки та технічних засобів регулювання дорожнього руху, а також їх постійного утримання у належному стані.

Будуть вимагати розробки додаткових протоколів міжнародні конвенції з безпеки дорожнього руху, адже, наприклад, ст. 8 Конвенції про дорожній рух керується обов'язковим положенням, що «кожний транспортний засіб або склад транспортних засобів, що знаходиться у русі, повинні мати водія (курсив наш – В. М.)» [6]. Відповідно не містять будь-яких положень про безпілотний автотранспорт Європейські угоди [7], що доповнюють Конвенцію про дорожній рух та Конвенцію про дорожні знаки та сигнали [8], а також Європейська конвенція про покарання за дорожньо-транспортні злочини [9].

Окрім цього, у світовій царині впровадження безпілотного автотранспорту залишається необхідним вирішення питань, пов'язаних із застосуванням норм публічного права, адже якщо у контексті цивільно-правових норм питання визнання штучного інтелекту є таким, що викликає менше складнощів щодо відповідальності за заподіяння шкоди, то кримінальне

право не визнає суб'єктами злочинів нікого, окрім фізичних осіб. Певною рекомендацією у цьому відношенні для національного законодавства за стандартами ЄС є «наділення в перспективі робіт особливим правовим статусом, в рамках якого найбільш просунуті автономні роботи можуть створюватися як електронні особи і нести відповідальність за завдану ними шкоду у тих випадках, коли вони приймають рішення автономно або іншим чином самостійно взаємодіють з третіми особами» [10]. Така рекомендація покликала ідею визнання штучного інтелекту в якості електронної особи у Розділі XIV¹ Кримінального кодексу України.

Разом з цим, питання кримінальної відповідальності щодо штучного інтелекту при заподіянні шкоди у дорожньо-транспортних злочинах поки ще не має консолідованого вирішення юридичною спільнотою та вимагає його подальшого дослідження.

Список використаних джерел:

1. Когда беспилотные автомобили появятся на дорогах. URL: <https://bespilot.com/chastye-voprosy/kogda-ba-poyavyatsya-na-dorogakh> (дата звернення: 16.11.2019 р.).
2. Беспилотные автомобили: как они изменяют ситуацию на дорогах. URL: <https://yodnews.ru/articles/city/avtopilot> (дата звернення: 16.11.2019 р.).
3. Мисливий В. А. Злочини проти безпеки дорожнього руху та експлуатації транспорту : монографія. Дніпропетровськ : Юрид. акад. Мін-ва внутр. справ, 2004. 380 с.
4. Деякі питання визначення середньострокових пріоритетних напрямів інноваційної діяльності галузевого рівня на 2017-2021 роки : Постанова Кабінету Міністрів України від 18 жовтня 2017 р. № 980. URL: <https://zakon.rada.gov.ua/laws/show/980-2017-%D0%BF> (дата звернення: 16.11.2019 р.).
5. Положення про Міністерство цифрової трансформації України : Постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF> (дата звернення: 16.11.2019 р.).
6. Конвенція про дорожній рух. Відень, 8.11.1968 р. URL : [file:///C:/Users/vladi/Downloads/f23621n11%20\(1\).pdf](file:///C:/Users/vladi/Downloads/f23621n11%20(1).pdf) (дата звернення: 16.11.2019 р.).
7. Європейські угоди. Відень 01.05.1971 р. URL: https://zakon.rada.gov.ua/laws/show/994_866 (дата звернення: 16.11.2019 р.).
8. Конвенція про дорожні знаки та сигнали. Відень, 08.11.1968 р. URL: <file:///C:/Users/vladi/Downloads/f62430n7.pdf> (дата звернення: 16.11.2019 р.).
9. Європейська конвенція про покарання за дорожньо-транспортні злочини (ETS № 52). Страсбург, 30.11.1964 р. URL: https://zakon.rada.gov.ua/laws/main/994_484 (дата звернення: 16.11.2019 р.).
10. Нормы гражданского права о робототехнике : Резолюция Европарламента от 16.02.2017 г. 2015/2013(INL) P8_TA-PROV(2017)0051. URL: http://robopravo.ru/riezoliutsiia_ies (дата звернення: 16.11.2019 р.).

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

Жиляєв І., д.е.н., с.н.с., завідувач відділом економіки вищої освіти Інституту вищої освіти Національної академії педагогічних наук України

Фурашев В. М., к.т.н., с.н.с., доцент кафедри ІППВ, к.т.н., с.н.с.

ПРОБЛЕМИ НАЦІОНАЛЬНОГО ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ НОВІТНІХ ІКТ (НА ПРИКЛАДІ ІНТЕРНЕТУ РЕЧЕЙ)

Сучасний глобальний розвиток безпосередньо залежить від розробки та застосування новітніх ІКТ, які змінюють соціально-економічні відносини, як в світовому просторі, так й в конкретних країнах. Безперечно, поява та розповсюдження новітніх технологій вимагає формування нових правових регуляторів, пов'язаних з зазначеними технологіями.

Фактично, процес розбудови системи правових регуляторів застосування новітніх ІКТ в економіці та суспільному житті, відбувається двома шляхами: 1) створення глобальних наднаціональних норм та правил⁹, закріплених у відповідних угодах, стандартах та рекомендаціях тощо; 2) формування національного законодавства або на основі імплементації глобальних документів (на прикладі формування національного законодавства в країнах ЄС), або створення національних актів, які лише частково гармонізовано з актами міжнародного права у цій сфері. Безперечно, політика створення національних актів, які лише частково гармонізовано з актами міжнародного права у цій сфері, яка переважно застосовується в Україні завідомо приречена на значне відставання. Міжнародне право, що регулює відносини в ІКТ-сфері, стрімко розвивається як кількісно (поява нових актів), так й якісно (у відповідь на нові виклики і ризики).

Україна, вибравши політику часткової гармонізації національного права в ІКТ-сфері з вже чинними міжнародними актами (у першу чергу – ЄС), фактично нарізає відставання, оскільки не приймає активної участі в законотворчій діяльності, пов'язаній із створенням нових норм та правил.

Така національна законотворча політика вже показала свої значні недоліки при формуванні законодавчої бази регулювання у таких вразливих сферах, як захист персональних даних, штучний інтелект та кібербезпека¹⁰

⁹ Прикладом є формування протягом XX-XXI століть міжнародного права, що регулює авторські права та права інтелектуальної власності. Національні системи права у цих сферах будуються за гармонізованою консенсусною структурою, за єдиними принципами його побудови.

¹⁰ Законодавство ЄС (EU law) включає 919 актів європейського права, які використовують термін «cybersecurity» (кібербезпека) та стрімко розвивається. Тільки в 2019 році цей масив було поповнено 188 правовими документами. Не менш активно розвивається правове забезпечення

тощо. Виявилось, що запропонований правовий дизайн об'єкту регулювання новітніх ІКТ (образ системи правових відносин) та обрана модель української системи правового регулювання є мало релевантними як між собою, так й з системою чинних та перспективних актів наднаціонального правового регулювання.

Фактично новітні ІКТ займають достатньо скромне місце серед національних пріоритетів розвитку науки і техніки України¹¹.

Окрім того, варто зазначити, Україна втрачає певні позиції на глобальному ринку новітніх ІКТ за всіма стадіями життєвого циклу (від ідеї до утилізації), перетворюючись переважно у споживача новітніх ІКТ, втілених в товарах та послугах.

Виникає питання: чи варто розробляти свою національну нормативно-правову базу регулювання новітніх ІКТ або приєднатись до європейської системи правого регулювання?

Сучасна Україна має певні проблеми із ефективним застосуванням ІКТ. В значному ступені країна стала споживачем новітніх ІКТ.

Достатньо повільне впровадження новітніх ІКТ в українську економіку. Так, за даними державного статистичного спостереження щодо використання інформаційно-комунікаційних технологій на підприємствах у 2018 році:

- лише кожне четверте підприємство, що використовувало комп'ютери, мало ІКТ-фахівців (майже 11 тис. з 44 тис.). Лише кожне шосте з цих 11 тис. проводило курси для ІКТ-фахівців, кожне п'яте – ІКТ-курси для працівників;
- лише кожне десяте підприємство, що використовувало комп'ютери (4831 з 44 тис.), купували послуги хмарних обчислень упродовж року, з них: 2585 – фінансові або бухгалтерські прикладні програми; 2548 – електронної пошти; 2125 – офісне програмне забезпечення; 1788 – сервіс для зберігання файлів тощо;
- 632 підприємства здійснювали 3D-друк з використанням власних 3D-принтерів (включаючи орендовані), з них для 3D-друку: 1) 355 – прототипів або моделей для продажу; 2) 558 – прототипів або моделей для власного

використовують термін «Artificial intelligence» (штучний інтелект). Європейська стратегія щодо штучного інтелекту знайшла своє відображення в базових документах COM/2019/168 final «Building Trust in Human-Centric Artificial Intelligence» та COM(2018) 795 final Coordinated Plan on Artificial Intelligence [1].

¹¹ Див., зокрема: Перелік найважливіших науково-технічних (експериментальних) розробок за пріоритетними напрямками розвитку науки і техніки в рамках виконання державного замовлення на найважливіші науково-технічні (експериментальні) розробки та науково-технічну продукцію у 2019-2020 роках : розпорядження Кабінету Міністрів України від 10.07.2019 р. № 530-р; Перелік пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 року : постанова Кабінету Міністрів України від 07.09.2011 р. № 942; Перелік найважливіших науково-технічних (експериментальних) розробок за пріоритетними напрямками розвитку науки і техніки в рамках виконання державного замовлення на найважливіші науково-технічні (експериментальні) розробки та науково-технічну продукцію у 2018-2019 роках : розпорядження Кабінету Міністрів України від 26.07.2018 р. № 543-р тощо.

використання; 3) 230 – товарів для продажу за винятком прототипів або моделей; 4) 465 – товарів, які будуть використовуватись у виробничому процесі підприємства, за винятком прототипів або моделей [2].

“Інтернет речей” (Internet of Things). Для цілей статті будемо використовувати базове концептуальне визначення Міжнародного союзу електрозв’язку: Інтернет речей (Internet of things, IoT) – глобальна інфраструктура для інформаційного суспільства, що забезпечує розширені послуги шляхом з’єднання (фізичного та віртуального) речей на основі сумісних ІКТ. З широкого погляду IoT можна сприймати як концепцію з технологічними та суспільними наслідками [6].

Число пристроїв, підключених до Інтернету наприкінці 2018 року досягало 22 млрд. Згідно з підрахунками Strategy Analytics, майже половина – це корпоративний Інтернет речей. Очікується, що в найближчі роки найбільш швидко буде зростати кількість домашніх IoT-пристроїв. Експерти вважають, що до 2025 року в світі буде підключено 38,6 млрд. пристроїв, а до 2030 року – 50 млрд. [3].

Нормативно-правове регулювання ІКТ-сфери відносять до одного з ключових факторів розвитку електронної торгівлі. В доповіді Світового банку про світовий розвиток – 2106 зазначається, що для отримання максимальних цифрових дивідендів країнам, що розвиваються (Україну в доповіді – 2016 віднесено до групи країн, де цифрова економіка тільки народжується) доведеться не тільки провести реформи, покликані поліпшити доступ до інтернету, а й зосередити увагу на «аналоговому фундаменті» цифрової економіки, а саме - на навичках, інститутах і нормативно-правовій базі. При цьому жорсткість механізмів нормативно-правового регулювання відповідних ринків відносять до однієї з причин низьких обсягів (рівнів) електронної торгівлі [4].

В цьому сенсі Україна має значне відставання від розвинених країн із розвитком нормативно-правового регулювання розробки та впровадження новітніх ІКТ. Зазначений розрив має тенденцію до збільшення.

Законодавство України має майже 700 нормативних актів з використанням терміну “Інтернет”. Термін “Інтернет речей” використовується на рівні виключно постановки не зовсім чітко сформульованих завдань у декількох українських нормативно-правових актах: 1) вже майже забутий Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та плані заходів щодо її реалізації (2018)¹²; 2) Середньострокових пріоритетних напрямках інноваційної діяльності загальнодержавного рівня на

¹² Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р URL: <https://zakon.rada.gov.ua/laws/show/67-2018-p> (Дата звернення: 25.11.2019)

2017-2021 роки (напряма «Розвиток та впровадження систем Інтернету речей»)¹³; 3) Середньострокових пріоритетних напрямках інноваційної діяльності галузевого рівня на 2017-2021 роки (напряма «Розвиток та впровадження систем Інтернету речей», зокрема: технологій ідентифікації об'єктів; технологій обміну інформацією між пристроями та об'єктами; розробка систем захисту елементів Інтернету речей від несанкціонованого втручання)¹⁴.

Законодавство ЄС включає 515 актів європейського права, які використовують термін «Internet of Things» (All EU law). З них за авторами: European Commission (224); Council of the European Union (172); European Economic and Social Committee (61); Directorate-General for Communications Networks, Content and Technology (59); European Parliament (48) тощо; за роками видання: 2019 – 77; 2018 – 149; 2017 – 107; 2016 – 83; 2015 – 15 тощо [1].

Проблеми безпеки в новітніх ІКТ займають ключове місце. Так, дослідники Світового банку зазначають, що при впровадженні передових ІКТ, наприклад, хмарних технологій або Інтернету речей (IoT), фірми можуть зіткнутися з більш серйозними ризиками порушення безпеки: в рамках цих технологій пристрої з'єднуються за допомогою Інтернету, і відбувається обмін даними між різними бізнес-функціями. Замість створення бар'єрів на шляху транскордонних потоків даних уряди можуть активізувати свої зусилля в сфері навчання підприємців методам забезпечення безпеки в ІТ області, розробки нормативно-правової бази, що гарантує наявність у більшості фірм мінімального рівня ІТ безпеки, і забезпечення захищеності національної Інтернет-інфраструктури від несанкціонованого доступу [5].

Міжнародна організація стандартизації (МОС) сформувала сукупність з 21 стандарту, присвячених «Інтернету речей». Ще 11 стандартів на цей час у стадії розробки¹⁵.

Рекомендації. За прикладом державної політики в сфері стандартизації перейти до кваліфікованого перекладу та визнання чинними в Україні актів європейського права, що регулюють діяльність у ІКТ-сфері.

Список використаних джерел:

1. База даних EUR-Lex <https://eur-lex.europa.eu/homepage.html>
2. Використання інформаційно-комунікаційних технологій на підприємствах у 2018 році. Держстат України, 2019.

¹³ Постанова Кабінету Міністрів України від 28.12.2016 р. № 1056 URL: <https://zakon.rada.gov.ua/laws/show/1056-2016-п> (Дата звернення: 25.11.2019)

¹⁴ Постанова Кабінету Міністрів України від 18.10.2017 р. № 980 URL: <https://zakon.rada.gov.ua/laws/show/980-2017-п> (Дата звернення: 25.11.2019)

¹⁵ Див.: URL: <https://www.iso.org/ru/committee/6483279.html> (Дата звернення: 25.11.2019)

3. Internet of Things Now Numbers 22 Billion Devices But Where Is The Revenue? URL: <https://iotbusinessnews.com/2019/05/16/04619-internet-of-things-now-numbers-22-billion-devices-but-where-is-the-revenue/> (Дата звернення: 25.11.2019)

4. World Bank. 2016. World Development Report 2016: Digital Dividends. Washington, DC: World Bank. URL: <http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf> (Дата звернення: 25.11.2019)

5. Kelly, Tim, Aleksandra Liaplina, Shawn Tan, and Hernan Winkler. 2017. "Reaping Digital Dividends: Leveraging the Internet for Development in Europe and Central Asia." Washington, DC. World Bank. doi: 10.1596/978-1-4648-1025-1.

6. Recommendation ITU-T Y.2069 Terms and definitions for the Internet of things <http://handle.itu.int/11.1002/1000/11700>

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

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

ДО ПИТАННЯ ВИЗНАЧЕННЯ ПРОБЛЕМАТИКИ МІЖНАРОДНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ ПРИ ВИКОРИСТАННІ НОВІТНІХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Інститут міжнародно-правової відповідальності держави за інформаційну діяльність має особливості, викликані характером міжнародних інформаційних відносин. Конвенційні та окремі доктринальні джерела розглядають питання відповідальності держави, як суб'єкта міжнародного права, виключно з позицій поширення інформації традиційними засобами інформації (радіомовлення, телевізійне мовлення, поширення друкованої, візуальної та аудіо продукції). При цьому міжнародно-правова відповідальність передбачається виключно за поширення протиправної, неправдивої або перекрученої інформації.

Зауважимо, що, тематика використання та відповідальності ЗМІ у міжнародних відносинах не відходить на другий план, вона залишається актуальною і на сьогодні, і на майбутнє.

Зміни у інформаційних відносинах, що викликані застосуванням технологій Інтернету речей, штучного інтелекту, робототехніки, криптовалют, технологій блокчейн, «хмарних» технологій, «великих даних» та інших,

викликають широке коло питань, вагомими серед яких постають питання, пов'язані із інститутом міжнародно-правової відповідальності

Сучасна проблематика інституту міжнародно-правової відповідальності за правопорушення при використанні новітніх інформаційно-комунікаційних технологій є доволі широкою. У зв'язку з цим обмежимося розглядом питань відповідальності у сфері кібернетичної безпеки, зокрема при використанні штучного інтелекту.

Враховуючи постійне розширення спектру використання цих технологій у кримінальних, терористичних і військових (військово-політичних) цілях, провідні країни світу впродовж десятиліть активно формують і вдосконалюють власні сектори безпеки. Разом з тим, не припиняються спроби світового співтовариства впорядкувати використання інформаційно-комунікаційних технологій, і запровадити відповідальність за незаконні дії з їх використанням як з боку окремих осіб, угруповань і організацій, так і з боку держав.

Вагомими серед загроз, які охоплюють і визначають об'єкти, на захист яких повинні спрямовуватись намагання кібернетичного захисту, виступають:

- використання інформаційно-комунікаційних технологій для здійснення ворожих дій та актів агресії, а також на шкоду основним правам і свободам людини;

- цілеспрямований деструктивний вплив на критично важливі структури інших держав (в тому числі інформацію і інформаційні ресурси, елементи інфраструктури, програмне забезпечення, засоби і комплекси зв'язку, технологічні процеси тощо);

- дії в кібернетичному просторі з метою дестабілізації політичної, економічної і соціальної системи іншої держави;

- створення умов технологічної залежності у сфері інформаційно-комунікаційних технологій та інші.

Вважаємо, що крім зазначених, одним із майбутніх випробувань кібернетичних систем безпеки держав, і вірогідно, майбутніх напрямків міжнародно-правового регулювання відносин відповідальності за правопорушення, буде відбуватись з боку штучного інтелекту.

У зв'язку з чим актуальними можуть виступити наступні питання:

- 1) що впливатиме на кібернетичні системи безпеки держав в нових умовах?;
- 2) на що саме впливатиме?;
- 3) які першочергові питання повинні бути вирішені для запобігання такому впливу?;
- 4) які можуть бути напрямки правового (міжнародно-правового) регулювання?

Вважаємо, що вплив на кібернетичні системи держав будуть здійснювати кілька чинників, серед яких:

а) кількість кінцевих пристроїв, що отримуватимуть найрізноманітнішу інформацію (прогнозовано – 1 млн. кінцевих пристроїв на 1 кв. км);

б) нові засоби і способи швидкісної передачі інформації (LiFi, квантовий зв'язок);

в) засоби і технології, що працюватимуть із гігантськими обсягами зібраної, переданої і отриманої інформації (Super Data Base).

Здійснення впливу відбуватиметься на управління державою в цілому (управлінські рішення на рівні держави).

Серед першочергових питань, що повинні бути вирішені для запобігання такому впливу:

- яка інформація стане пріоритетною для запобігання її збиранню з нашої території (не тільки з баз даних, але й з території держави)?

- як контролювати потоки інформації, що збиратимуться на постійній основі гігантськими обсягами з нашої території?

- як впливати на масштабні потоки інформації, які пасивно вводяться на нашу територію?

- як впливати на масштабні потоки інформації, які цілеспрямовано вводяться на нашу територію?

- якими є вірогідні впливи на алгоритми та технології захисту інформації в умовах поширення технологій штучного інтелекту?

Вважаємо, що для України, актуальними напрямками міжнародно-правового регулювання, серед яких окреме місце буде виокремлено відповідальності, постануть:

- укладення двосторонніх, регіональних і універсальних міжнародних угод з інформаційної і кібернетичної безпеки;

(варіант з укладенням універсальної міжнародної угоди (кількох угод) – на сьогодні - проблематичний і малоймовірний, враховуючи тривалу і не результативну діяльність Групи урядових експертів з інформаційної безпеки ООН, на яку покладено, серед інших, і розробку проекту угоди);

- входження до систем колективної безпеки, що передбачатиме спільні плани і заходи [1]; цей варіант – вірогідний, потребуватиме укладання окремої угоди (кількох угод) з міжнародною організацією. У разі, якщо вступ до такої (регіональної або універсальної) організації потребуватиме проходження тривалої процедури, це може стати альтернативним варіантом, що сприятиме забезпеченню кібернетичної безпеки держави в умовах масового впровадження і використання технологій штучного інтелекту.

На нашу думку, вартими є подальші дослідження окремих аспектів режиму міжнародно-правової відповідальності за інформаційну діяльність

суб'єктів міжнародного права, зокрема пов'язаних із протиправним використанням державами сучасних інформаційно-комунікаційних технологій і засобів.

Список використаних джерел:

1. Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій / І.М. Забара // Журнал порівняльного і європейського права. – 2017, - №3. – С. 1-12.

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

Гордієнко С., д.ю.н., доцент

БУТИ, ЧИ НЕ БУТИ ЗБАЛАНСОВАНОМУ РОЗВИТКУ ЛЮДСЬКОГО КАПІТАЛУ В УКРАЇНІ?

Заголовок для тез виступу запозичено з назви парламентських слухань 10 квітня 2019 року. Підставою цьому є підтвердження теоретичних напрацювань автора у галузі інформаційної та інноваційної діяльності, а також сфери захисту інтелектуальної власності. Адже творцем і носієм якісно нових знань є люди - найцінніший капітал держави, який політичне керівництво України повністю ігнорує.

У своїх дослідженнях автором зроблено висновок, що в сучасних умовах розвитку суспільних відносин назріла нагальна потреба кодифікації норм права зазначених сфер життєдіяльності суспільства для створення реальних можливостей для капіталізації нематеріальних активів. Підтвердженням цьому є цікавий історичний приклад: «... своїм захопленням науками і кодифікацією імперських указів більше чим за 100 років займався візантійський імператор Феодосій Другий у 420-423 роках нашої ери»¹⁶.

Автор впевнений, що процедура кодифікації є незначною, але вкрай важливою частиною стратегії інформаційної безпеки України. А в якому ж стані знаходиться державна практика? Спробуємо це проілюструвати.

Так, адвокат юридичної фірми «Ілляшев та Партнери», стверджує, що Антимонопольний комітет України зобов'язав Державне підприємство «Національний офіс інтелектуальної власності» скасувати процедуру закупівлі послуги з розробки проекту Національної стратегії розвитку та функціонування державної системи правової охорони інтелектуальної власності після 2020 р.

Даний проект у березні цього року було доручено розробляти Громадській організації «Український інститут майбутнього». Повного тексту

¹⁶ <http://www.newsru.co.il/israel/16apr2019/coin307.html>

рішення АМКУ ще немає, тому в чому точно полягає порушення, невідомо, але ця ситуація дуже добре показує стан реформи у сфері інтелектуальної власності України загалом, яка загальмувала. Велику кількість законопроектів так і не було прийнято Верховною Радою України¹⁷, а може це й добре, бо окремі їх положення було б доцільним врахувати у стратегії.

Остання має бути ретельно опрацьована, оскільки саме цей документ буде взято за основу подальшої державної політики у сфері інтелектуальної власності. Хочеться сподіватися, що подальшу стратегію розвитку буде сформовано з урахуванням думок фахівців у цій сфері, для яких і мають створюватися умови.

Щоб сформувавши правильну стратегію, безумовно, потрібно оцінити стан сфери на момент її розробки. Наскільки сильно просунулася Україна в розвитку охорони інтелектуальної власності?

Останні п'ять років втілювалися в життя Концепція реформування державної системи правової охорони інтелектуальної власності в Україні та Національна стратегія розвитку сфери інтелектуальної власності в Україні на період до 2020 р.

Проаналізувавши обидва вищезгадані документи, можна виокремити основні проблеми галузі інтелектуальної власності України, визначені на державному рівні: недосконала та інертна на зміни система державного управління сферою правової охорони інтелектуальної власності; відсутність істотного прогресу в адаптації нормативно-правової бази в сучасних економічних і політичних умовах; складні економічні умови; недостатнє нормативно-правове регулювання питань, пов'язаних із порушенням прав на об'єкти права інтелектуальної власності; недостатнє використання інноваційного потенціалу об'єктів інтелектуальної власності; низький економічний потенціал запатентованих винаходів і корисних моделей, дія яких не підтримується після п'яти років.

Підсумовуючи останню п'ятирічку, можна сказати, що станом на початок 2019 р. для вирішення зазначених проблем було започатковано ряд дій, які незавершені.

¹⁷ До одних із найважливіших неприйнятих проектів можна віднести: "Про внесення змін до деяких законодавчих актів України щодо вдосконалення правової охорони географічних зазначень"; "Про внесення змін до деяких законодавчих актів України щодо вдосконалення правової охорони інтелектуальної (промислової) власності"; "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення прав у сфері інтелектуальної власності та захисту цих прав"; "Про внесення змін до деяких законодавчих актів України щодо вдосконалення правової охорони винаходів (корисних моделей)"; "Про національну систему охорони інтелектуальної власності в Україні".

Можна з упевненістю заявити, що проблеми, з якими Україна входила в 2014 р., залишилися невирішеними. Тому в наступній стратегії потрібно обов'язково проаналізувати причини такого провалу реформ і розробити шляхи їхнього вирішення.

Важливо, щоб до стратегії ввійшли такі ідеї, як створення сприятливих умов для активізації інноваційної діяльності, формування інноваційної культури; визначення та впровадження неподаткового механізму стимулювання суб'єктів господарювання до впровадження винаходів і технологій; удосконалення системи економічного стимулювання суб'єктів господарювання з комерціалізації об'єктів інтелектуальної власності та формування ринку таких об'єктів; посилення відповідальності за порушення прав інтелектуальної власності; завершення реформи відносно ефективної структури державного управління сферою інтелектуальної власності та ліквідація корупційних ризиків; підвищення культури громадян щодо чужої інтелектуальної власності¹⁸.

Тобто, практично всі основні теоретико-прикладні висновки автора тез практикуючим адвокатом озвучено¹⁹.

Однак, як ми вже писали раніше - науково-обґрунтовані потреби суспільства розходяться діаметрально з практикою нашого державного будівництва. Підтвердженням цього ще раз виступають парламентські слухання на тему: «Збалансований розвиток людського капіталу в Україні: завдання освіти і науки», які відбулися 10 квітня 2019 року, які підготував Комітет з питань науки і освіти.

До участі були запрошені народні депутати, представники Кабінету Міністрів, центральних органів виконавчої влади, обласних державних адміністрацій і обласних рад, Національної академії наук України, національних галузевих академій науки, закладів освіти та наукових установ, роботодавців, громадських освітянських і студентських організацій.

¹⁸ Нікулеско Д. Нової стратегії розвитку сфери інтелектуальної власності не буде? // Дзеркало тижня №13, 6 квітня-12 квітня. https://dt.ua/macrolevel/novoyi-strategiyi-rozvitku-sferi-intelektualnoyi-vlasnosti-ne-bude-307764_.html

¹⁹ Гордієнко, С. Г. Інноваційна діяльність та право на інтелектуальну власність. Теоретичні основи, правові регулятори [Електронний ресурс] : курс лекцій : [розділ 1- 3] / С. Г. Гордієнко; НТУУ «КПІ». – Електронні текстові дані (3 файли: 832 Кбайт; 1,12 Мбайт; 140 Кбайт). – Київ : НТУУ «КПІ», 2018. – Назва з екрана. Електронний ресурс: <http://ipp.kpi.ua/about/vikladachi/gordienko/>; Гордієнко, С. Г. Теорія та практика протидії загрозам інноваційній діяльності та інтелектуальній власності в Україні [Електронний ресурс] : курс лекцій / С. Г. Гордієнко. – Електронні текстові дані (1 файл: 1,01 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 348 с. – Назва з екрана. Електронний ресурс: <http://ipp.kpi.ua/about/vikladachi/gordienko/>.

Міністр освіти та науки Л. Гриневич наголосила, що розвиток людського капіталу – це надзвичайно важлива тема і «одна з першочергових цілей, про які йдеться у Середньостроковому плані пріоритетних дій Уряду до 2020 року». Міністр звітувала про стан освітньої галузі на усіх рівнях: від початкової і до вищої освіти, а також про хід і результати реформ.

Водночас, з метою самореалізації людей, Л. Гриневич закликала розвивати ринок праці, національний бізнес – вкладати кошти в Українські інновації, державу - створювати податкові стимули. «Коли ми навчили, дали освіти, захистили, коли люди завершили аспірантуру-докторантуру, після того, як в них держава Україна вклала стільки коштів, і вони отримали хорошу освіти, яку визнають всі індекси, можна вкрати їхнє майбутнє, якщо не дати їм можливості самореалізуватися в цій країні. І при цьому можна вкрати майбутнє України», - наголосила Міністр.

Із співдоповіддю виступив перший заступник голови Комітету з питань науки і освіти О. Співаковський, який наголосив на важливості проведення таких слухань. «Ми повинні розуміти – де є погане, а де є гарне. Що зроблено? Що не зроблено? Що потрібно зробити? Де є тренди, на які ми повинні дати відповідь? Бо ця відповідь – це філософія подальшого розвитку нашої освіти», - зазначив О. Співаковський.

Виступаючи на засіданні, представник Президента України у Верховній Раді І. Луценко розповіла про зміни у всіх суспільних галузях з метою збалансованого розвитку людського капіталу.

Є. Нищук відзначив, що відбувається переосмислення освітніх підходів у світі і, зокрема, невід’ємною складовою освіти стає мистецтво. Міністр окремо зупинився на проблемах мистецької освіти і перспективах їх вирішення.

Учасники засідання говорили про необхідність: збільшення фінансування сфери освіти; покращення доступності навчання, зокрема, для дорослих; розвитку інклюзивності і гендерної рівності; реформи професійно-технічної освіти; стимулювання розвитку ринку праці; гармонізації розвитку економіки і людського капіталу; створення молодіжної інфраструктури на місцях; покращення профорієнтації; розвитку мережі дошкільної та шкільної освіти; забезпечення освіти з прав людини; популяризації робочої освіти.

Із заключним словом на Парламентських слуханнях виступив перший заступник голови Комітету з питань науки і освіти О. Співаковський, який зазначив, що «людський капітал – достатньо складна і динамічна абстракція, яка визначає ключовий елемент розвитку нації, держави і її економіки, добробуту громадян, визначає як сукупність життєвих, духовних та професійних компетентностей громадян, які забезпечують сталий розвиток країни у її основних проявах. Проблема створення, збереження і розвитку

людського капіталу та вимірювання відповідних трендів, сьогодні є не просто актуальною, а в умовах України, на мій погляд, є питанням національної безпеки».

Закриваючи засідання, заступник Голови Верховної Ради О. Сироїд наголосила на важливості проведеної дискусії і необхідності більше часу відводити на виступи представників з народу, а не влади, хоча все вийшло навпаки!!!

Згідно з підготовленим Комітетом з питань науки і освіти проектом резолюції за підсумками парламентських слухань на тему: «Збалансований розвиток людського капіталу в Україні: завдання освіти і науки», **вироблено конкретні рекомендації** Верховній Раді, Кабінету Міністрів, профільним міністерствам, силовим структурам, НАН України, місцевій владі і керівникам навчальних закладів у сфері дошкільної, повної загальної середньої та вищої освіти, а також освіти дорослих і позашкільної освіти²⁰.

Тобто, Верховна Рада України парламентсько-президентської республіки знову лише **РЕКОМЕНДУЄ** всім і вся, і знову очевидно, що «ВСЕ»!!!, замість визначення конкретних завдань відповідним органам та строків з їх реалізації. Також з прес-релізу парламентських слухань не помітно уваги влади до науки та інноваційної діяльності, а тим паче з питання визначення завдань освіти і науки у напрямі збалансованого розвитку людського капіталу в Україні.

Останнє означає, що проблеми підготовки фахівців з інтелектуальної власності, інформаційної, аналітичної та інноваційної діяльності в Україні цікавлять лише наукові установи та навчальні заклади, які працюють у зазначеній сфері, а не Міністерство Освіти України та владу.

Тобто, як показує життя, чекати збалансованого розвитку людського капіталу в Україні не приходитьсья.

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

*Головко О., к.ю.н., ст. викладач
кафедри публічного права КПП імені
Ігоря Сікорського, старший науковий
співробітник НДІ інформатики і
права НАПрН України*

ЗАГРОЗИ ПРАВАМ ЛЮДИНИ: ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІОТ

Технології «Інтернету речей» (IoT) активно входять у суспільно-побутове життя людини. Однак, бажання бізнес-груп швидко отримати

²⁰ <https://www.rada.gov.ua/news/Novyny/170143.html>

великий дохід від продажу IoT технологій становить величезну загрозу безпеці користувачів. Відповідальність за це має бути покладена на розробників та постачальників IoT товарів. Це необхідно передбачити в національному законодавстві. Правила користування та навіть доступу до IoT мають бути узгодженими з вже існуючими національними нормами щодо використання звичайних товарів чи послуг, не пов'язаних з IoT технологіями, втім, мати ряд особливостей.

Наразі є потреба гармонізувати міжнародні стандарти безпеки, враховуючи сферу використання технологій Інтернету речей. Йдеться, зокрема, про обов'язкову сертифікацію такої продукції. Окрім цього, пропонуємо ввести обов'язкове страхування по аналогії з передбаченим законодавством страхуванням майнових інтересів потерпілих від дорожньо-транспортної пригоди.

Такий захід передбачатиме забезпечення відшкодування шкоди, заподіяної життю, здоров'ю чи майну потерпілих внаслідок використання технологій IoT в побутових умовах та захист майнових інтересів страхувальників.

Об'єктом обов'язкового страхування цивільно-правової відповідальності мають стати майнові інтереси, пов'язані з відшкодуванням шкоди, заподіяної життю, здоров'ю, власності потерпілих внаслідок експлуатації конкретної технології Інтернету речей, вираженої у певному предметі.

З одного боку, технології IoT полегшують життя людини у багатьох сферах, сприяють реалізації певних потреб та сприяють доступу до більш ефективних механізмів реалізації прав людини. З іншого боку, може виникнути нова загроза тим же правам людини. Адже технології IoT можуть стати зброєю нової епохи, забезпечивши потенційним злочинцям доступ до тих сфер життя людини, в яких задіяні технології IoT. Дану загрозу доречно розглядати на прикладі Deepfake, методики використання зображення людини для заміщення ним вже існуючих персонажів на відео. Відмінність даної технології від подібних, не пов'язаних з використанням штучного інтелекту полягає в тому, що виявити неправдивість зображення досить складно і на перший погляд не видається за можливе. Фактично, будь-яке зображення особи може бути використано проти неї з метою політичної, соціальної, професійної дискредитації з особистих, корисливих, хуліганських чи навіть сексуальних мотивів.

Deepfake-підроблення у новинах мають в першу чергу політичний мотив, а фінансові шахрайства посягають на гарантоване Конституцією право власності.

Використання технологій Deepfake у порнографічних відео та нове явище, таке як «порно-помста» зараз є реаліями країн Західної Європи, США. Найпоширенішими з них є використання облич зірок у відео порнографічного характеру. Окрім цього, Deepfake використовується як свого роду віртуальне насилля над минулими партнерами, що ставить за мету зруйнувати її/його життя, дискредитувати в суспільстві, зламати кар'єру тощо.

Ще одним небезпечним надбанням технологій IoT є пілотний проект VoC від Adobe, який виробник проголосив «Photoshop для аудіо». Дана технологія може перетворити 20-хвилинний аудіо-запис у кардинально іншу промову з такими ж мовними поворотами, паузами та іншими особливостями вимови людини.

Закордонні криміналісти вже навчились виявляти технології Deepfake як за допомогою технічних засобів та програм (e.g., проект «Media Forensics»), так і за рахунок аналізу фейкових відео та виявлення особливостей, таких як відсутність дихання чи кліпання очима. Втім, поєднання Deepfake та VoC значно ускладнює це завдання, адже основним в даному випадку є принцип своєчасності виявлення фейку до того моменту, поки він не набув масового спричинення, спричинивши невідворотні негативні наслідки, такі, наприклад, як паніка серед населення.

Проблематика, з якою зіштовхнулись на заході полягає у тому, що виробники Deepfake-відео відстоюють реалізацію цієї можливості в межах першої поправки, говорячи, що створені ними відео це форма карикатури, пародії чи сатири, яка жодним чином не видається за реальність. Наприклад, перші творці порнографічних матеріалів з обличчями зірок стверджували, що це був мистецький проект еротичного змісту.

На відміну від США, у Великобританії є практика притягнення до відповідальності за такі дії, розцінюючи їх як харасмент (від англ. «harassment» — переслідування, домагання). Більше того, проголошена ініціатива на виокремлення цього діяння як окремого виду злочину. В США пропонують з цього приводу виокремити нові склади злочинів, такі як крадіжка особистих даних (identity theft) та кібер переслідування (cyberstalking) та порно-помста (revenge porn).

Чи можуть технології IoT становити загрозу людині, опинившись в руках зловмисників? Так, однозначно. Чи йдеться в даному випадку, виключно про посягання на інформаційні права людини? Ні, в жодному разі такі посягання не обмежуються інформаційною складовою, адже за допомогою технологій IoT може здійснюватись посягання на право на життя, освіту, вільний розвиток своєї особистості, на повагу до його гідності, втручання в його особисте і сімейне життя, на свободу світогляду і віросповідання.

Наприклад, із застосуванням технологій Deepfake можливе створення такого відео, де людина нібито буде не коректно виражатися щодо своєї релігії, що може спричинити виключення її з релігійної общини, що в деяких випадках є несумісним із проживанням в певних регіонах, а інколи викликає надмірну агресію та навіть насилля.

Іншим прикладом негативного впливу методики Deepfake є складнощі в реалізації права доступу до державної служби чи до служби в органах місцевого самоврядування через фейкове відео, яке відображає неетичну поведінку такого службовця. Згідно чинного закону України «Про державну службу», порушення правил етичної поведінки державного службовця є підставою для притягнення його до дисциплінарної відповідальності.

Узагальнюючи зазначимо, що є три моделі розвитку подій у зв'язку з масовим впровадженням технологій IoT. Перша передбачає вкрай негативний розвиток, який створить умови для інтенсифікації загроз у кіберпросторі через підвищення рівня кіберзлочинності, що спричинить абсолютну руйнацію конфіденційності користувачів, систематичні порушення прав людини, та навіть створення загрози кібервійни.

Друга модель полягає в зловживанні владою при використанні технологій IoT, що передбачатиме тотальний контроль кіберпростору за допомогою використання можливостей Інтернету речей, використання цензури, штучне створення перепон для реалізації населенням своїх потреб з метою збільшення економічної вигоди еліти. Прикладом останнього може стати тотальний контроль та обмеження вільного потоку товарів, послуг, капіталу та даних. В умовах цифрової трансформації суспільства такі дії цілком можна вважати такими, що порушують основоположні права людини, а отже створюють фундамент для вчинення міжнародних злочинів проти миру та безпеки людства. Адже в пояснювальній записці до Римського статуту Міжнародного кримінального суду вони визначені як «найбільш ненависними злочинами, так як являють собою серйозний руйнівний вплив на людську гідність, принижують та спричиняють деградацію особистості».

Третя модель покликана створити умови для задоволення інтересів та потреб людини, забезпечення та підвищення ефективності в реалізації своїх прав за рахунок використання технологій IoT та превенції ризиків від використання цих технологій. Реалізація даної моделі потребує поєднання зусиль юристів та розробників технологій IoT, покликане створити сприятливі умови використання досягнень Інтернету речей, однак не виходити за межі правового поля. Більше того, існує потреба в розробці комплексу морально-етичних норм для розробників та користувачів технологій IoT.

Окремим аспектом варто розглядати правові дослідження з питань цивільної та кримінальної відповідальності у правовідносинах з використанням ІоТ, зокрема, йдеться про аспекти захисту конфіденційності та власності особи, забезпечення інформаційної безпеки тощо.

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

Мошко М., співробітник Служби безпеки України

Прозоров А., к.ю.н., старший викладач Національної академії Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ЛЮДИНИ І ГРОМАДЯНИНА В УМОВАХ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІОТ

Аналіз діяльності органів влади України свідчить про недосконалість державної політики в інформаційній сфері в аспекті забезпечення прав та свобод людини і громадянина в умовах використання технологій Інтернет-речей. Зазначеному сприяють такі неагтивні фактори як: корупція, консервативність державного апарату, непристосоване до сьогоднішніх реалій законодавство, неефективна система підвищення кваліфікації кадрів, і, водночас, ефективно діючі деструктивні державні запобіжні механізми, які заохочують посадовців відмовлятися від конче-потрібних реформ та змін. Останні, як не парадоксально, допомогли б зберегти систему від стагнації, постійного відставання, руйнації та колапсу. Також це сприяло б зменшенню передумов до порушень чи посягань на конституційні права громадян [1].

Підтвердженням неефективності в цьому напрямку можна назвати публічні ініціативи з поступового запровадження якісного 3G-Інтернету по всій території України, а вже потім плавного переходу на 4G та можливо на 5G. У зв'язку з цим включаються відповідні бюрократичні державні механізми гальмування та обмеження, наприклад, на частоти, які забезпечують належне функціонування 5G-Інтернету. При цьому, вітчизняним компаніям під виглядом новітніх технологій в Україні часто доводиться закуповувати застаріле обладнання із розвинених країн Заходу або Сходу, щоб «вписатися» в державні обмеження. У зв'язку з цим українські суб'єкти господарювання втрачають фінансові та технологічні ресурси на постійну заміну застарілого обладнання, а також на його подальший перепродаж чи утилізацію, що сприяє виникненню передумов до порушення Закону України «Про інформацію» [2]. Звичайно, що фінансовий тягар та втрату сучасних технологій відчують на

собі і громадяни України через підвищення вартості послуг за не завжди якісний продукт.

Варто зазначити, що поряд із неспростовними перевагами, вступ України до Світової організації торгівлі [3] та підписанням відповідної угоди [4] дозволив приватним монополістам, які займають значну долю ринку Інтернету-речей в Україні укріпити свою монополію за рахунок громадян України. Зокрема це стосується блокування дрібного опту під час імпорту товарів забезпечення Інтернет-речей для громадян України в обхід офіційних дилерів.

Схожу ситуацію можна спостерігати на ринку цифрового телебачення, який замість імплементації більш сумісного з різними пристроями та технологією «IPTV» стандарту «ATSC 3.0», примусово переводився на старіючий стандарт «DVB-T2». Щоправда ситуація виявилася ще гіршою. Замість очікуваного результату зі збільшення охоплення територій, автори на особистому досвіді переконалися, що навіть на території м. Києва для прийому всіх телеканалів «Т-2» потрібна якісна зовнішня антена з підсилювачем, оскільки кімнатна забезпечувала якісний прийом лише у безпосередній близькості до телевізійної вежі, в іншому разі якість телебачення була не кращою за аналогове мовлення, не говорячи про ситуацію в українських регіонах. У результаті пересічний український громадянин при бажанні використовувати «безкоштовне» цифрове мовлення в Україні повинен був витратися на покупку, встановлення та налаштування за середніми оцінками суму у розмірі майже мінімального прожиткового мінімуму.

У той же час, державні органи, в яких циркулює інформація з обмеженим доступом суттєво втратили свою ефективність через обмеження, передбачені в підзаконних нормативно-правових актів, які регламентують впровадження та функціонування комплексних систем захисту інформації (КСЗІ) в частині запровадження організаційних заходів захисту системи від витоку інформації та порядку обліку матеріальних носіїв інформації [5]. У даному аспекті, страждають як самі чиновники так і громадяни, оскільки через уповільнені процеси та масову бюрократизацію процедур перші не здатні оперативно виконувати функціональні обов'язки, а другі страждають від надто уповільнених процесів, від яких вони залежать в силу обставин, незважаючи на те, що безпосередньо не беруть у них участі через обмеженість доступу до цієї інформації [6-8].

Останній аспект у поєднанні з окремими проявами корупції та нормативно-правовими актами, які регламентують подвійні та потрійні стандарти, створює перешкоди для проведення ефективної державної політики в даній сфері. У зв'язку з цим створюються передумови до створення КСЗІ на

об'єктах, де обов'язковість та доцільність їх створення викликає запитання. Цьому сприяє відсутність дієвого механізму контролю над доцільністю присвоєння грифів обмеження доступу до інформації та підзаконних нормативно-правових актів, доступ до яких автоматично втрачає велика кількість висококваліфікованих юристів. Разом з цим, чиновники часто опиняються в ситуаціях, коли будь-яка з двох можливих дій буде незаконною. У зв'язку з цим часто обирається варіант бездіяльності із усіма впливаючими наслідками та втратою авторитету державних органів перед громадянами через неефективну діяльність та неможливість захисту їх інтересів.

Варто зазначити, що ухилення представниками державних органів влади від реєстрації підзаконних правових актів в Міністерстві юстиції України всупереч статті 2 Постанови КМ України від 28.12.1992 № 731 (*чинна редакція від 08.04.2019*) «Про затвердження Положення про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади», незважаючи на відсутність в них інформації з обмеженим доступом, може створювати передумови до порушення прав, свобод й законних інтересів громадян [9].

Підсумовуючи викладене, можна констатувати застарілість нормативно-правових актів, які прямо чи опосередковано регулюють сферу Інтернет-речей. Тому з метою недопущення поглиблення кризи неефективного державного механізму регулювання зазначеної сфери з витікаючими наслідками порушення конституційних прав та свобод громадян, на нашу думку, бажано в найближчій перспективі забезпечити розроблення з використанням сучасних методів та з урахуванням науково-технічного прогресу відповідної нормативної бази.

Список використаних джерел:

1. Конституція України, редакція від 21.02.2019 № 254к/96-ВР, URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Закон України «Про інформацію», редакція від 16.07.2019 № 2657-XII URL: <https://zakon.rada.gov.ua/laws/show/2657-12>
3. Протокол про вступ України до Світової організації торгівлі, редакція від 16.05.2008 № 981_049, URL: https://zakon.rada.gov.ua/laws/show/981_049
4. Угода про заснування Світової організації торгівлі, редакція від 27.11.2014 № 995_342, URL: https://zakon.rada.gov.ua/laws/show/995_342
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», редакція від 19.04.2014 80/94-ВР URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр>
6. Закон України «Про державну таємницю», редакція від 05.08.2018 № 3855-XII URL: <https://zakon.rada.gov.ua/laws/show/3855-1201>
7. Закон України «Про затвердження Зводу відомостей, що становлять

державну таємницю», редакція від 19.04.2019 № z0902-05 URL: <https://zakon.rada.gov.ua/laws/show/z0902-05>

8. Закон України «Про доступ до публічної інформації», редакція від 01.05.2015 № 2939-VI, URL: <https://zakon.rada.gov.ua/rada/show/2939-17#n3>

9. Постанова КМУ «Про затвердження Положення про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади», редакція від 08.04.2019 № 731-92-п, URL: <https://zakon2.rada.gov.ua/laws/show/731-92-%D0%BF>

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

Телька А., студент Національного авіаційного університету
Безкорвайна Ю., ст. викладач кафедри інженерії програмного забезпечення факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету

ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ НА ЗАХИСТ І ПРАВА НА ПРИВАТНІСТЬ

Починаючи з другої половини XVIII століття людство бореться за свої права: свобода слова, релігійні вподобання, рівноправ'я жінок, – кожні 10-20 років вектор боротьби міняється в залежності від людських потреб. Сьогодення диктує – боротьбу за приватність. Ще 20 років тому, ми не замислювалися про приватність, це були проблеми публічних особистостей аніж пересічних людей. Проте, у вік технологій важко залишитися непоміченим: на вулицях встановлюють відео-камери, будь-який запис в мережі зберігається майже все життя автора і таких прикладів безліч [1].

Конфіденційність - це питання прав людини. Технологічні досягнення, такі як, IoT (Internet of Things – інтернет речей), мають серйозні проблеми конфіденційності. Якщо використовувати цю технологію з відповідальністю, можна навіть захистити право на приватність. IoT та конфіденційність були описані як несумісні - ідеї, створені в різні часи з різними цілями. В Загальній Декларації Прав Людини (1948 р.) визначено: «Ніхто не повинен зазнавати свавільного втручання у його приватне життя, родину, будинок або листування, а також нападів на його честь чи репутацію. Кожна людина має право на захист закону від такого втручання чи нападу...». З розвитком технологій, на початку 70-х років минулого століття в Європі вийшли перші закони, що регулюють використання особистої інформації. Вже тоді стало зрозуміло, що нові форми спілкування потребують нових форм захисту. Не

тільки за допомогою законів регулюють права та свободи, а й самі технології регулюють захист прав і свобод людей [2].

Шифрування та інші методи безпеки можуть сприяти та захищати право на приватність у багатьох випадках. Шифрування реорганізує інформацію у нечитабельний формат, доступний лише за допомогою ключа шифрування. Надійне шифрування може забезпечити захист певних повідомлень і, таким чином, певних особистих даних від сторонніх «очей». У багатьох випадках це може допомогти підтримати право на свободу вираження поглядів, асоціацій та зборів, особливо серед уразливих груп.

Однак шифрування, може замаскувати заворушення та інші проблеми громадської безпеки. Захист конфіденційності людей не завжди означає захист безпеки всіх людей. Зі злочином важче боротися, коли інформація не є такою доступною для поліції. Часто важко зрозуміти, які саме особисті дані охоплені «правом на приватність» та які дані є загальнодоступними [3].

Конфіденційність та безпека часто зустрічаються в протизв'язі один до одного. Доступ до даних та контроль за ними залишаються ключовими рушіями захисту та порушень прав людини на цій арені. Уразливості в системі IoT можуть безпосередньо призвести до невпевненості та відсутності конфіденційності.

Таким чином, повинні бути запроваджені стандарти конфіденційності, щоб гарантувати захист права на приватне життя однаковою мірою. В іншому випадку вона буде маніпулюватися.

Список використаної літератури:

1. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв'язку з автоматизованою обробкою даних : посіб. / В. Брижко, М. Швець [та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.

2. Internet of Things: Privacy&Security in a Connected URL: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IPrpt.pdf>

3. K. Rose, S. Eldridge, L. Chapin The Internet of Things : An Overview. Understanding the Issues and Challenges of a More Connected URL: <http://www.internetsociety.org/sites/default/files/ISOC-IP-Overview-20151022.pdf>

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

*Зуєв В., к.ю.н., доцент кафедри
філософії*

*Антонець К., магістрант
кафедри філософії*

БЕНЧМАРКІНГОВА ПРИРОДА ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУРЕЧЕЙ У СОЦІАЛЬНІЙ РОБОТІ

Теоретико-методологічні засади соціальної роботи формуються в наслідок кумуляції різних наукових знань, які системно реалізуються в притаманних соціальній роботі процесах та явищах. Кожна наука виокремлює у навколишній реальності й робить предметом розгляду конкретну сферу, яка досліджується за допомогою спеціально розроблених методів та належним чином підібраних засобів. Оскільки об'єктом соціальної роботи є індивіди й різні соціальні групи та колективи, вона спирається на дослідження інших соціогуманітарних наук, зокрема, історії, соціології, психології тощо. А про її інтегративну природу свідчать наявні міжпредметні зв'язки, якими соціальна робота узалежнена з окремими природничими дисциплінами – медициною, біологією, фізіологією та ін. Водночас наукове пізнання здійснюється з метою задоволення матеріальних, соціальних і духовних потреб людини і передбачає інтеграцію досягнень учених у різних галузях наукового знання. Цим зумовлена наявність міждисциплінарних зв'язків теорії соціальної роботи з дослідженнями різних соціогуманітарних наук, а також застосування соціальними працівниками під час роботи з клієнтами комплексних та загальнонаукових методів і технологій.

Водночас теоретичною і методологічною основою соціальної роботи є філософія, яка увиразнює найзагальніші засади буття людини і суспільства. Саме філософія розглядає людину як активну живу істоту, яка існує в світі різними способами. Найтехнологічнішими серед них є діяльність та спілкування. Але не меншою мірою і екзистенцію, і навіть «діяльність душі» (Е.Фромм) можна також зарахувати до високотехнологічних способів існування людини. З огляду на це важливо не тільки змістовно конкретизувати найзагальніші способи людської буттєвості, але й досконало освоїти серед них ті, які увиразнюють життя людини в його найбільш технологічних проявах – від практики і праці до внутрішнього споглядання і рефлексії. Успішно справитися з цим завданням в царині соціальної роботи може допомогти застосування бенчмаркінгу – однієї з найпродуктивніших сучасних соціальних технологій. Бо саме бенчмаркінгова технологія як вивчення і впровадження методів і прийомів успішної діяльності лідерів-надавачів соціальних послуг

дозволяє на підставі порівняння з ними виявити і вдосконалити слабкі сторони і напрями власної роботи.

Ключовими аспектами на шляху подібного вдосконалення є «порівняння» й «еталон». Водночас порівняння може і має проводитися не тільки з іншими надавачами соціальних послуг, але й усередині власної організації з її кращими підрозділами, службами, процесами тощо. Це дає підстави вважати бенчмаркінг технологією еталонного порівняння і безперервного вдосконалення будь-якого способу існування людини. Але слід пам'ятати, що еталон як умовний критерій не може залишатися постійним. Він має повсякчас відповідати зміні зовнішніх умов і внутрішніх чинників, а також можливостям безперервного самовдосконалення.

Бенчмаркінг дає можливість соціальним працівникам встановлювати більш амбітні, але водночас реалістичні цілі роботи на підставі розгляду еталонів, які окреслюють кращі методи функціонування соціальних служб, та шляхом порівняння критично важливих елементів провадження власної діяльності з цими еталонами. Такий підхід має особливі переваги під час удосконалення допоміжних процесів соціальної роботи. Еталоном для їх порівняння можуть бути обрані не тільки лідери соціальної роботи, але й ті надавачі соціальних послуг, які є безпосередніми конкурентами. Так само критерієм можуть слугувати соціальні установи, які належать до інших галузей продукування соціальних послуг, оскільки допоміжні процеси часто мають схожість незалежно від галузевої приналежності.

Позаяк система надання соціальних послуг – це складна, відкрита соціально-економічна і соціально-політична конструкція, яка складається з сукупності державних органів і недержавних організацій, діяльність яких спрямована на надання соціальних послуг особам або окремим соціальним групам, які перебувають у складних життєвих обставинах, не можуть самотійно їх подолати та потребують сторонньої допомоги. Метою такої системи є розв'язання життєвих проблем, від яких потерпають індивіди або соціальні групи. Втім, функціонування подібної системи має бути спрямоване насамперед на профілактику негативних соціально-економічних явищ, сутність якої полягає в попередженні та запобіганні виникнення складних життєвих обставин, формами реалізації яких є, зокрема, соціальна реабілітація, інтеграція та реінтеграція тощо. Загалом, система надання соціальних послуг має репрезентувати таку соціальну підтримку клієнтам соціальної роботи, яка сприятиме створенню умов для самотійного розв'язання ними власних життєвих проблем, відновленню втрачених навичок і функцій, подоланню або мінімізації негативних наслідків обставин, котрі вони не в змозі подолати за допомогою наявних у них ресурсів [1].

Нині бенчмаркінг розглядається не тільки як технологія одержання інформації для порівняння і вироблення методики відбору кращих організацій, які можуть виявитися еталоном для інших, але й як розробка таких стандартів корпоративної культури в середині будь-якого соціального інституту, які могли би сприяти застосуванню кращих методів діяльності. Тому бенчмаркінгу соціальній роботі допомагає вирішувати різні завдання – орієнтувати соціальні установи або надавача соціальних послуг на зовнішнє середовище з метою постійного пошуку нових можливостей для розвитку; визначати лідерів серед надавачів соціальних послуг та їх сильних і слабких сторін; усвідомлювати необхідність постійних змін щодо надання соціальних послуг; планувати власну діяльність на підставі цілепокладання й оцінки умов зовнішнього середовища; формулювати тривалі цільові показники якості роботи, які значно перевершують поточні; здійснювати відбір ідей щодо кардинального покращення соціальної політики та надання соціальних послуг; підвищувати ефективність функціонування соціальної установи; орієнтувати організаційну й управлінську культуру на прагнення до вдосконалення і розвитку, підвищення кваліфікації, компетентності соціальних працівників.

З огляду на притаманну йому змагальність бенчмаркінг є потужним інструментом соціальної роботи, за допомогою якого надавач соціальних послуг може проводити порівняльний аналіз її наслідків, засобів, персоналу і процесів. Він дозволяє соціальним працівникам усвідомити необхідність відриву від старого способу дії і дає можливість зрозуміти, що тільки шляхом постійних змін на краще заклад або установа, в якій він працює, здатна належним чином функціонувати. Тому з кожним роком у світі популярність бенчмаркінгу в соціальній роботі зростає. Але в Україні, на жаль, переважна більшість соціальних працівників про бенчмаркінг в соціальній роботі майже нічого не знає. Водночас сьогодні жодна соціальна установа не може вижити, не приділяючи належної уваги вивченню сильних рис лідерів галузі та не навчаючись у кращих у сфері власної діяльності.

Необхідність упровадження бенчмаркінгу в соціальній роботі полягає в тому, що він, по-перше, уточнює, наскільки успішним може бути надавач соціальних послуг; по-друге, свідчить про те, як змінити спосіб надання таких послуг, щоб клієнт міг не тільки їх одержати, але й прагнув самотійно вирішити власні проблеми. Крім того, щоб не залишитися «на задвірках історії», всім надавачам соціальних послуг – від уповноважених органів державної влади до юридичних і фізичних осіб та фізичних осіб-підприємців – незалежно від розміру та сфери їх діяльності треба постійно вивчати і застосовувати передовий досвід в царині соціальної роботи.

Отже, предметом бенчмаркінгу в соціальній роботі є дослідження з метою одержання інформації шляхом порівняння методів і технологій, прийомів і засобів конкретної соціальної установи або надавача соціальних послуг з еталонним процесом надання соціальних послуг іншими соціальними установами чи надавачами таких послуг, яке допоможе запозичити і використати їх знання та досвід у власній діяльності. Водночас предметом здійснення бенчмаркінгу в соціальній роботі є вдосконалення або покращення роботи власної соціальної установи чи надавача соціальних послуг з метою покращення соціальної ситуації як реального стану проблеми конкретного клієнта. Тому, використовуючи бенчмаркінгу соціальній роботі, соціальний працівник має докладати значних зусиль, оскільки метою його діяльності є покращення соціальної ситуації клієнта, превенція як попередження її погіршення або, принаймні, полегшення суб'єктивного переживання клієнтом власного становища. Зокрема, в умовах спаду виробництва та масового безробіття допомогти індивідам знайти нове робоче місце не так вже й легко. Але надати їм соціально-психологічну підтримку, позбавити від негативних особистісних реакцій на безробіття соціальний працівник цілком спроможний.

Інакше його найближчим часом доведеться замінити роботами, здатними серйозно впливати на розвиток сучасного суспільства. Це дозволить багатьом процесам відбуватися без участі людини, на зміну якій приходить Інтернет речей як глобальна мережа предметів, оснащених необхідними для взаємодії один з одним технологіями. Соціальні проекти Інтернету речей стають усе масовішими – від лічильників і «розумних» будинків до надання медичних та різних соціальних послуг. Наприклад, вже сьогодні лікарі можуть віддалено відслідковувати стан здоров'я пацієнтів і в разі необхідності оперативно втручатися в режимі реального часу в процес лікування та істотно покращувати якість життя людей. Так само завдяки Інтернету речей одержувачі соціальних послуг мають усе більше можливостей для раціонального управління ресурсами й оптимізації процесу одержання соціально-побутових, соціально-медичних, психологічних, юридичних, інформаційних та інших соціальних послуг.

Здавалося б, що саме тут і клієнтам, і організаторам соціальної роботи могла б стати в нагоді бенчмаркінгова природа технологій Інтернету речей: вивчай, порівнюй, критично осмислюй і запроваджуй їх у власній діяльності з огляду на різні способи прояву людської активності. Але застосування технологій Інтернету речей в соціальній роботі ще не набуло ні популярності, ні системної природи не лише тому, що їх широкому впровадженню перешкоджають складні технічні та організаційні проблеми. Насамперед потребує вирішення ціла низка теоретичних питань – від визначення понять і

концептуального обґрунтування необхідності впровадження технологій Інтернету речей до затвердження стандартів та нормативних актів їх застосування в соціальній роботі.

Список використаних джерел:

1. Дубич К.В. Сучасна система надання соціальних послуг України // Державне управління: удосконалення та розвиток. № 3, 2015 / URL : <http://www.dy.nayka.com.ua/?op=1&z=821>

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

Некрутенко В., Сертифікований спеціаліст із захисту персональних даних (CIPP/E), юрист компанії Legal Nodes

PRIVACY OF THINGS: СОЦІАЛЬНО-ПРАВОВІ ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ

28 вересня 2018 року, Каліфорнія схвалила законопроект, який врегульовує питання конфіденційності та безпеки в одному із провідних секторів розвитку технологій - Інтернеті Речей (Internet of Things, IoT). Каліфорнійський закон регулює використання і захист даних, зібраних пристроями Інтернету Речей. Дане регулювання є одним із перших прикладів прийняття спеціалізованого акта регулювання сфери Інтернету Речей та показує наявність соціального запиту у даній сфері.[1]

Кажучи про Інтернет Речей зазвичай мається на увазі будь-яка річ, яка підключена до інтернету і збирає дані навколо неї через датчики. Термін Інтернет Речей також використовують для опису мережі розумних пристроїв, які спільно збирають і зіставляють дані навколо них, використовуючи для цього інтернет-з'єднання та/або інші мережеві підключення.

Вважається, що перший пристрій Інтернету Речей створив американський технолог Джон Ромки ще в 1989 році. [2] Сьогодні, завдяки розвитку технологій, мережі інтернет, а також збільшенню обчислювальних потужностей, розумні пристрої стають звичайним явищем у повсякденному житті. Майже будь-який предмет підключається до внутрішньої або всесвітньої мережі інтернет - холодильники, дверні дзвінки, колонки, пілососи і навіть розетки.

З однієї сторони, підключення пристроїв дає людині переваги мережі інтернет та комп'ютера у будь-якому предметі навколо. Це дозволяє залишити значну частину повсякденної рутини для таких пристроїв, завдяки віддаленому контролю над пристроями і даними, які вони збирають. Єдине, що повинна

зробити людина - відрегулювати роботу Інтернету Речей відповідно до свого повсякденного графіку.

З іншої сторони, зручність створює ризики для кінцевих користувачів, про які вони можуть і не знати. Робота розумних пристроїв повністю залежить від їх підключення до Інтернету, якості їх датчиків і даних, які вони збирають. Крім того, пристрої Інтернету Речей спроектовані таким чином, що управляти або регулювати їх роботу вручну є досить важко, на відміну від класичного персонального комп'ютера або смартфонів.

Говорячи про інформацію, використання розумних пристроїв в повсякденному житті людей значно розширює збір персональних даних. Наприклад, «фітнес-трекери», підключені іграшки або автоматичні транспортні засоби збирають великі обсяги інформації про кожного користувача. Фактично, підключені пристрої можуть збирати дані цілодобово, часто без відома чи згоди кінцевих користувачів.

Це призводить до виникнення двох основних соціально-правових проблем Інтернету Речей:

1. Захист пристрою або інформації, яку він збирає, від несанкціонованого доступу; та
2. Забезпечення приватності користувачів Інтернету Речей.

Оскільки пристрої Інтернету Речей у значній кількості випадків збирають інформації про конкретну особу, яка ними користується, на таку інформацію буде поширюватися режим захисту персональних даних. У відповідності до визначення законодавства України, персональні міданими є відомості про фізичну особу, яка була або може бути ідентифікована. Під таке досить широке формулювання підпадає і будь-яка статистика або історія користування розумним пристроєм, що збирається у систематичному вигляді.[3]

Основними вимогами із захисту персональних даних, які будуть стосуватися збору даних через Інтернет Речей та які знайшли своє відображення у статтях 6, 8, 11, 12, 24 ЗУ «Про Захист Персональних Даних» є:

1. Забезпечення прозорості збору та використання даних (статті 6, 8, 12) - повідомлення про збір даних і його подальша обробка повинні надаватися кожному кінцевому користувачеві до моменту (або в той час), коли пристрій починає збирати дані;

Значна частина пристроїв Інтернету Речей влаштовані так, що вони можуть тільки отримувати інформацію, а не надавати її. Через це виробники пристроїв не інформують користувачів про збір їх даних. Отже, користувачі не знають, хто саме обробляє дані, яким чином вони використовуються, які треті

сторони мають доступ до даних і як користувачі можуть здійснювати свої інформаційні права.

2. Надання згоди на збір та обробку даних (стаття 11) – у передбачених законом випадках, наприклад, використовуючи дані для рекламних цілей, постачальник пристроїв Інтернету Речей повинен спочатку отримати конкретну згоду від користувача;

Крім того, постачальники пристроїв не замислюються про отримання згоди на використання даних, що стосуються здоров'я (стаття 7). Однак згода на використання таких даних може бути основною і часто єдиною законною підставою для обробки даних, наприклад, через «фітнес-трекер».

3. Мінімізація (стаття 6) - хоча часто цього важко дотримуватися, власник пристрою / провайдер може збирати і обробляти тільки ті дані, які є необхідними для функціонування пристрою або задоволення інших законних цілей. Будь-який збір даних, який не є обґрунтованим законною ціллю, забороняється.

Як нещодавній приклад з міжнародної практики, принцип «мінімізації» публічно застосував Французький регуляторний орган із захисту даних – Commission nationale de l'informatique et des libertés (CNIL). 20 листопада 2017 року CNIL вислав офіційне попередження компанії, що використовує технологію розпізнавання мови в іграшках. Розумні іграшки були оснащені мікрофоном і динаміком і були підключені до мобільного додатку. Для розпізнавання мови дитини, іграшка направляла записи розмов на сервери в Китай, де вони оброблялися спеціальною програмою, без будь-яких гарантій безпеки. Такі великі обсяги збору даних в дитячій іграшці не відповідали принципу «мінімізації», особливо в зв'язці з відсутністю заходів безпеки. Не було ніякої необхідності відправляти дані в Китай для надання функціоналу іграшки. [4]

Один із перших штрафів за порушення Європейського Загального Регламенту із захисту даних (GDPR) також був накладений у зв'язку з принципом мінімізації даних при використанні відеоспостереження, що теж відноситься до сфери Інтернету Речей. Австрійський підприємець встановив перед своїм магазином камеру відеоспостереження - камера здійснювала зйомку значної частини тротуару. На жаль для підприємця, австрійський наглядовий орган порахував, що запис вулиці перед магазином є моніторингом громадської території. У поєднанні з відсутністю публічного повідомлення про зйомку вулиці за допомогою CCTV, таке використання камер не відповідає Австрійському закону про захист персональних даних, тому австрійський орган наклав штраф в розмірі 4800 євро за порушення принципу мінімізації

даних. Щоб відповідати вимогам захисту даних, компанія може збирати тільки мінімум інформації, необхідної для її цілей, у ясний та прозорий спосіб. [5]

4. Безпека та обмежений доступ до даних (стаття 24) - пристрої Інтернету Речей повинні бути захищені технічними заходами від стороннього доступу, такими як безпечне з'єднання, брандмауери і паролі. Доступ до зібраних даних повинен обмежуватися тільки тими співробітниками, які підтримують роботу пристрою.

Інтернет Речей не є винятком для зломів та отримання несанкціонованого доступу. Більше того, користувачі розцінюють розумний пристрій як звичайний домашній прилад, забуваючи про основні заходи комп'ютерної безпеки, тому ситуація погіршується. Те саме можна сказати і про виробників пристроїв Інтернет Речей - через обмежену функціональність вони зазвичай вирішують не дотримуватися відповідних для комп'ютерної індустрії стандартів безпеки.

Приклад ризиків слабких паролів за замовчуванням був представлений атакою Bricker Bot в 2017 році. Шкідлива програма Bricker Bot могла підключитися до будь-якого пристрою Інтернет Речей з ім'ям і паролем, поставленим заводом за замовчуванням (таку інформацію можна легко знайти через інтернет), і наносила настільки серйозну шкоду пристроям, що після цього була потрібна повна заміна обладнання. [6]

Ми не звикли до розуміння побутової техніки як об'єкту загрози для кібербезпеки. Постачальники Інтернету Речей зазвичай не додають у пристрої належні технічні та організаційні гарантії проти кіберзагроз та особливо порушень конфіденційності користувача. Більше того, навмисне чи ні, вони також порушують приватність користувачів постійним та часто таємним збором персональних даних.

Відповідно, персональні дані збираються без відома користувача, за замовчуванням, без гарантій їх безпеки. Така ситуація дозволяє володільцям даних використовувати зібрану інформацію у будь-який спосіб, що потребує адекватного реагування як зі сторони спільноти, так і зі сторони держави.

Список використаних джерел:

1. SB-327 Information privacy: connected devices. An act of September 28, 2018, to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy;
2. Postscapes URL:англ. версія / медіа-холдинг "Postscapes". – Текст. — <https://www.postscapes.com/iot-history/> (дата звернення: 13.11.2019). — Назва з екрана;
3. Про захист персональних даних. Закон України від 1 червня 2010р. [станом на 30.01.2018] // Відомості Верховної Ради. – 2010р. - №34. – ст.481;

4. Commission nationale de l'informatique et des libertés: англ. версія / французький регуляторний орган із захисту персональних даних "CNIL". — Текст. — URL:<https://www.cnil.fr/en/connected-toys-cnily-publicly-serves-formal-notice-cease-serious-breach-privacy-because-lack-security>(дата звернення: 13.11.2019). — Назва з екрана;

5. Fresh fields: англ. версія / медіа-холдинг "Fresh fields". — Текст. — URL: <http://digital.freshfields.com/post/102f39w/first-gdpr-fine-issued-by-austrian-data-protection-regulator> (дата звернення: 13.11.2019). — Назва з екрана;

6. ZDnet: англ. версія / медіа-холдинг "ZDnet". — Текст. — URL: <https://www.zdnet.com/article/homeland-security-warns-of-brickerbot-malware-that-destroys-unsecured-internet-connected-devices/> (дата звернення: 13.11.2019). — Назва з екрана.

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

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

СИСТЕМА ЗАГРОЗ ТА РИЗИКІВ КОНФІДЕНЦІЙНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ЗАСТОСУВАННІ ТЕХНОЛОГІЙ ІНТЕРНЕТ РЕЧЕЙ

Інтернет речей, без сумніву, - прогресивна технологія, що кардинально змінює людську життєдіяльність. Проте разом із тим, вона несе цілий ряд загроз та проблем, які необхідно визначити, попередити їх виникненню та запропонувати ефективні шляхи їх вирішення.

Проблема безпеки Інтернету речей стоїть на одному з перших місць і викликає цілком обґрунтовані побоювання. Вплив мережевих технологій, особливо тих, які втручаються в особистий і суспільний простір, від яких залежить життя і здоров'я людей, має бути не тільки пасивно безпечним, але й захисним. Неможливо допускати поширення технологій здатних викликати суттєвий негативний або навіть катастрофічний вплив на споживачів, або промислових систем, якщо вони належним чином не застраховані від ризиків, якщо не вжито всіх заходів з моніторингу їх безпечної роботи і не передбачені способи мінімізації та усунення наслідків несприятливих подій .

У технічно складних системах, особливо тих, які втягують безліч окремих пристроїв, алгоритмів та інформації, виключити виникнення ризикованих ситуацій не було і не буде можливим. Потрібне створення системи захисту від широкого спектра ризиків: технічних, методичних, інформаційних, кон'юктурних, ресурсних та багатьох інших.

Організація Open Web Application Security Project, яка активно займається вивченням питання IoT склала топ-10 уразливостей Інтернету речей:

1. Незахищений веб-інтерфейс.
2. Недостатній захист аутентифікації/авторизації (використання логінів та паролів за замовчуванням або використання «слабких «паролей», використання небезпечних механізмів відновлення пароля, тощо).
3. Незахищені мережеві служби (зловмисник використовує вразливі мережеві сервіси, аби може атакувати сам пристрій).
4. Відсутність цілісної перевірки транспортного шифрування (відсутність транспортного шифрування дозволяє проглянути «шлях подорожі» інформації в мережі Інтернет).
5. Конфіденційність (нелегальний збір персональних даних через певні мобільні додатки, хмарні інтерфейси).
6. Уразливий інтерфейс хмарних технологій (відсутність блокування після декількох некоректних спроб введення даних облікового запису, тощо).
7. Незахищений мобільний інтерфейс (в такому випадку дуже легко вгадати облікові дані користувача через недостатній ступінь захищеності).
8. Недостатня безпека конфігурацій (йде мова про те, що користувач пристрою має обмежені можливості або взагалі не має можливість управляти безпекою пристрою).
9. Незахищеність програмного забезпечення (неможливість оновлення ПЗ, яке дає змогу усунути дефекти самого ПЗ; небезпека полягає у можливості захоплення файлів оновлень).
10. Недостатня фізична безпека пристроїв (йде мова про використання USB-портів, SD-карт або інших форм зберігання інформації, коли зловмисник може розібрати пристрій та легко отримати доступ до середовища зберігання даних) [1].

Крім безліч технічних проблем існує не менш загрозливі фактори порушення конституційних прав та свобод людини в частині забезпечення безпеки та приватності при застосуванні технології Інтернет речей.

Так, Робоча група по захисту персональних даних, яка була заснована для реалізації Директиви 95/46/ЄС, у документі «Opinion 8/2014 on the on Recent Developments on the Internet of Things» визначила основні виклики приватності та захисту персональних даних, пов'язаних із IoT. До них відносяться:

1. Відсутність контролю та якості згоди користувача В результаті необхідності надання широко поширених послуг, користувачі можуть на практиці виявити, що їхні дані знаходяться під контролем у третіх сторін.

(наприклад, медичні дані користувача передаються до конкретного лікаря, і при виявленні певної хвороби передадуться іншому лікарю. В такому випадку пацієнт може втратити ланцюг передачі даних та контроль над ними).

2. Висновки, що здійснені на підставі персональних даних і перепрофілювання даних первісної обробки. Збільшення обсягу даних, генерованих IoT в комбінації з сучасними технологіями, пов'язане із аналізом таких даних та їх можливого перехресного зіставлення із іншими фактами. Вторинна обробка даних може призвести до того, що така оброблена інформація може служити для прийняття тих чи інших висновків певними суб'єктами (наприклад, інформація дасть змогу кредиторам прийняти рішення, надати кредит особі чи ні).

3. «Нав'язливе винесення моделей поведінки» і профілювання. Навіть якщо різні об'єкти будуть окремо збирати окремі частини інформації, достатня кількість зібраних даних і їх подальший аналіз може виявити конкретні аспекти життя та звичок індивіда. [2].

Підсумовуючи вищенаведене, приходимо до висновку, що систему загроз та ризиків конфіденційності персональних даних при застосуванні технологій Інтернет речей, становлять технічні, організаційні та правові проблеми.

Список використаних джерел:

1. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство / Т. І. Обуховська // Вісник Національної академії державного управління при Президентові України. - 2014. - № 1. - С. 95-103. - URL: http://nbuv.gov.ua/UJRN/Vnadu_2014_1_17.

2. А. Л. Петрицький Правове регулювання заходів припинення у сфері захисту персональних даних // Європейські перспективи. - 2014. - № 5. - С. 14-20.

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

*Коваль В., аспірант кафедри
адміністративного права і процесу
ДВНЗ «Київський економічний
університет імені Вадима Гетьмана»*

ПРАВОВІ УМОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ГОСПОДАРЮЮЧИХ СУБ'ЄКТАХ, ЯКІ ЗДІЙСНЮЮТЬ ГОСПОДАРСЬКУ ДІЯЛЬНІСТЬ В МЕРЕЖІ ІНТЕРНЕТ

Сучасне інформаційне суспільство характеризується не тільки стрімким зростанням обсягів інформації, що циркулює в ньому. Крім цього існує стійка тенденція до зростання ролі інформації в різних сферах діяльності, починаючи

від підприємницької і закінчуючи окремими сферами державного управління. Інформація все більше набуває статусу нового фактора виробництва, який нерідко і не без підстав називають «ною нафтою». Зокрема, володіння великими масивами інформації в сукупності з необхідними інструментами для її збору і обробки дозволяє створювати товари і послуги з високою часткою доданої вартості, а також приймати ефективні управлінські рішення.

Дослідження, проведені Масачусетським технологічним університетом показали, що організації, які використовують у своїй діяльності автоматизовані механізми прийняття рішень, засновані на аналізі даних, збільшували свою продуктивність в середньому на 5-6%. Експерти відзначають, що «збір, інтеграція і аналіз даних більше не вважаються витратами на ведення бізнесу; дані - це ключ до досягнення ефективності і прибутковості бізнесу. В результаті швидко розвивається індустрія, що підтримує аналіз даних» [6].

У свою чергу Р. Жаринов зазначає, що питання обробки персональних даних є особливо актуальними в світлі зростаючого числа персональних даних, які збираються через мережу Інтернет. Це пов'язано в тому числі з ростом ринку електронної комерції, а також з прагненням більшості компаній забезпечити присутність в мережі Інтернет. Використання Інтернету для комунікації зі споживачами, як правило, має на увазі отримання їх персональних даних для цілей організації доставки товарів або надання послуг, поширення таргетированной реклами (тобто повідомлень, що демонструються строго визначеної вибірці користувачів), публікації відгуків і так далі [3, с.188].

Очевидно, що такі санкції за порушення законодавства, як блокування інтернет-сайтів, створюють серйозні ризики для організації, що активно використовують Інтернет в повсякденній господарській діяльності.

В.М. Брижко звертає увагу на те що, необхідність забезпечення безпеки персональних даних в наш час - об'єктивна реальність. Сучасна людина не може самотійно протидіяти посяганню на його приватне життя. Зрослі технічні можливості щодо збору та обробки персональної інформації, розвиток засобів електронної комерції і соціальних мереж роблять необхідним вжиття заходів щодо захисту персональних даних. Крадіжка персональних даних може завдати правовласнику відчутної матеріальної шкоди [2, с.7].

Важко не погодитися з автором, оскільки, зловмисники, які володіють достатніми технічними знаннями, викрадають реквізити банківських карт (скімінг, тобто мається на увазі шахрайство за допомогою зчитування інформації злочинцями з магнітної стрічки картки користувача) або імітують сайти фінансових установ, щоб змусити користувача показати свою особисту

інформацію (фішинг, тобто виманювання в користувачів інтернет-магазину персональних даних з метою подальшого шахрайства над даним користувачем).

Так, в країні існують, можливо, мільйони баз даних, в яких накопичується інформація про громадян. У багатьох випадках громадяни ніяк не захищені. На сьогоднішній день в Україні прийнятий тільки один закон про захист персональних даних, прийняття якого, на жаль, обумовлене швидше бажанням вступити в Європейський Союз, ніж бажанням захистити своїх громадян від несанкціонованого доступу до їх особистих даних. Закон України «Про захист персональних даних». Він регулює відносини, пов'язані із захистом персональних даних при їх обробці [5]. Закон містить цілком пристойно написані і зрозумілі базові положення, яке в багатьох аспектах схожі з Конвенцією Ради Європи.

В.П. Іванський визначає, що законодавчі акти багато в чому схожі між собою і переслідують єдину мету - забезпечити максимальний захист і юридичну підтримку громадян при вирішенні питань захисту своїх персональних даних в сучасних умовах різкого зростання обчислювальних можливостей, виникнення і зростання кібертероризму, появи нових загроз і атак на персональні дані користувачів локальних і глобальних мереж [4, с.45].

Деякі зарубіжні автори зазначають, що на сьогоднішній день інтерес до розвитку законів про захист персональних даних проявляють не тільки Європа і США, а також і Україна. У країнах Європи і США дуже стурбовані проблемою захисту персональних даних.

Так, Ю. Трифонова зауважує, що іншими словами, внутрішні заходи щодо захисту розробляються індивідуально кожним власником баз персональних даних з урахуванням специфіки цих даних, роботи з ними, а також їх важливості. Найчастіше такі внутрішні заходи є комерційною таємницею і не підлягають поширенню. До внутрішніх заходів відносять: введення внутрішніх керівних вказівок або принципів; прийняття Кодексів практики або поведінки; установа якоїсь посади спеціального відповідального [3, с.189].

Так, для реалізації спільних організаційних заходів щодо захисту персональних даних користувачів мережі Інтернет законодавчою базою України визначено, що забезпечення безпеки персональних даних при їх обробці в інформаційних системах персональних даних має передбачати: оцінку обстановки; обґрунтування вимог щодо забезпечення безпеки персональних даних і формулювання завдань їх захисту; розробку плану забезпечення безпеки персональних даних; вибір доцільних способів (заходів і засобів) захисту персональних даних відповідно до завдань і задумом захисту;

вирішення питань управління забезпеченням безпеки персональних даних в динаміці зміни обстановки і контролю ефективності захисту; забезпечення реалізації прийнятого задуму захисту; планування заходів щодо захисту персональних даних; безпеки персональних баз даних, тобто такі як організаційні, технічні і правові; організацію і проведення робіт зі створення системи захисту персональних даних в рамках розробки (модернізації) інформаційних систем персональних даних, розробка та розгортання засобів захисту персональних даних або її елементів в інформаційних системах персональних даних, вирішення основних завдань взаємодії, визначення їх завдань і функцій на різних стадіях створення і експлуатації інформаційних систем [5].

Дехто з вітчизняних авторів вважають, що в Україні на сьогоднішній день, на жаль, захист персональних даних організований на достатньо низькому рівні, на «розсуд і компетентність» системних адміністраторів або технічних директорів компаній.

Звичайно, технічні засоби захисту персональних даних є важливою складовою при захист персональних даних. Існує три основних види технічних засобів захисту даних, реалізованих апаратно, програмно і апаратно-програмно. До апаратних засобів відносять комплекси електронних, електричних і механічних пристроїв, які забезпечують захист персональних даних на апаратному (фізичному) рівні.

Програмні методи захисту - це сукупність алгоритмів і програм, що забезпечують розмежування доступу і виключення несанкціонованого використання інформації. Найчастіше програмні засоби використовуються для захисту великих баз персональних даних і систем обробки. Апаратно-програмними засобами є пристрої, що представляють комплексний захист даних і виключають можливість злому програмного коду (неліцензійного використання) програмного продукту [1, с.139].

Отже, проаналізовані питання не можна вирішити, не відповівши спочатку на головне питання: чи є персональні дані товаром або вони є невідчужуваним немайновим благом? На користь кожного із трактувань можна привести безліч аргументів. Однак одним з найбільш значущих є те, що більша частина успішних бізнес-моделей суб'єктів господарювання, які ведуть свою діяльність в мережі Інтернет заснована на використанні персональних даних як «валюти», якій користувач розплачується за можливість використання відповідного сервісу.

Саме дані користувачів є одним джерелом багатомільярдних доходів соціальних мереж, пошукових сервісів та інших ІТ-компаній.

Список використаних джерел:

1. Абаєв Ф.А. Історико-правові передумови формування і сучасні тенденції розвитку інституту персональних даних в трудовому праві // Юридичний журнал. - 2013. № 5. С. 139.
2. Брижко В. М. Захист персональних даних в умовах розвитку інформаційного суспільства // Винахідник України. - 2011. -№ -С. 7-19.
3. Жаринов Р., Трифонова Ю. Можливості знеособлення персональних даних в системах, що використовують реляційні бази даних // Управління, обчислювальна техніка та інформатика. № 2 (32), 2014. С. 188-194.
4. Іванський В.П. Персональні дані як основний об'єкт посягань на недоторканність сфери приватного життя: законодавчий досвід у зарубіжних державах // Адміністративне право і процес. - 2012. - № 8.
5. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст.481.
6. Brynjolfsson E. et al. Strength in Numbers: How Does Data-Driven Decision -Making Affect Firm Performance? (April 22, 2011). Available at SSRN: <http://ssrn.com/abstract=1819486>

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

*Некіт К., к.ю.н., доцент, доцент
кафедри цивільного права Національного
університету «Одеська юридична
академія»*

ПЕРСОНАЛЬНІ ДАНІ ЯК ВАЛЮТА: ТРАНСФОРМАЦІЇ ЦИФРОВОЇ ДОБИ

Наявність цінності персональних даних визнана вже давно і беззаперечно. Їх називають «нафтою», «новим золотом», «валютою ХХІ сторіччя». Вже давно ні для кого не секрет, що численні компанії використовують персональні дані користувачів для ведення бізнесу. Настав вже час, коли дедалі більше користувачів починають розуміти цінність своїх персональних даних. Така ситуація збуджує все більше дискусій навколо правового режиму персональних даних. Все частіше висловлюються пропозиції розглядати персональні дані як товар, поширити на них правовий режим власності, надати нарешті не лише компаніям, але й користувачам отримувати користь від своїх персональних даних. Однак стійке розуміння «невідчужуваності» природи персональних даних, наявність «чутливих» персональних даних та багато інших питань, що залишаються невирішеними у цій сфері, змушують науковців (не кажучи вже про законодавця) обережно ставитись до визначення їх правового режиму.

Наприклад, Томас Дж. Фаркас, аналізуючи правову природу прав на дані, отримані в сфері Інтернету речей, коливається у виборі норм, які мають бути тут застосовані. Він аналізує такі дані крізь призму теорій авторського права, положень про захист баз даних, ноу-хау та комерційної таємниці, положень законів про захист персональних даних, але в жодних нормативних актах не знаходить положень, які б повною мірою могли б застосовуватись до них. Більшою мірою він схиляється до поширення положень про право власності на такі дані, але убаचाє тут проблеми при визначенні, кому саме мають належати дані, отримані у сфері Інтернету речей, а також як забезпечити належний баланс між інтересами окремих індивідів та правом інших осіб на інформацію[1].

Зазначимо, що питання про можливість поширення на персональні дані правового режиму власності дискутується вже досить давно. Так, О.А. Баранов, В.М. Брижко та Ю.К. Базанов у своєму дослідженні «Права людини та захист персональних даних» майже десятиріччя тому підіймали питання про те, що персональні дані можуть розглядатися як товар та виступати об'єктом права власності. Як зазначають дослідники, економічний аспект персональних даних виражається в тому, що зі ставленням та функціонуванням внутрішнього ринку, який передбачає рух товарів, послуг та капіталів, виникає необхідність і в русі персональних даних, дієвому забезпеченні захисту їх споживчої та мінової вартості [2, с. 168].

Прийняття нових нормативних актів актуалізують проблеми визначення правової природи персональних даних. Наприклад, після прийняття GDPR[3] з визначенням у цьому акті деяких повноважень володільців персональних даних, зокрема, можливості отримувати копії своїх даних, передавати дані від одного контролера до іншого, вимагати їх знищення тощо (ст. ст. 17, 20, 26 GDPR), деякі дослідники висловлювались на користь того, що персональні дані можна визнавати різновидом власності [4]. Мотивували вони свої міркування тим, що вказані повноваження аналогічні повноваженням власника з користування, розпорядження, отримання доходів від належного їм нематеріального блага [5]. Так, відповідно до ст. 17 GDPR, суб'єкт даних повинен мати «право на забуття», тобто вимагати стирання (знищення) своїх даних, яке має бути здійснено без будь-яких безпідставних затримок, що розглядається як аналогія правомочності власника на розпорядження. Відповідно до ст. 20 GDPR, суб'єкт даних має право на мобільність даних, тобто можливість в будь-який момент отримати передані ним контролеру персональні дані в структурованому та такому, що легко зчитується машиною форматі, і передати їх іншому контролеру без жодних перепон з боку

попереднього контролера. У цьому углядається паралель з правомочностями власника на володіння та користування своїм майном.

Інші дослідники піддавали критиці можливість розглядати персональні дані як різновид власності. Наприклад, Л. Маурел зазначав, що деякі повноваження, що надаються користувачам в рамках GDPR помилково прирівнюються до форми приватної власності. Цей термін не використовується у Регламенті, а дані в ньому захищаються як атрибут особи, а не різновид майна.

Формулювання GDPR, на думку дослідника, дійсно породжують питання про можливість продажу персональних даних третій особі і про те, чи можна вважати такі правочини дійсними. Наприклад, ситуація, коли людина хоче продати свої особисті дані третій особі, є можливою на підставі ст. 6 GDPR, згідно якій «обробка законна лише в тому випадку, якщо суб'єкт погодився на обробку своїх персональних даних», відповідно, зацікавлений у такій обробці суб'єкт може бути готовим сплачувати кошти за надання згоди на обробку. Однак у зазначеній статті вказано, що згода дається «для однієї або кількох певних цілей». Отже, на відміну від продажу товару, що припускає реальну передачу права власності, компанія, яка збирає персональні дані, буде зобов'язана вказувати цілі, з якими вони передаються. Таким чином, на думку автора, така ситуація вже скоріше нагадує не купівлю-продаж, а надання певної ліцензії, схожої з наданням дозволу у питаннях, пов'язаних із авторськими правами, але таке порівняння теж не зовсім актуальне, оскільки цесія прав третій особі є неможливою з точки зору особистих даних [6].

На користь того, що персональні дані не можуть розглядатись як товар говорить і позиція, відображена у Керівництві 2/2019 щодо обробки персональних даних відповідно до ст. 6(1)(б) GDPR в контексті надання онлайн послуг суб'єктам даних. Так, у п. 54 вказаного Керівництва зазначено, що з урахуванням того, що захист даних є фундаментальним правом, і приймаючи до уваги, що одна з головних цілей GDPR є забезпечення можливості для суб'єктів даних контролю інформації, що їх стосується, персональні дані не можуть вважатися товаром. Навіть якщо суб'єкт даних може погодитись на обробку персональних даних, вони не можуть відчужувати свої фундаментальні права за такими угодами [7].

Здавалося б, позиція нормотворців є однозначною – персональні дані є невідчужуваними за своєю природою, являються атрибутом особи, а тому не можуть розглядатись як товар чи об'єкт права власності.

Однак революційною у розумінні правової природи персональних даних може стати нещодавно прийнята Директива (ЄС) 2019/770 Європейського парламенту і Ради від 20 травня 2019 р. про певні аспекти стосовно договорів

поставки цифрового контенту та надання цифрових послуг (далі – Директива). Ця Директива спрямована на посилення захисту споживачів в он-лайн середовищі і вносить зміни у законодавство ЄС про захист прав споживачів в рамках єдиного цифрового ринку та пакетів «Новий курс для споживачів». Директива охоплює договори між трейдерами та користувачами, у яких трейдер поставляє чи зобов'язується поставити цифровий контент або цифрову послугу в обмін на оплату ціни (яка визначається у Директиві як гроші чи цифрове вираження вартості – електронні купони, ваучери, криптовалюти) або надання персональних даних [8].

Відповідно до п. 24 Директиви, цифровий контент або цифрові послуги часто надаються також там, де споживач не сплачує ціну, а надає персональні дані трейдеру. Такі бізнес-моделі використовуються у різних формах на значній частині ринку. Визнаючи, що захист персональних даних є фундаментальним правом і тому персональні дані не можуть розглядатись як товар, Директива спрямована забезпечити споживачам в контексті таких бізнес-моделей право на договірні засоби правового захисту. Таким чином, Директива має застосовуватися до контрактів, у яких трейдери постачають чи зобов'язуються поставити цифровий контент чи цифрову послугу споживачу, а споживач надає або зобов'язується надати персональні дані. Персональні дані можуть бути надані трейдеру або під час укладення договору, або пізніше, наприклад, коли споживач дає згоду на використання трейдером будь-яких персональних даних, які споживач може завантажити або створити з використанням цифрового контенту або цифрового сервісу. Ця Директива повинна застосовуватися до будь-якого контракту, в якому споживач надає або зобов'язується надавати особисті дані трейдеру. Наприклад, ця Директива повинна застосовуватися в тих випадках, коли споживач відкриває обліковий запис в соціальній мережі і надає ім'я та адресу електронної пошти, які використовуються не тільки для надання цифрового контенту або цифрових послуг, або для виконання вимог законодавства. Вона також повинна застосовуватися в тих випадках, коли споживач дає згоду трейдеру на обробку в маркетингових цілях будь-яких матеріалів, що становлять особисті дані, таких як фотографії або публікації, які завантажує споживач [9].

Таким чином, Директива фактично визнає персональні дані «валютою» в цифровому світі. Поширення сфери дії Директиви на договори, за якими споживач «платить» своїми персональними даними є революційною для законодавства про захист прав споживачів та надає захист споживачам у сфері контрактів, які раніше вважалися «безоплатними». Метою розробки концепту «контракту на поставку цифрового контенту та цифрових послуг, за які споживач надає персональні дані замість сплату грошей» було

поширення принципів захисту споживачів на так звані «безкоштовні сервіси». В обґрунтуванні такої позиції було вказано, що деякі сервіси не можуть вважатися «безкоштовними» з урахуванням зростаючої економічної цінності персональних даних. Несправедливим є той факт, що у випадках, коли споживачі не сплачують гроші, але все ж таки надають свої персональні дані за користування послугами, вони не отримують належного захисту своїх прав, оскільки така ситуація не підпадає під вимоги законодавства ЄС щодо захисту прав споживачів. Тому запропоновано було поширити захист положення про захист прав споживачів на випадки, коли останні отримують сервіс за надання персональних даних, оскільки це відповідає сучасним економічним реаліям та потребам [10].

В контексті Директиви цифровий контент означає дані, які виробляються і надаються в цифровій формі, незалежно від того, чи використовується матеріальний носій чи ні, наприклад, комп'ютерні програми, додатки, відео- і аудіофайли та електронні книги. Цифрові послуги - це послуги, які: (1) дозволяють створювати, обробляти, отримувати доступ або зберігати дані; або (2) дозволяють ділитися чи іншим чином взаємодіяти з даними в цифровій формі, які завантажені або створені споживачем чи іншими користувачами цих послуг. Прикладами можуть бути платформи для обміну відео і аудіо, послуги хмарних обчислень і соціальні мережі [8].

Фактично наведена Директива визнає можливість обміну персональних даних на цифровий контент та цифрові послуги. Якщо ж за певним явищем визнається цінність та можливість обміну на інші блага (мінова цінність), це є нічим іншим, як введенням цього явища у цивільний обіг. Видається, що положення, передбачені Директивою, є першим кроком на шляху перегляду концепції персональних даних та, можливо, навіть поширення на них правового режиму власності.

Список використаних джерел:

1. Thomas J. Farcas. Data created by the Internet of Things: the new gold without ownership? // Revista la proprietad in material. – 2017. - № 23. – P. 5-17.
2. Баранов А.А., Брыжко В.М., Базанов Ю.К. Права человека и защита персональных данных. – Киев: Государственный комитет связи и информатизации Украины, 2000. – 280 с.
3. Некіт К.Г. Значення GDPR (General Data Protection Regulation) для забезпечення захисту персональних даних у сфері Інтернету речей (IoT) // Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції : матеріали Міжнародної науково-практичної конференції (м. Одеса, 18 травня 2018 р.) У 2-х т. Т. 2 / відп. ред. Г.О. Ульянова. – Одеса : Видавничий дім «Гельветика», 2018. – с. 491-493.

4. Некит Е.Г. Право собственности на персональные данные в контексте GDPR: миф или реальность. URL: <https://blog.liga.net/user/%D0%B5nekit/article/31189>

5. My data are mine. Why we should have ownership rights on our personal data: report. URL: <https://www.generationlibre.eu/wp-content/uploads/2018/01/Rapport-Data-2018-EN-v2.pdf>

6. Le RGPD interdit-il aux individus de «vendre» leurs données personnelles? URL: <https://scinfolex.com/2018/05/12/le-rgpd-interdit-il-aux-individus-de-vendre-leurs-donnees-personnelles/>

7. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. October 8, 2019. URL: https://edpb.europa.eu/sites/edpb/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

8. Consumers to be better protected when concluding online contracts Consumers to be better protected when concluding online contracts. URL: <https://www.altius.com/blog/474/consumers-to-be-better-protected-when-concluding-online-contracts>

9. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0770>

10. EDPS Opinion 8/2018 on the legislative package “A New Deal for Consumers”. October 5, 2018. URL: https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf

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

*Скаржинський В. В., магістрант ФСП
КПІ ім. Ігоря Сікорського*

*Науковий керівник: Дубняк М. В.,
к.ю.н., ст. викладач кафедри ІППІВ КПІ
ім. Ігоря Сікорського*

СПЕЦИФІКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ

Україна знаходиться на шляху побудови демократичного суспільства, де головною цінністю є людина. В останні роки людину неможливо розглядати у відриві від інформаційного суспільства, оскільки розвиток інформаційно-комунікаційних технологій, інтернет-мережі поставив на перше місце інформаційні відносини. У зв'язку з цим держава на даному шляху зіткнулася з низкою проблем, які потребують свого негайного вирішення. Серед цих проблем виділяється забезпечення захисту сфери приватного життя громадянина, особливо такої його важливої похідної як «персональні дані» в контексті розвитку технологій, пов'язаних з інтернетом речей.

Спочатку зауважимо, що в науковій літературі під інтернетом речей

найчастіше розуміється комплекси та системи, які складаються з різноманітних технічних чи обчислювальних ресурсів та пристроїв, локального та / або розподіленого характеру програмного забезпечення, технологій хмарних обчислювань, передача даних між якими здійснюється через мережу Інтернет, які призначені для надання послуг та проведення робіт в інтересах відповідних суб'єктів [Error! Reference source not found., с. 7]. Функціонування та активне розповсюдження таких пристроїв, програмного забезпечення та технологій змушує по-новому поглянути на персональні дані та їх захист.

Виокремлення категорії «персональні дані» з більш загальної категорії «приватне життя», перш за все, пов'язано з поширенням автоматизованих систем обробки та зберігання інформації, в першу чергу, комп'ютерних баз даних, до яких можливий віддалений доступ через технічні канали зв'язку. Саме ці системи, по суті, спричинили революцію в питаннях структурування, зберігання і пошуку необхідних даних, створили передумови для виникнення проблеми захисту персональних даних. Подальший розвиток технологій інтернету-речей, який є пріоритетним напрямом розвитку в багатьох країнах, може призвести до потенційних витоків персональних даних через мережу інтернет.

Розвиток цієї проблеми викликає природну необхідність в забезпеченні надійного захисту персональних даних і процесів, впорядкування суспільних відносин в сфері технології інтернет-речей. В Україні тривають процес розробки та впровадження комплексного підходу до забезпечення захисту персональних даних. У зв'язку з цим особливо важливо, щоб підхід, який при цьому буде вироблений, охоплював весь спектр проблем, а не зводився до розгляду лише їх технічної складової. Правове регулювання захисту персональних даних має бути системним, а не лише охоплювати вирішення точкових, ситуаційних проблем. Аналіз практики правозастосування нормативно-правових актів в сфері захисту персональних даних свідчить про неврегульованість деяких питань у сфері захисту персональних даних та потребу в удосконаленні законодавства.

У переважній більшості наукових робіт питання, які в тій чи іншій мірі розкривають зміст персональних даних, сутність і нормативно-правове регулювання їх захисту, до теперішнього часу розглядалися у відриві від розвитку інтернет-речей. Відповідно необхідно з'ясувати особливості захисту персональних даних в умовах активного формування відносин у зв'язку з розвитком технологій інтернету-речей. Адже, як правильно зауважує Ю. Є. Петрухно, інформаційне суспільство стало якісно новим етапом розвитку людства, в якому будь-хто за допомогою інформаційно-

комунікаційних технологій може отримувати, переробляти, розповсюджувати інформацію, а держава забезпечує високий рівень інформатизації всіх галузей [Error! Reference source not found., с. 129]. В контексті розвитку технологій інтернет речей таке трактування може свідчити про отримання нових можливостей для зловмисників щодо отримання персональних даних через канали зв'язку, які використовуються в процесі реалізації функцій інтернету речей, прогалин у захисті відповідних пристроїв, програмного забезпечення чи технологій.

Специфіка суспільства у якому активно використовується технологія інтернету-речей характеризується виникненням технології автоматизованих баз даних, впровадженням в побут технологій розумних будинків; засобів безконтактної ідентифікації за біометричними даними (за сканом сітківки ока, узору судин на долоні, за голосовими параметрами) з метою активізації комп'ютера, мобільного телефону, ввімкнення автомобіля, роботи «розумного» будинку тощо); засобів оплати товарів у супермаркеті не тільки за допомогою сканування відбитків пальців, а й піднесення телефону з великою кількістю персональних даних та доступів у ньому [Error! Reference source not found., с. 22]. В результаті цього відбувається зміна свідомості – технології інтернет-речей використовується для обміну даними, як елемент спілкування, навчання, туризму, довідковий ресурс, організаційний ресурс, засіб контролю та розвитку, прийняття рішень. В свою чергу, це призводить до необхідності посилення захисту персональних даних в умовах розвитку технологій інтернету-речей, оскільки сучасні технології дозволяють з великою швидкістю передавати дані по всьому світу, при цьому зникає природний бар'єр особистого простору фізичної особи. Як правильно зауважує О.А. Баранов та В.М. Брижко «технології інтернет речей значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркулювання і використання великого, просто величезного територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину» [Error! Reference source not found., с. 87].

В сучасних умовах в Україні та усьому світі постійно реєструється низка порушень, які стосуються персональних даних. Переважна більшість їх включають наступні випадки: невиконання вимог щодо повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних; недодержання вимог щодо отримання від працівників зобов'язань не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків,

недотримання вимог щодо визначення відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці; недодержання обов'язку володільця персональних даних повідомити Уповноваженого про створення структурного підрозділу або призначення відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці; неналежне ведення обліку операцій, пов'язаних з обробкою персональних даних та доступом до них; невідповідність внутрішніх положень та документів володільця персональних даних вимогам чинного законодавства про захист персональних даних; недотримання принципу строкowości обробки персональних даних; відсутність зобов'язання про нерозголошення персональних даних працівниками, які мають доступ до персональних даних; відсутність плану дій на випадок несанкціонованого доступу до персональних даних пошкодження технічного обладнання, виникнення надзвичайних ситуацій [**Error! Reference source not found.**, с. 106]. Проте окремої уваги в останні роки набувають порушення права на персональні дані в сфері саме інтернет речей, що пов'язано з активним розширенням переліку персональних даних, збору їх у великі масиви, підвищення ризиків передачі цих даних пристроями до агенцій, які займаються таргетованою рекламою, зростання ризиків кібератак.

З метою забезпечення захисту прав та свобод людини і громадянина при обробці його персональних даних в Україні було прийнято Закон України «Про захист персональних даних». Водночас закон був прийнятий на фоні прогалин в захищеності персональної інформації та постійних публічних витоків персонофікованих баз даних, що порушує конституційні права громадян та несе шкоду діловій репутації організацій, які володіють такою інформацією. З моменту прийняття його постійно удосконалюють – на поточний момент до його тексту більше 10 разів вносилися зміни.

Специфіка захисту персональних даних передбачає два ключових елемента:

- зобов'язання визначене в ст. 24 Закону України «Про захист персональних даних» володільця вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних;

- зобов'язання визначене в ст. 10 Закону України «Про захист персональних даних» кожного працівника володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків [**Error! Reference source not found.**].

Однак такий підхід недостатньо враховує ризики обробки персональних даних, які виникнуть при активному розвитку технологій інтернету речей, а

значить і специфіку захисту персональних даних в результаті його функціонування.

Таким чином, поява та розвиток технологій інтернету речей спричиняє потребу в зміні підходів до системи захисту персональних даних. У зв'язку з цим розширюється коло персональних даних, збільшується кількість порушень прав суб'єктів персональних даних, змінюються вимоги до захисту таких даних. На сьогодні в Україні законодавчо визначено поняття персональних даних, встановлено коло суб'єктів даних та окреслено їх права, власників та розпорядників, мету та процедури обробки персональних даних, принципи захисту персональних даних та механізм контролю за дотриманням такого законодавства щодо захисту персональних даних. Але все це недостатньо враховує специфіку використання персональних даних під час застосування технологій інтернету речей. Тому на сьогодні існує необхідність створення багаторівневої і багатооб'єктної системи захисту персональних даних, що потребує удосконалення системи правового регулювання, у цій частині.

Список використаних джерел:

1. Конституція України : Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. // ВВР України. – 1996. – № 30. – Ст. 141.
2. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI // ВВР України. – 2010. – № 34. – Ст. 481.
3. Баранов О. А. Огляд правових проблем Інтернету речей / О.А. Баранов // Інтернет речей: проблеми правового регулювання та впровадження: Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. – С. 7-15.
4. Баранов О.А. Захист персональних даних в сфері інтернет речей / О.А. Баранов, В.М. Брижко // інформація і право. – 2016. – №2. – С. 85-91.
5. Гронь О.В. Проблеми захисту персональних даних у контексті сучасної комунікації / Р.В. Гронь // Науковий вісник Ужгородського національного університету. – 2018. – №19. – С. 102-108.
6. Кучерявый А.Е. Интернет вещей / А.Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21-24.
7. Петрухно Ю.Є. Інформаційне суспільство: поняття, основні складові, характеристика / Ю.Є. Петрухно // Вісник ОНУ. – 2014. – Т. 19. – Вип. 1. С. 127-133.

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

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КОНТЕКСТІ ІНТЕРНЕТ РЕЧЕЙ

Нині інформаційні технології пронизують собою всі сфери суспільного життя. І відповідно з переходом людства до нової епохи почався стрімкий прогрес технологій. Завдяки цьому, зросла цінність на електронні ресурси і почала відігравати важливу роль для суспільства.

Поняття «Інтернет речей» був введений Кевіном Ештоном у 1999 році, щоб проілюструвати можливості радіочастотної ідентифікації (RFID), яка використовується в корпоративних системах поставок, щоб порахувати і відстежити товари без людського втручання [1]. Ми погоджуємося з думкою Ожевана М.А., що важко визнати поняття Ештона вдалим, оскільки в ньому від самого початку закладена опозиція «людина-річ», а це неодмінно провокує на роздуми щодо загроз і викликів перетворення людей на «речі» або «речей» на людей чи, принаймні щось людиноподібне [2].

На думку Баранова О.А. під «Інтернетом речей» варто розуміти комплекси і системи, що складаються з сенсорів, мікропроцесорів, виконавчих пристроїв, локальних та / або розподілених обчислювальних ресурсів і програмних засобів, програм штучного інтелекту, технологій хмарних обчислювань, передача даних між якими здійснюється за допомогою мережі Інтернет, та які призначені для надання послуг і проведення робіт в інтересах суб'єктів (юридичних або фізичних осіб) [3].

Отже, слід розуміти Інтернет речей, як систему, що об'єднує матеріальні речі (фізичні) за допомогою мережі Інтернет завдяки чому Інтернет речей може глобально вплинути на розвиток суспільства знань та дозволить численним процесам відбуватися без участі людини.

Лідерами у розробці та впровадженні Інтернету речей є країни, в яких розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів — США, Китай, Південна Корея, крім того, значний прогрес у цій галузі демонструють європейські країни та Японія.

З 2008 р. відбувся перехід від «Інтернету людей» до «Інтернету речей». Кількість підключених до мережі «речей» перевищила кількість людей. З того часу інтерес на концепцію «Інтернету речей» не спадає, а навпаки зростає. Застосування технологій т Інтернету речей призводить до фундаментальних змін в нашому суспільстві [4].

Поширеними є низка технологій Інтернет речей: «розумний будинок», Інтернет речей для медицини, «розумне місто», Інтернет речей для транспорту, Інтернет речей для держави тощо. Звісно технології Інтернет речей можуть покращити наше повсякденне життя, але вони також представляють безліч нових проблем з конфіденційністю.

У наш час багато пристроїв вже мають датчики, що дозволяють збирати інформацію про фізичний світ і людину – камери, гіроскопи, акселерометри, термометри, пристрої розпізнавання мови та ін. Активне використання різних гаджетів, що забезпечують інформаційну взаємодію, призводить до того, що за допомогою Інтернет-технологій можна стежити практично за кожним куточком і за кожною подією у світі, збирати різні персональні дані [5]. Описано випадок, коли в Нідерландах було відхилено проект зі створення інтелектуальних електромереж на основі «розумних» лічильників спожитої електроенергії в квартирах і будинках. Відхилений на підставі підозри про те, що збір кожні 7 секунд інформації про рівень споживання електроенергії, зберігання такої інформації і її подальший аналіз може привести до розкриття в деталях способу життя споживачів електроенергії та до можливого її незаконного використання зловмисниками[5].

Слід погодитися із думкою В.Пилипчука, що технології Інтернет речей значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркуляцію і використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання цих даних і правового забезпечення їх захисту від несанкціонованого використання [6].

Нині технології Інтернет речей впроваджені у традиційні закриті та обмежені для розголосу інформаційні простори, тобто у наше приватне життя. Поступово зростаючи, за кількістю датчиків, будуть ще більше збирати даних про людину, тому широке застосування технологій Інтернет речей робить актуальним питання **контролю, узгодження та прозорості** щодо розмежування між приватним й суспільними сферами. Це обумовлено насамперед тим, що пристрої Інтернет речей генерують та збирають безліч персональних даних, отже, управління є серйозним *юридичним питанням*.

Право власності на персональні дані є основною проблемою, що обертається навколо управління та контролю даних, таких як *конфіденційність, довіра, безпека*, а також важливі наслідки для майбутнього "цифрової" економіки та торгівлі даними.

Відповідно до ст.3 Конституції України людина, її життя і здоров'я, честь і гідність, **недоторканність і безпека** визнаються в Україні **найвищою**

соціальною цінністю. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави. Як вбачається із ст.32 Конституції України «ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. **Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди**, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Забезпечення конструкційних гарантій потребує створення ефективних державно-правових механізмів захисту задекларованих конституцією прав людини, насамперед, у сфері обігу персональних даних.

Враховуючи те, що захист персональних даних в умовах застосування технології Інтернет речей є юридичною проблемою, то вона має привернути увагу як науковців, експертів, так і громадськості до обговорення.

У такій дискусії бажано розглянути наступні питання:

- *не відстати від технологій.* Врахувати пропозиції науковців та експертів щодо *конфіденційності та захисту персональних даних*, а також обговорити можливі зміни до Закону України «Про захист персональних даних», а саме: передбачити загрози сфері технологій, які вимагають захисту конфіденційності. Цей Закон повинен розкрити природу даних датчиків і забезпечити захист конфіденційності;

- *забезпечення безпеки.* Це ключовий момент, який підтримує довіру до Інтернет речей та взаємодії із суспільством. Більшість пристроїв Інтернет речей уразливі ззовні. Варто замислитися і про національну безпеку держави, адже зловмисники теж можуть скористатися можливістю технологій Інтернет речей та викликати негативні наслідки (наприклад, руйнування дамб, мостів та елементів електромережі). Отже питання безпеки завжди є актуальним;

- *на жаль, Інтернет речей розмиває поняття приватного та публічного права* (наприклад, особа, яка знаходиться в чужому будинку немає уявлення, що її голос, зображення або дії фіксуються на датчик та передаються третім особам);

- *прозорість.* Інформація, яка надається для споживачів повинна підвищити прозорість і контроль, необхідно будувати чіткі, точні, актуальні моделі з деталізацією.

Список використаної літератури:

1. HowlingPixel. Інтернет речей / HowlingPixel // Інтернет речей URL: https://howlingpixel.com/i-uk/Інтернет_речей

2. ОжеванМ.А. Технофіліяvs. технофобія: розвиток цивілізації як розв'язання суперечностей між новітніми технологіями та культурними

традиціями Інтернет речей: проблеми правового регулювання та впровадження: Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : НТУУ «КПІ ім. Ігоря Сікорського» Вид-во «Політехніка». 2017. – 238 с.

3. Баранов О. А. ІНТЕРНЕТ РЕЧЕЙ (IoT): ОГЛЯД ПРАВОВИХ ПРОБЛЕМ Інтернет речей: проблеми правового регулювання та впровадження: Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : НТУУ «КПІ ім. Ігоря Сікорського» Вид-во «Політехніка». 2017. – 238 с.

4. Овідіу Вермесан, Маркус Ейзенхауер, Харальд Сандмакер, Патрік Гіймен, Мартін Серрано, Еліас Трагос, Хав'єр Валіно. Інтернет речей когнітивної трансформації «Тенденції дослідження технологій та програми» [Електронний ресурс] / Вермесан О., Ейзенхауер М., Сандмакер Х., Гіймен П., Серрано М., Трагос Е., Валіно Х. // Інтернет речей когнітивної трансформації «Тенденції дослідження технологій та програми». URL: <https://docs.google.com/document/d/1VgqUvgSQmfFsrAWG7HOtlqnATHbaoufl1ZXzGhUmNw/edit>

5. Брижко В.М. Інтернет вещей : чему угрожает будущее. – URL : <http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee>

6. Пилипчук В.Г. Становлення і регулювання суспільних відносин у сфері новітніх інформаційних технологій (Інтернет речей) Інтернет речей: проблеми правового регулювання та впровадження: Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : НТУУ «КПІ ім. Ігоря Сікорського» Вид-во «Політехніка». 2017. – 238 с.

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

Ворушило С., к.ю.н., доцент кафедри адміністративного права і процесу ДВНЗ «Київський економічний університет імені Вадима Гетьмана»

УПРАВЛІННЯ МЕРЕЖЕЮ ІНТЕРНЕТ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ БЕЗПЕКИ

Характеристика мережі Інтернет і система управління ним впливають не тільки на міжнародно-політичний стан глобального інформаційного простору, але й на міжнародну інформаційну безпеку. З точки зору стабільності і безпеки розвитку і використання мережі Інтернет та міжнародної інформаційної безпеки в цілому, найважливіше значення має складатися з система міжнародного управління Інтернетом, а також роль провідних держав в даній системі.

Дослідженню питання управління мережею Інтернет в контексті національної та міжнародної безпеки були присвячені роботи таких

вітчизняних та зарубіжних вчених вчених як Л. Лессіг, М. Мюллер, Д. Носетті, К. Фьюкс, І.А. Бронніков, Д. Най, А.А. Головка та багато інших.

Відповідно до визначення, представленим в підсумковому звіті Робочої групи з питань управління Інтернетом ООН «правове управління Інтернетом є запровадження та застосування урядами, приватним сектором і громадянським суспільством, при виконанні ними своїх відповідних ролей, загальних принципів, норм, правил, процедур прийняття рішень і програм, що регулюють еволюцію і застосування мережі Інтернет » [4].

Відсутність регулювання з боку урядів і міжнародних організацій розглядалося авторами як загроза стабільному функціонуванню мережі Інтернет і безпеки користувачів. Однак у міру розвитку Інтернету збільшувався і масштаб державного та правового регулювання даної технології, так само, як і попередніх йому інформаційно-комунікаційних технологій(далі ІКТ) таких як телеграф, телефон, радіомовлення, тощо.

Звичайно, держави почали створювати правила, які керують поведінкою користувачів і розвитком Інтернету. Одним з перших кроків на шляху до формування системи управління Інтернетом було створення ICANN [5].

Безумовно, ініціативи уряду США, спрямовані на комерціалізацію Інтернету, що передували створенню ICANN (а саме, передача функцій управління технічною інфраструктурою інтернету комерційній структурі), спровокували протест як з боку широкої громадськості (перш за все, користувачів Інтернету), так і представників держав. З метою збереження контролю над ключовими елементами інфраструктури Інтернету, уряд США прийняло рішення передати функції управління системою доменних імен (Domain Name System, DNS) 148 некомерційної організації, з метою захистити Інтернет від урядового впливу (за винятком уряду США, які зберігали контрактні відносини з створюваної організацією).

Звичайно, угода між ICANN та Міністерством торгівлі США в останній раз було переглянуто 30 вересня 2016 року, давало цьому державному відомству повноваження з контролю над діяльністю ICANN і участі в ній. На сьогоднішній день функції IANA були передані і в 2016 році була зроблена чергова реформа ICANN[5].

Таким чином, вищезгадана реформа не вирішує проблем з легітимністю існуючої моделі управління Інтернетом, залишаючи уряду США досить істотні важелі впливу.

Як зазначає Д. Носетті, «в настільки політизованому контексті для США було життєво важливим зберігати контроль над ходом дебатів про управління Інтернетом», і в ході зустрічі в Бразилії домовитися про істотні зміни в існуючому режимі управління Інтернетом не вдалося. «США прагнуть

закріпити лідерство в глобальному інформаційному просторі, зберігаючи за собою контроль над ключовими інфраструктурами Інтернету. Разом з тим, зростає кількість держав, що оспорюють лідируючі позиції США в режимі управління Інтернетом, при цьому великі Інтернет-компанії, такі як Google і Facebook, сприймаються як провідники впливу США. Існуюча ситуація все частіше трактується як загроза міжнародній безпеці представниками дослідного товариства» [6, с.45].

У свою чергу Головка А.А. вказує на діяльність Інтернет-компаній (або компаній «Інтернет-індустрії») являє собою самостійну проблему, так як їх діяльність в контексті формування глобального інформаційного суспільства має низку відмінних характеристик і породжує специфічні міжнародно політичні проблеми. Інтернет-компанії визначають обличчя сучасного інформаційного суспільства, внаслідок чого їх діяльність має значущий політичний вимір і породжує суперечності на міжнародному рівні. Під компаніями «Інтернет-індустрії» (також використовується термін «Інтернет-компанії») розуміються бізнес-структури, які отримують основний дохід (понад 50% доходу) від надання послуг в он-лайн режимі.

Основне значення комерційної діяльності в даній області досить велике - Інтернет-компанії визначають, яким чином користувачі шукають інформацію, впорядковують її, спілкуються, формують контекст, в якому діє користувач Інтернету, керують його перевагами. Найбільш великими Інтернет-компаніями світу, за оцінками аналітиків Boston Consulting Group, є Amazon, Apple, Facebook, Google, Baidu, Tencent (країна базування перших чотирьох - США, останніх двох - Китай; причому останні чотири компанії є виробниками контенту, інформаційного вмісту Інтернету). У сучасній цифровій економіці домінує так звана олігополія GAFA (Google-Apple- Facebook-Amazon) [2, с.13].

Так, бренд-менежемент більшості західних Інтернет-компаній заснований на ідеях свободи доступу і поширення інформації. Так, компанія Google визначає свою місію як «організація Світової інформації, забезпечення її доступності та користі для всіх». Офіційна позиція США полягає в тому, що такі компанії забезпечують свободу слова і самовираження, а для незахідних країн виступають роллю інструментів інформаційного впливу, нав'язування західних цінностей. Одна з недавніх тенденцій в розвитку Інтернету, пов'язана, в тому числі і з діяльністю великих Інтернет-компаній, пов'язана з виникненням так званих «великих даних».

Бронніков І. А. стверджує, що на сучасному етапі управління інформацією, доступною користувачам, стає вкрай політизованою темою. У світлі подій «арабської весни», які отримали в пресі також назви «Twitter-революції» або «Facebook-революції», все більше держав схильні бачити

загрозу для національної безпеки в діяльності Інтернет-бізнесу. Інтернет-компанії розглядаються як провідники впливу США, підтвердженням чому стали дискусії в ході конференції в Дубаї в грудні 2012 року[1, с.1015].

Безперечно, на сучасному етапі розвиток Інтернету та ІКТ відбивається на всіх сферах життя суспільства і держави (в економіці, політиці, соціокультурній сфері), трансформуючи і саму природу світової політики. Сучасний етап інформаційної революції сприяє поширенню мережевих форм організації у світовій політиці, дифузії влади і посилення недержавних акторів.

Таким чином, у міжнародному співтоваристві існують суперечливі погляди на те, яким чином повинен бути організований Інтернет і яка роль держав і недержавних акторів в його управлінні. США прагнуть закріпити лідерство в глобальному інформаційному просторі, зберігаючи за собою контроль над ключовими інфраструктурами Інтернету. Разом з тим, зростає кількість держав, що оспорюють лідируючі позиції США в режимі управління Інтернетом (в їх числі Китай, велика частина країн пострадянського простору, а також цілий ряд країн, що розвиваються), при цьому великі Інтернет-компанії, такі як Google і Facebook, що підтримують існуючу модель управління інтернетом і забезпечення інформаційної безпеки, сприймаються як провідники впливу США.

Отже, сучасний правовий режим управління мережею Інтернет не відображає змін міжнародно-політичного ландшафту глобального інформаційного простору, що в свою чергу породжує загрози конфліктів і нестабільності. Коли політичні рішення класифікуються як технічне регулювання, стає можливим їх прийняття за закритими дверима, поза суспільним контролем, як це показали відкриття Е. Сноудена, в результаті порушуються не тільки демократичні процедури, а й руйнується атмосфера довіри, без якої неможливо співпрацю.

Звісно ж важливо, щоб політичні, економічні і технічні питання, що мають відношення до правового управління Інтернетом, вирішувалися за участю всіх зацікавлених сторін, так як забезпечити інформаційну безпеку і зберегти зв'язність Інтернету як глобальної системи жодна держава не в змозі без багатостороннього співробітництва.

Список використаних джерел:

1.Бронніков І. А. Інтернет як ресурс політичної влади // Право і політика. 2017. № 6. С. 1015.

2.Головка А. А. Інститути громадянського суспільства в системі інформаційної безпеки України / А. А. Головка // Вісник Національного технологічного університету України «Київський політехнічний інститут». Серія: Політологія. Соціологія. Право. – 2016. – № 1/2 (25/26). – С. 13-16.

3. Долженко К. І. Нормативно-правове регулювання інформаційної безпеки регіону / К. І. Долженко // Право і Безпека. – 2014. – № 3. – С. 43-48.

4. Доповідь Міжнародного союзу електрозв'язку «Захищеність мереж інформації та зв'язку: передовий досвід зі створення культури кібербезпеки». Женева: МСЕ 2010 // http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-R.pdf.

5. Кастельс М. Інформаційна епоха: економіка, суспільство і культура / пер. з англ. під наук. ред. О. І. Шкаратана. - М.: ГУ ВШЕ 2017.

6. Носетті Д. Життя після Едварда Сноудена: майбутнє управління Інтернетом // Комерсант. 09.04.2014. URL: <http://kommersant.ru/doc/2448799>

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

*Шрамко С., к.ю.н., в.о. вченого
секретаря Науково-дослідного
інституту вивчення проблем
злочинності імені академіка В.В.
Сташиса НАПрН України*

ВИКОРИСТАННЯ ІНТЕРНЕТУ РЕЧЕЙ (ІОТ²¹) У ЗАБЕЗПЕЧЕННІ ГРОМАДСЬКОЇ БЕЗПЕКИ: ПОСТАНОВКА ПРОБЛЕМИ²²

Забезпечення громадської безпеки є одним із пріоритетних напрямів діяльності державних органів у всіх країнах світу. У Законі України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII визначено, що громадська безпека і порядок – це захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації і захисту національних інтересів від впливу загроз [1]. У сучасному світі необхідною умовою для успішної реалізації покладених на державу завдань безпекового характеру є використання інноваційних технологій.

Із розвитком Інтернету речей (ІоТ) його можливості отримали певну ступінь використання у сфері громадської безпеки. ІоТ відіграє важливу роль у змінах нашого сучасного життя. Він розкриває можливості для державного сектора суттєво покращити якість надання послуг за допомогою даних, аналітики та автоматизації. Що таке ІоТ і який вплив він справляє на

²¹ ІоТ – скороч. від Internet of Things.

²² Матеріал підготовлений на виконання фундаментальної теми відділу кримінологічних досліджень НДІ вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України «Стратегія зменшення можливостей вчинення злочинів: теорія та практика».

суспільство? IoT – це будь-який об’єкт, підключений до Інтернету, що дозволяє безперешкодно надсилати та отримувати дані. Після підключення до загальної мережі в Інтернеті отримані дані можна легко використовувати для аналізу. У той час як приватний сектор активно впроваджує IoT у різноманітний спосіб, державні органи, покликані забезпечувати громадську безпеку, лише починають використовувати його переваги та можливості.

Використовуючи єдину систему інформаційних технологій передачі даних та пристроїв IoT ми вступаємо в епоху «розумних міст», де датчики та автоматика можуть суттєво підвищити рівень публічних послуг, а отже, й повсякденне життя громадян. Розумне місто – це не лише комплекс ІТ-технологій, це «розумний» спосіб життя загалом, а також управління міською інфраструктурою, у тому числі транспортною, інженерною, безпековою, екологічною та інші заходи, спрямовані на покращення міського середовища у різних сферах господарського життя. Так, застосування камер відеоспостереження і фотофіксації, засобів відеоаналізу, зв’язку та комп’ютерних інформаційних технологій дає можливість забезпечити безпеку міському середовищу, комфортну для проживання. «Розумне місто» здатне самостійно простежити за належним рухом транспорту і пішоходів, за ситуацією в громадських місцях, за лікарнями і школами [2].

Головною метою цього комплексу заходів є підвищення безпеки, комфорту проживання та якості самого життя для мешканців міста. Досягнення цієї мети можливе завдяки використанню пристроїв IoT за такими напрямками.

Моніторинг в реальному часі. Використовуючи мікрофони, відео, датчики та інші підключені пристрої, стратегічно розташовані по всьому місту, поліція може легко визначити, коли і де відбувається злочин, що дозволить швидко встановити особу злочинців.

Швидкість у прийнятті рішень, що полягає у можливості за необхідності зламати сховища даних для збирання цінної інформації, щоб у подальшому використати її для прийняття обґрунтованих рішень у сфері громадської безпеки. Наприклад, IoT може об’єднати безліч релевантних даних із різних джерел і аналізувати їх у режимі реального часу, що дозволить швидко вжити заходи убезпечення громадян від потенціальних загроз. Таким чином, IoT дозволяють містам використовувати аналітику в реальному часі, яка може допомогти їм відразу ж зрозуміти і усунути загрози громадській безпеці.

Утім, говорячи про переваги IoT, слід вказати і на його недоліки, а саме: відсутність загальних правил і стандартів, що ускладнює впровадження універсальних рішень; енерговитратність (не завжди вдається домогтися

автономності мережі та отримання енергії з навколишнього середовища); питання безпеки та конфіденційності інформації; висока вартість техніки [3].

Щоб повною мірою використовувати усі переваги, які IoT обіцяє надати для ініціатив у сфері громадської безпеки, міста мають прийняти горизонтальну платформу, яка послужить основою для їх вирішення. Це кращий спосіб гарантувати, що вони упровадять нововведення безпечним і ефективним способом для досягнення своєї головної мети – убезпечення населення від загроз, у тому числі кримінальних.

Звичайно, новітні технології лише упроваджуються у наше повсякденне життя, але вже зараз стає очевидним, що трансформація міст має відбуватися лише за умови співпраці між державним і приватним секторами. Виклики перед сучасними містами настільки серйозні та ресурсозатратні, що державний сектор сам по собі не зможе забезпечити інструменти та рішення, які містам необхідно адаптувати до змін, яких очікують суспільство та громадяни.

Список використаної літератури:

1. Про національну безпеку: Закон України від 21 червня 2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 11.10.2019).

2. Горошко М. Що таке «розумне місто» і чи вдасться Україні перейняти світовий досвід. URL: <https://life.pravda.com.ua/columns/2018/11/27/234336/> (дата звернення: 11.10.2019).

3. Інтернет речей: концепція IoT. Що чекати від майбутнього? URL: <https://futurum.today/internet-rechei-kontseptsii-iot-shcho-chekaty-vid-maibutnoho/> (дата звернення: 11.10.2019).

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

*Гоц О., старший викладач
Національної академії СБУ*

ІНФОРМАЦІЙНА БЕЗПЕКА І СУЧАСНІСТЬ

Наукове поняття «Інформаційна безпека» включаючи його кількісний і якісний аспект; підводить під поняття кількості інформації, визначеної як величина, зворотно пропорційна степені ймовірності тієї події, про яку йде мова в повідомленні. Чим більша ймовірність події, тим менше інформації несе повідомлення про те, що вона відбулась і навпаки. В наш час, завдяки розкриттю нового наукового поняття інформації, відкрито та запроваджено новий аспект матеріальної єдності світу який дає можливість визначення єдиної точки зору до багатьох раніше абсолютно різних думок пов'язаних із передачею інформації технічними каналами, функціонуванню персональних

електронно-обчислювальних машин та телекомунікаційних систем. Все це в першу чергу пов'язано із необхідністю зберігання передачі і обробки закритої інформації а також її безпеки. Поняття інформації у даному випадку відіграє роль аналогічну поняттю енергії у фізиці. В понятті інформації необхідно відрізняти два аспекти. По-перше, інформація являє собою міру організації системи. Математичний вираз для інформації тотожний виразу для *ентронії*, взятої із зворотнім знаком. Як ентропія системи виражає степінь її не упорядкованості, так інформація дає міру її організації. Так поняття інформації складає внутрішню систему процесу і може бути названо структурною інформацією. По-друге, від структурної інформації необхідно відрізняти інформацію, завжди зв'язану з відношенням двох процесів. Теорія інформації як правило має справу з відносною інформацією яка тісно пов'язана з *відображенням*. Якщо в предметі відбуваються зміни що відображають вплив іншого предмета то можна сказати, що перший предмет стає носієм інформації про другий предмет. В інформаційних системах зміни в предметі (А), визначені впливом предмета (Б), являються не просто окремими характеристиками А, але є також фактором функціонування інформаційної системи саме в якості носія інформації про Б. Відносна інформація із потенційної, якою вона являється в до електронних системах (системах ніжної природи, не пов'язаної з *управлінням*), перетворюється тут в актуальну інформацію, тобто з пасивного відображення у до електронних системах у активне відображення. З цієї точки зору мозок людини представляє виключно складну електронну систему, зберігаючи і перероблюючи наступаючу із зовнішнього світу відносно актуальну інформацію. Властивості мозку пізнавати і відображати зовнішній світ, який виступає як ланцюг у розвитку процесів пов'язаних із передачею і переробкою інформації. У сучасному філософському вченні про інформацію необхідно бачити конкретну властивість матерії до відображення.

Інформація (лат. *Informatio* - роз'яснення, викладення) – а) відомості, совокупність даних, знань, б) одне із основних понять інформатики. інформації, в багатьох випадках відходить від змістової сторони повідомлення.

У ХХІ столітті система забезпечення інформаційної безпеки сучасних держав зіткнулася з низкою чинників, які негативно впливають на можливості держави ефективно забезпечувати захист своїх національних інтересів в інформаційній сфері. Серед зовнішніх чинників найбільш небезпечним уявляється процес глобалізації, який супроводжується нав'язуванням країнам і народам інших цінностей і підривом їх традиційних цінностей за допомогою нових, інформаційно-телекомунікаційних систем і технологій.

На сучасному етапі боротьби держав за сфери впливу акцент із явного застосування сили усе помітніше зміщується на використання більш гнучких засобів, основним з яких є контроль і керування інформаційними ресурсами. Для досягнення цих цілей в умовах зростаючої насиченості інформаційними і керуючими засобами, у тому числі й іноземного виробництва, може бути використане високоефективне і таємне проникнення в програмне забезпечення державних інформаційних та управлінських систем України.

Крім того, висока результативність використання інформаційно-телекомунікаційних систем і технологій, широкий спектр їх застосування і прихований характер дії виявилися причинами, з яких багато країн ведуть розробки в галузі теорії й практики їх застосування як інформаційної зброї і, як наслідок, розробки теорії ведення інформаційних війн.

Стрімкий розвиток технологій роботи з інформацією в розвинених країнах обумовлює формування стратегій “інформаційної війни”, головною метою якої є інформація, оволодіння нею чи зміна у своїх інтересах. Очевидним стає той факт, що інформаційні технології відіграють надзвичайно важливу роль не тільки в забезпеченні національної безпеки, але й у розвитку особистості, суспільства і держави в сучасних умовах.

Виходячи із реалій загарбницької інформаційної політики Росії, Україна однією із перших зазнала інформаційного тиску з боку сусідньої держави - агресора. Інформаційні атаки з боку РФ не припиняються протягом останніх п'яти років. Інформаційна війна яку здійснює агресор проти суверенної держави Україна відбувається також на фоні реальних бойових дій що відбуваються на території Донбасу. Постійному інформаційному впливу що супроводжується страхом за майбутнє підлягають також громадяни України що тимчасово перебувають на території тимчасово окупованого Криму.

По-перше, інформація займає одне з провідних місць у системі забезпечення життєво важливих інтересів усіх країн і безумовно України. Це, насамперед, зумовлено нагальною потребою створення розвинутого інформаційного середовища українського суспільства, однак, саме через таке середовище найчастіше здійснюються загрози національній безпеці.

По-друге, в сучасних умовах система забезпечення інформаційної безпеки України, яка склалася раніше, явно не відповідає новим принципам забезпечення інформаційної безпеки і не може надійно протидіяти інформаційним загрозам. Тому в сучасний період розвитку України гостро постало питання визначення пріоритетів у сфері державної політики забезпечення інформаційної безпеки і зосередження зусиль на найбільш важливих ділянках потенційних і реальних загроз.

По-третє, проблема забезпечення інформаційної безпеки в сучасних умовах зумовлена особливою роллю інформації у функціонуванні всіх сфер суспільного життя, оскільки саме інформаційні фактори набувають усе більшого значення. Особливе місце займає інформація в забезпеченні і здійсненні зовнішньополітичної діяльності держави. Без створення умов формування достовірної, повної і своєчасної інформації для прийняття зовнішньополітичних рішень і запобігання незаконного використання актуальної інформації про зовнішньополітичну діяльність, тієї інформації, що забезпечує пріоритети України на зовнішньополітичній арені, Україна не зможе відігравати гідну роль у світовій спільноті. Тому існує необхідність подальшого поглибленого пізнання сутності інформаційної безпеки, насамперед, на філософському рівні.

По-четверте, в умовах розширення інформатизації українського суспільства, коли інформація стає товаром і ресурсом розвитку, та нарощування політичної, економічної, воєнної та духовної потужності держави, коли інформаційна сфера безпеки все більше й більше виступає системоутворючим чинником усієї багаторівневої системи забезпечення безпеки особи, суспільства і держави, визначення пріоритетних напрямів діяльності державних органів країни стосовно забезпечення інформаційної безпеки стає найважливішим теоретичним і політичним завданням.

По-п'яте, оскільки інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових сфер життя і діяльності особи, суспільства і держави в Україні, і водночас вона являє собою самостійну галузь національної безпеки, покликану забезпечити не лише захист інформації, а й збереження самобутності вітчизняної культури, необхідним є наукове обґрунтування і розробка чітких і дієвих механізмів забезпечення інформаційної безпеки України та можливостей використання її теоретичних конструкцій у практичних цілях.

По-шосте, інтеграція України у світовий інформаційний простір як планетарного, так і регіонального масштабів, супроводжується все більшим зростанням відкритості українського суспільства. Процес раціонального сполучення вітчизняного інформаційного простору, що формується, і міжнародного простору, що постійно змінюється, вимагає наукового обґрунтування пріоритетів діяльності державних органів і суспільних організацій у вирішенні завдань інформаційної безпеки України. Україна має гостру потребу в ефективній політиці забезпечення безпеки своїх національних інтересів в інформаційній сфері, яка повинна враховувати об'єктивні реалії сучасного інформаційного середовища і базуватися на науково-методичних засадах. Вона дозволить державним органам влади

відійти від стилю рефлексії управління інформаційною безпекою та спрямувати свою діяльність на запобігання загрозам в інформаційній сфері.

По-сьоме, протидія загрозі так званого «Руского міра», під хворобливим пропагандистським впливом якого перебуває частина українців. Що по своїй суті становить загрозу також і національній безпеці нашої держави її суверенітету і територіальній цілісності.

По-восьме протидія інформаційного впливу на значну частину віруючих українців, adeptів «Руского православ'я» що по своїй суті і методах впливу не відрізняється від методів політичного впливу пропагандистських медіа каналів сусідньої держави.

По-дев'яте встановлення історичної справедливості та надання оцінки через засоби масової інформації дійсним фактам участі українців у розбудові європейського суспільства і особливо ролі Українського народу у II світовій війні; спотворені російською пропагандистською машиною.

Важливо підкреслити, що проблемі забезпечення інформаційної безпеки України постійно приділяється особлива увага з боку вчених і практиків. Однак наукових праць, в яких безпосередньо досліджується інформаційна безпека України, явно недостатньо. На сьогодні, переважна більшість наукових розробок стосовно проблеми інформаційної безпеки належить до технічних наук.

Список використаних джерел:

1. Биченок М. М. Основи інформатизації управління регіональною безпекою / Биченок М. М. – К. : РНБОУ, 2005. – 194. – 194
2. Богданович В. Ю. Методологические основы системных Я. Маначинский. – К. : исследование проблем военной безопасности и государства / В. Ю. Богданович, А. НИСД, 2001. – 172 с.
3. Бойко О. Інформатизація культури України / О. Бойко // Філософські обрії. – 2006. – №16. – С. 164–178.
4. Бондар Ю. В. Національний інформаційний простір новітньої України: становлення та функціонування у процесі політичної трансформації суспільства / Ю. Бондар. – К. : МАУП, 2007. – 184 с.

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

*Гуртовенко С., асистент кафедри
адміністративного права і процесу
ДВНЗ «Київський економічний
університет імені Вадима Гетьмана»*

ПОНЯТТЯ ТА КЛАСИФІКАЦІЯ ВИКЛИКІВ І ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИ

Питання поняття та класифікації викликів і загроз інформаційної безпеки так і не знайшло свого рішення. У той же час, актуальність даного аспекту не викликає сумнівів, в зв'язку з чим робиться спроба проведення класифікації видів викликів і загроз інформаційної безпеки - в ключі досліджуваного предмета - до безпеки особи. Тобто мова про ту сукупність умов і факторів, які створюють реальну небезпеку порушення інформаційної безпеки особи.

Дослідженням поняття та класифікації викликів і загроз інформаційної безпеки особи займалося багато зарубіжних і вітчизняних науковців, серед них А.К. Жарова, А.М. Тарасов, А.В Шамраєв, Л.К. Терещенко, О.Г. Рогова, Г.Г. Камалова та інші.

Підійти до класифікації видів і форм загроз безпеки особи в глобальному інформаційному суспільстві можна з урахуванням різних підстав. По-перше, має значення мета, яку переслідують джерелом тієї чи іншої загрози. За даним критерієм можна виділити загрози, що переслідують цілі: а) вплив на свідомість особи, на її психологічний стан; б) надання деструктивності, що завдає шкоди впливу на здоров'я особи (наприклад, шляхом поширення в обіг заборонених лікарських засобів, тощо); в) оволодіння особистою інформацією, в тому числі - з метою використання її в протиправних цілях; г) поширення ідеології тероризму, радикальних ідей в мережі Інтернет; д) впливу на статеву недоторканість і статеву свободу особи; е) фінансового шахрайства, ж) розвитку антигромадських стереотипів поведінки, тощо.

Серед наведених видів загроз інформаційній безпеці найпотужніше поширення сьогодні набуло фінансове шахрайство, про що свідчать конкретні дані міжнародних лабораторії, які наводить в одній зі своїх робіт А.В. Жданов: «приблизно 20% інтернет-користувачів при здійсненні банківських операцій і онлайн-покупок як мінімум два рази ставали жертвами кіберзлочинців, втрачаючи при цьому грошові кошти» [1].

Так, загрози можуть виходити ззовні, тобто бути зовнішніми, або - виходити від самої людини (внутрішні загрози). Приклад внутрішньої загрози - відкриття доступу до особистої інформації необмеженому числу осіб самим

користувачем в соціальних мережах. Прикладами зовнішніх загроз можуть виступати численні способи злому персональних комп'ютерів з метою крадіжки особистих даних і паролів.

А.В. Шамраєв зазначає, що залежно від характеру впливу, критерієм виникнення загрози інформаційної безпеки особи можуть бути ненавмисними, випадковими, викликаними, наприклад, технічними збоями, або - навмисно, цілеспрямовано створюють небезпеку, що заподіюють шкоду, що веде до несприятливих наслідків для особи [6, с.17].

Так, виключно умисний характер - інформації, поширюваної за допомогою мережі Інтернет, забороненої до поширення в нашій країні. З метою обмеження доступу до сайтів, що містять таку інформацію, створена Єдина автоматизована інформаційна система «Єдиний реєстр доменних імен, показників сторінок сайтів в інформаційно-телекомунікаційній мережі Інтернет і мережевого адресу, що дозволяють ідентифікувати сайти в інформаційно-телекомунікаційній мережі Інтернет, що містять інформацію, поширення якої в Україні заборонено».

Рогова О.Г. звертає увагу, що в якості підстави для класифікації загроз інформаційній безпеці особи окремо можна виділити джерела загроз в мережі Інтернет. В якості таких загроз виступають: небезпечні інтернет-сайти (ряд пошукових сервісів передбачають різні способи інформування користувачів про рівень благонадійності того чи іншого сайту), фішингові сайти, шкідливе програмне забезпечення, спам-розсилки, шахрайські сайти, що рекламуються з метою отримання прибутку (фінансові піраміди, так звані фальшиві інтернет-магазини, тощо)[84, с.512].

Безумовно, загроза інформаційної безпеки особи може бути визначена і всередині конкретного правового інституту - наприклад, інституту персональних даних. Так, Камаловою Г.Г. виділені такі загрози, як: а) впровадження та використання операторами інформаційних технологій, спрямованих на збір і поширення інформації, що відноситься до суб'єктів персональних даних, обробка яких не відповідає цілям їх первісного збору; б) поява в системі законодавства України в галузі персональних даних сегмента нормативних правових актів, що не відповідає положенням Закону України «Про захист персональних даних»; в) зростання числа фактів неправомірної обробки персональних даних щодо чутливої інформації (біометричні і спеціальні категорії персональних даних, персональні дані неповнолітніх); 4) пропаганда моделей поведінки громадян, спрямованих на вільне поширення персональних даних [2, с.8].

Таким чином, підбиваючи підсумки вище проаналізованої інформації, ми можемо запропонувати таку класифікацію викликів та загроз для особи в сучасному інформаційному суспільстві:

- *Залежно від мети*: вплив на свідомість особи, на її психологічний стан; надання певної деструктивності, що завдає шкоду щодо впливу на здоров'я особи (наприклад, шляхом поширення у обіг заборонених лікарських засобів тощо.); оволодіння особистою інформацією, в тому числі - з метою використання її в протиправних цілях;

- *Залежно від джерела загрози* - загрози безпеці особи, які виходять від: злочинців і злочинних співтовариств, діяльність яких спрямована на крадіжку особистої інформації, персональних даних, на розкрадання чужого майна шляхом шахрайства в сфері комп'ютерної інформації; націоналістичних, релігійних, етнічних та інших організацій і структур, які використовують інформаційно-телекомунікаційні технології для терористичної діяльності;

- *Залежно від розташування джерела загрози щодо самого об'єкта*: загрози можуть виходити ззовні, тобто бути зовнішніми; загрози, які виходять від самої людини (внутрішні загрози).

Джерела загроз в мережі Інтернет: небезпечні інтернет-сайти (ряд пошукових сервісів передбачають різні способи інформування користувачів про рівень благонадійності того чи іншого сайту); фішингові сайти; шкідливе програмне забезпечення; спам-розсилки; шахрайські сайти, що рекламуються з метою отримання прибутку (фінансові піраміди, фальшиві інтернет-магазини, тощо)

Загрози інформаційної безпеки новітнього типу: загрози, які виходять від спеціальних файлів куки (від англ. Cookie); погрози, спрямовані на трафік віртуальної валюти Bitcoin; загрози конфіденційності персональних даних внаслідок новітньої технології онлайн-реклами Real-TimeBidding (RTB).

Звичайно, при реалізації проекту створення об'єднаної картотеки справ судів загальної юрисдикції, з урахуванням специфіки вирішуваних справ і вимог вилучення з текстів рішень судів загальної юрисдикції інформації, яка розкриває персональні дані процесу, для особи існує реальна небезпека проблем недобросовісного використання її персональних даних.

Так, приклади масованих кібератак, здатних привести до серйозних наслідків в формах витоку службової інформації, персональних даних, збоїв в роботі банків і автоматизованих систем управління виробничими і технологічними процесами критично важливих об'єктів інфраструктури держави відомі і широко обговорюються.

Отже, на основі наукового дослідження нових викликів і загроз та виявлення небезпечних тенденцій інформаційної безпеки в умовах в

глобального інформаційного суспільства здається можливим враховувати такі критерії як джерело тієї чи іншої загрози, залежно від джерела виклику (загрози), характер розташування джерел загрози щодо самого об'єкта (зовні або всередині), а також характер впливу. Це дозволило сформулювати авторський підхід до класифікації видів викликів і загроз інформаційної безпеки особи з метою вдосконалення системи правового забезпечення інформаційної безпеки особи в Україні.

Аналіз застосовуваних інформаційних технологій дозволив зробити висновок про наявність особливої групи загроз, що виникають у сфері цифрової економіки, розвитку фінансово-кредитних відносин (пов'язаних з обігом електронних грошових коштів, криптовалюта BitCoin, LitCoin, OneCoin, інших різновидів криптовалюта, загроз конфіденційності персональних даних внаслідок новітньої технології онлайн-реклами Real-TimeBidding (RTB), загроз, що виходять від спеціальних файлів куки (cookie).

Список використаних джерел:

1. Жданов А. В. Інтернет, ЗМІ та кібердифамація: Актуальні проблеми // Проблемний аналіз та державно-управлінське проектування. 2012. №5 (25) [Електронний ресурс] // <http://cyberleninka.ru/article/n/internet-smi-i-kiberdiffamatsiya-aktualnye-problemy>

2. Камалова Г.Г. Біометричні персональні дані: визначення та сутність // Інформаційне право. - 2016. - № 3. - С. 8 - 12.

3. Наумов В.Б. Право та Інтернет: Нариси теорії і практики. - М.: Книжковий Будинок Університету, 2012. - С.68-95.

4. Полякова, Т.А. Правове забезпечення інформаційної безпеки при побудові інформаційного суспільства в Україні: дис. ... докт. юрид. наук / Т. А. Полякова. - М., 2018. - С. 94.

5. Рогова О.Г. Захист персональних даних у законодавстві Європейського Союзу та України / Теорія та практика державного управління: зб. наук. пр. — Х.: Вид-во ХарПІ НАДУ «Магістр», 2011. — Вип. 3 (34). — 512 с.

6. Шамраєв А.В. Правове регулювання інформаційних технологій. Аналіз проблем і основні документи. - М., «Статут», 2013. - С. 17.

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

*Гречана А., студентка КПІ ім.
Ігоря Сікорського*

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Однією із рушійних сил розвитку сучасного суспільства являється впровадження інноваційних технологій в усі сфери життя. Інформаційно-комунікаційні технології – невід’ємна частина щодення і важлива ланка становлення інформаційного суспільства в Україні, проте з їхнім поширенням

зростають також і ризики застосування цих технологій для вчинення правопорушень та злочинів.

Конвенція про кіберзлочинність, яку було ратифіковано Україною, виділяє правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями), правопорушення, пов'язані з комп'ютерами (підробка, шахрайство), правопорушення, пов'язані зі змістом (праваопорушення, пов'язані з дитячою порнографією), правопорушення, пов'язані з порушенням авторських та суміжних прав [3].

Поняття «кіберзлочину» визначено Законом України «Про основні засади забезпечення кібербезпеки України» як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, а під кіберзлочинністю мається на увазі сукупність кіберзлочинів [2]. Злочини, які вчиняються за допомогою або в кіберпросторі, закріплені в шістнадцятому розділі Кримінального кодексу України [4]. Закон України «Про основні засади забезпечення кібербезпеки України» також виділяє серед ризиків порушення безпеки в кіберпросторі кіберрозвідку, кібертероризм та кібершпигунство [2].

До найбільш розповсюджених прикладів проблемних питань сучасного використання технологій можна віднести викрадення особистих даних в мережі Інтернет, розповсюдження комп'ютерних вірусів, викрадення коштів з банківського рахунку, порушення авторських прав, кібербулінг, продаж наркотиків та зброї в мережі Інтернет та інші.

Не дивлячись на прагнення держави забезпечити безпеку суспільства в інформаційному просторі шляхом ратифікації Конвенції про кіберзлочинність, прийняття законів, які регулюють сферу кібербезпеки, створення Департаменту кіберполіції, рівень кіберзлочинності є досить великим. Згідно із статистикою Департаменту кіберполіції Національної поліції України в 2018 році виявлено 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій, а в середньому щорічно кількість таких злочинів збільшується на 2,5 тисячі.

Можна виділити ряд причин поширення злочинів в сфері кібербезпеки. Наприклад, чинне правове регулювання сфери кібербезпеки не відповідає стрімкому розвитку інноваційних технологій, більш складний процес виявлення і розслідування кіберзлочину. Бондаренко О.С. та Рєпін Д.А. в своїй роботі «Кіберзлочинність в Україні: причини, ознаки та заходи протидії» серед

причин наводять також велику прибутковість, технічну простоту, психологічний фактор анонімності [1].

Для боротьби із кіберзлочинністю необхідно застосувати багатосторонній підхід як для профілактики і протидії кіберзлочинам, так і для їхнього розслідування. Зокрема проведення інформаційної кампанії задля протидії кіберзлочинності, відповідність законодавства сучасному рівню розвитку інформаційно-комунікаційних технологій, підготовка фахівців в сфері кібербезпеки.

Досить важливим є міжнародне співробітництво в цій сфері, оскільки кіберзлочинність має глобальний характер і подолати її тільки на національному рівні неможливо. Одним із перших кроків міжнародного співробітництва в сфері кібербезпеки в Україні була ратифікація Конвенції про кіберзлочинність. Лешукова І. В. в своїй роботі «Проблемні питання міжнародного співробітництва у сфері протидії кіберзлочинності» серед причин підвищеної небезпеки кіберзлочинності для міжнародного товариства відзначає транскордонність (особа може вчиняти кіберзлочини з будь-якої точки світу, не зважаючи на кордони), відсутність усталеного механізму розкриття та розслідування даних злочинів, впровадження технологій в усі сфери функціонування держави і суспільства, тому необхідно застосовувати комплексний підхід до вирішення проблеми кіберзлочинності не тільки на національному рівні, а і на міжнародному [5].

Отже, однією із сучасних небезпек для нормального існування суспільних відносин є кіберзлочинність. Розвиток сфери кібербезпеки на національному і на міжнародному рівнях, дотримання і поліпшення законодавства, яке регулює кіберпростір, деталізації в нормативно-правових актах термінології стосовно кіберзлочинності, виконання міжнародних зобов'язань в сфері кібербезпеки, належне виконання співробітниками кіберполіції покладених на них обов'язків – це невичерпний перелік чинників, які стануть каталізатором розвитку інформаційного суспільства в Україні, а також зможуть мінімізувати рівень кіберзлочинності.

Список використаних джерел:

1. Бондаренко О.С., Репін Д. А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії / О.С. Бондаренко, Д.А. Репін // Порівняльно-аналітичне право. – 2018. – № 1. URL: http://www.par.in.ua/1_2018/73.pdf
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 19.06.2003 року// Відомості Верховної Ради України. –2003. – № 39. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
3. Конвенція про кіберзлочинність(підписана 23 листопада 2001 року. // Офіційний вісник України. –2007. – №65. — URL: https://zakon.rada.gov.ua/laws/show/994_575

4. Кримінальний кодекс України (Прийнятий 5 квітня 2001 р. на сьомій сесії Верховної Ради). // Відомості Верховної Ради України. – 2001. – № 25-26. — URL: <https://zakon.rada.gov.ua/laws/show/2341-14/print>

5. Лешукова І. В. Проблемні питання міжнародного співробітництва у сфері протидії кіберзлочинності//Актуальні питання розслідування кіберзлочинів. –Київ. –ВАІТЕ. – 2013.

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

*Коркач Д. В., Ткаченко Д. Д., студенти
Національної академії СБУ*

КІБЕРБЕЗПЕКА ЛОКАЛЬНИХ МЕРЕЖ ПІДПРИЄМСТВ

В сучасному Світі більшість людей майже не уявляє свого життя без смартфонів та персональних комп'ютерів. Інтернет простір стрімко розвивається, а разом із ним, пліч-о-пліч, збільшується кількість ІТ загроз. Підприємства, компанії, а особливо корпорації – переходять на повну автоматизацію в організації праці. Але не всі замислюються над тим, що звичайний на вигляд електронний лист з пошти офісного співробітника, здатний припинити роботу всієї локальної мережі організації. Що ж робити за для уникнення загроз, як організувати безпечну роботу компанії в інтернет просторі з раціональними витратами на запобіжні заходи, замість повного відновлення системи, та які заходи треба проводити для організації прийняттого рівня кібербезпеки і попередження проникнення шкідливих софтів в локальну мережу корпорацій та підприємств?

Кожна корпорація, незалежно від її розміру, повинна мати людину, яка відповідає за інформаційну безпеку. Це може бути окрема особа, відділ чи певні делеговані повноваження вже існуючому працівнику. Зазвичай, ці обов'язки покладають на системного адміністратора мережі, який питаннями безпеки опікується в останню чергу, особливо, якщо вона потребує додаткового фінансування. Тому, важливо, щоб на підприємстві була людина, яка відповідає, суто, за інформаційну безпеку. В тому випадку, якщо мережі великі, цим питанням може займатися спеціальний підрозділ, але, на жаль, в нашій країні, кількість компаній, в яких працюють повноцінні відділи спеціалістів по кібербезпеці, можна перерахувати на пальцях. Зазвичай, на великих підприємствах – це від 1 до 4 працівників, у великих холдингах – максимум п'ять. Працівник, який несе за це відповідальність, має бути професіоналом, котрий: володіє знаннями і вміннями, які дадуть змогу все правильно організувати, наділений відповідним досвідом, який має спроможність оцінювати головні загрози, формує чітке розуміння того, як

перш за все, необхідно захищатись від певного типу загроз і атак, співпрацювати і з фізичною безпекою, і з IT-департаментом, спроможний оцінювати рівень критичності кібератаки та розраховувати ступінь можливих втрат (партнерів, фінансів, тощо), щоб аргументувати свою позицію перед керівництвом бізнесу.

Проблема підключення мобільних гаджетів і особистих комп'ютерів до Wi-Fi мережі підприємства існує давно. Тема яка стала в свій час відома і популярна BYOD (Bring Your Own Device), що в перекладі означає «принеси свій власний девайс». Практично всі міжнародні вендори мають свої власні рішення з цього приводу і вітчизняні компанії або використовують, або адаптують вже міжнародні методи що до потреб Українського бізнесу (бо ціни не ті, і обсяги інші). Але існують певні рішення, напрацювання, які направлені на вирішення питання: яким чином користувач локальної мережі може безпечно використовувати власний девайс, яким користується як для особистих, так і для корпоративних цілей. Ця проблема не нова, тому, маючи бажання її вирішувати, вона успішно може бути виправлена. Головне питання полягає в тому, чи готові компанії, вони ж і потенційні жертви, витратити на це кошти, на скільки для них це актуально (а це, практично, актуально для всіх, коли, в середньому, на одну людину у використанні припадає 2 девайси). Тому метод по використанню пристрів, як і у власних цілях, так сумісно і у корпоративних мережах дуже зручний, бо вразі необхідності ви завжди зможете скинути прайс (або ще щось). Проблема не нова, не складна, але, як і на кожен захід по кібербезпеці – необхідно витратитися.

Дуже небезпечно підключення переносних модемів до комп'ютерів, які являються частиною локальної мережі компанії. Все що порушує правила безпеки компанії - автоматично стає небезпечним. Якщо у компанії є: план, уявлення, модель загроз, розуміння ризиків, правила безпеки для співробітників, мережевих адміністраторів (для керівництво в тому числі), то не має бути виключень по кібербезпеці. Хоча, насправді, це дуже рідко трапляється, бо, достатньо часто, керівництво, не дивлячись на заборону, просить надавати доступ до ненадійних ресурсів за власними потребами. Політика безпеки для того і створюється, щоб вона враховувала усі можливі ризики та канали витоку, а також імовірні вектори атаки. Коли в політику безпеки йде якесь несанкціоноване втручання, то воно повинно бути, принаймні, під контролем людини, яка відповідає за безпеку (хоча б поінформована). Наприклад, якщо все працює, а керівництво компанії звертається з проханням надати доступ до якогось забороненого сайту (який заборонений і є не легітимним, з точки зору законодавства), відбувається

виклик уповноваженого співробітника, який знаходить метод обходу заборони (прокладає тунель VPN). Але це буде санкціоновано, про це буде відомо, тому, в разі загрози, дасть змогу використати запобіжні заходи. Також можливий варіант відкриття VPN доступу обмеженого у часі. Таким чином флеш-модеми – це серйозне порушення. Цим шляхом для публічного доступу відкривається величезна кількість документів, які точно не призначені для розповсюдження. Останнім часом, саме через такі несанкціоновані підключення користувачів до корпоративної локальної мережі, сталося безліч витоків конфіденційної інформації.

Однозначно варто проводити тренінги по кібербезпеці для працівників компаній, які не являються іт-спеціалістами. Ефективність та користь таких заходів в плані покращення рівня безпеки організації просто вражаюча. Як показує практика найчастіше основним елементом вразливості системи є людський фактор. Зловмисники часто використовують прийоми соціальної інженерії, пишуть листи працівникам і ті піддаючись на цю провокацію, надають змогу хакерам отримати доступ до конфіденційних даних компанії, що може стати критичним для неї. Для попередження цього необхідно проводити тренінги для всіх працівників по цьому напрямку, розказувати як готуються фейкові листи, яка тема підбирається, що запитується, доносити інформацію про те, як «взламали» їх по соціальному каналу. Кожна людина яка має потенційні ризики, повинна знати що треба робити і чого не треба робити. Зазвичай достатньо одноденного тренінгу наприклад в суботу, щоб не забирати багато робочого часу. За чотири години можна донести достатньо корисної інформації. Ще один важливий момент в цьому- налагодження інтерактивного контакту зі слухачем. Щоб людина все зрозуміла на прикладах.

У галузі створено достатню кількість дієвих технологій для захисту локальних мереж. Вимоги безпеки вимагають постійного удосконалення цих технологій. Для забезпечення безвідмовності та стабільності у роботі продовжується пошук нових технологій та варіантів розширення можливостей існуючих систем захисту. Практичний досвід застосування сучасних технологій свідчить про необхідність забезпечення гнучкості та надійності систем захисту, а також їх багатоваріантності та постійного удосконалення. Багато компаній починають серйозно сприймають кібербезпеку, вже після того, як з ними трапиться негативний інцидент, а до того постійно відкладають організацію адекватного рівня захисту. Доцільним є ствення форумів кібербезпеки із накопиченням практики та можливостями мобілізації фахівців для нейтралізації конкретних атак в режимі реального часу.

Список використаних джерел:

1. Баранов, О.А., 2014. Про тлумачення та визначення поняття «кібербезпека», Правова інформатика.
2. Кононович В. Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 3: Архітектура безпеки. Концепція захисту інформації : [навч. посібник для вузів, затверджено Міністерством транспорту та зв'язку України] / В. Г. Кононович. – ОНАЗ. – Одеса, 2009. – 194 с.
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
4. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
5. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
6. Тардаскін М.Ф. Механізми забезпечення інформаційної безпеки телекомунікаційних мереж загального користування / М.Ф. Тардаскін, В.Г. Кононович, О.О. Вараксін, Т.М. Тардаскіна // Зв'язок – 2005. – No 8 – С. 24-28.

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

Андрій Благодарний, к. ю. н., старший науковий співробітник, професор кафедри загальноправових дисциплін Національної академії Служби безпеки України

ДО ПИТАННЯ ВДОСКОНАЛЕННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Дедалі більшу роль в процесах державотворення відіграє такий важливий прояв демократичного розвитку країни, як наявність ефективної комунікації між владними інститутами та громадянським суспільством. В сучасних умовах стратегічна комунікація в системі державного управління стає особливо результативною, оскільки передбачає реалізацію трьох основних цілей: передачу інформації, трансформацію позиції громадськості у ставленні до державно-управлінських інституцій та зміну поведінки громадянина. Це відкриває нові можливості для участі громадськості в процесах формування та реалізації державної політики, що дає змогу зробити її більш відкритою, прозорою та демократичною [1; с. 5–6].

Питання стратегічних комунікацій є предметом уваги провідних як вітчизняних, так і зарубіжних науковців та науково-експертних центрів. Формуванню сучасного бачення ролі стратегічних комунікацій у системі державного управління сприяли, зокрема, праці таких учених, як А. Баровська,

Т. Безверхнюк, С. Гуцал, Д. Дубов, Ю. Кальниш, Л. Кампанцева, О. Кушнір, В. Ліпкан, Г. Саймон, І. Пантелейчук, В. Пилипчук, Г. Почепцов та інших авторів.

Воєнна доктрина України визначає стратегічні комунікації як скоординоване і належне використання комунікативних можливостей держави її публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [2].

У науковій літературі вітчизняні автори, взявши за зразок стандарти НАТО, де питанням стратегічної комунікації приділено значну увагу, як правило, виділяють такі компоненти системи стратегічних комунікацій: зв'язки з громадськістю; публічна дипломатія та військові заходи в підтримку публічної дипломатії; зв'язки зі ЗМІ; інформаційні заходи міжнародного військового співробітництва; цивільно-військове співробітництво; дії в кіберпросторі, включаючи соціальні мережі; залучення ключових лідерів до проведення інформаційних заходів; внутрішня комунікація (робота з особовим складом/внутрішній PR); інформаційні операції; психологічні операції; інформування про ситуацію та документування подій на полі бою; розвідувальне забезпечення проведення інформаційних заходів; показ дій військ; введення в оману; безпека операцій; фізичний вплив; протиборство в електромагнітному просторі [3].

Розглянемо більш детально проблематику такої складової стратегічних комунікацій як зв'язки вітчизняних правоохоронних органів із громадськістю.

«Паблік рілейшенз» (public relations – PR), (англ. public – громадський, публічний і relations – відносини, зв'язки) означає «громадські відносини, зв'язки з громадськістю» [4, с. 5]. Для ефективної діяльності правоохоронним органам потрібна підтримка населення, порозуміння, обопільна корисність, обмін інформацією, гуманізація і прозорість дій між правоохоронцями та суспільством, узгодження пропозицій [5, с. 343]. Особливо актуальним питання формування позитивного іміджу державної влади взагалі та правоохоронних органів України зокрема постає в умовах гібридної війни проти України.

Не ставлячи перед собою за мету детальний аналіз поглядів вчених на багатоаспектність категорії гібридної війни, відзначимо лише явно виражені тенденції необхідності формування позитивного іміджу правоохоронних органів в сучасних умовах. Так, аналіз факторів, які об'єктивно впливали на кінцевий результат воєнних конфліктів кінця XX – початку XXI ст., дозволяє стверджувати, що в Першій світовій війні основним чинником досягнення перемоги була вогнева перевага над противником, у Другій світовій війні –

перевага в повітрі, нині запорукою успіху стає перевага в інформаційному просторі. Саме на досягнення перемоги у війні з мінімальними втратами спрямована інформаційна боротьба збройних сил провідних країн світу. З'явилися принципово нові концепції ведення війни, бойових дій, що передбачають завоювання інформаційної та морально-психологічної переваги над противником [6, с. 84].

Усе це стало причиною того, що в засобах масової інформації все частіше з'являються такі поняття, як інформаційна війна, інформаційна агресія, медіа-тероризм. Практично всі збройні конфлікти останніх десятиліть свідчать про ефективність застосування методів і засобів інформаційної боротьби [7].

Основним об'єктом впливу в гібридній війні є не противник, а населення, що "визволяється". Завдання і метод такої війни – спонукання громадян до зради власної держави та підтримки агресора. Важливою особливістю гібридної війни є активне використання асиметричних бойових дій, які характеризуються істотною різницею у військовій силі та стратегіях і тактиках сторін-учасниць. Така схема ведення війни надзвичайно складна для протидії, оскільки немає формальних підстав воювати з країною-агресором, яка лише неофіційно (але надактивно) підтримує бойовиків та терористів [7].

В інформаційно-психологічному протиборстві об'єктами впливу є групи людей та окремі особи. Інформаційно-психологічна складова інформаційної боротьби забезпечує цілеспрямоване створення і поширення спеціальної інформації, яка безпосередньо впливає (позитивно або негативно) на функціонування та розвиток інформаційно-психологічного середовища противника, його політичної і військової складової, а також на психіку та поведінку особового складу військ і населення країни [8].

Як казав Уїнстон Черчилль: «Хто володіє інформацією, той володіє світом». Сьогодні ця фраза набуває дедалі більшого значення, адже, той, хто контролює потоки інформації, контролює і свідомість населення, тому робота органів державної влади повинна бути організована так, щоб вони проводили ефективну інформаційну політику, могли контролювати інформаційний простір, відновити авторитет органів державної влади у проблемних регіонах. Необхідно забезпечити своєчасне оновлення законодавчої бази, яка б відповідала сучасним проблемам суспільства і впроваджувати заходи із формування позитивної репутації держави.

Отже, у сучасних умовах гібридної війни проти України вітчизняні правоохоронні органи повинні використовувати інформацію, перш за все, для підвищення патріотичної налаштованості громадян; посилення авторитету державної влади, Збройних Сил України серед населення; активізації антипропаганди; вивчення громадської думки і формування її в позитивному

напрямку; забезпечення громадського контролю за діяльністю правоохоронних органів; встановлення соціального партнерства з широкою громадськістю; посилення зворотнього зв'язку із суспільством; профілактики та усунення можливих непорозумінь з громадськістю.

Список використаних джерел:

1. Романенко Є. Комунікативна політика держави: теоретико-методологічний аналіз : монографія / Є. Романенко. – Київ : НАДУ, 2014. – 400 с.
2. Указ Президента України № 555/2015 «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». – URL: <http://www.president.gov.ua/documents/5552015-19443>.
3. Ліпкан В. А. Роль стратегічних комунікацій в протидії гібридній війні проти України / В. А. Ліпкан. – URL: <http://goal-int.org/rol-strategichnixkomunikacij-v-protidii-gibridnij-vijni-proti-Ukraini>.
4. Казанчук І. Д. Паблік рілейшнз в діяльності органів внутрішніх справ / І. Д. Казанчук / МВС України; Національний ун-т внутрішніх справ / О.М. Бандурка (ред.). – Х. : Основа, 2003. – 198 с.
5. Гусаров С. М. Адміністративно-юрисдикційна діяльність органів внутрішніх справ : дис. д-ра юрид. наук : 12.00.07. / С. М. Гусаров ; Ін-т законодавства Верховної Ради України. – К., 2009. – 462 с.
6. Нечхаєв С. Інформаційно-військова складова мережоцентричних воєнних дій / С.М. Нечхаєв, О.Л. Голда // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. – 2013. – № 3(49). – С. 84–86.
7. Петров В.В. Актуальні проблеми формування державної інформаційної безпеки у сфері безпеки й оборони. / В.В.Петров. – URL: http://www.niss.gov.ua/public/File/Str_prioritetu/2011_4-21.pdf.
8. Парубій А. Війна Росії проти України і світу / А. Парубій // Українська правда.–2014–URL:<http://www.pravda.com.ua/articles/2014/08/6/7034046/attempt>

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

*Кунєв Ю., д.ю.н., професор, професор
кафедри Національного авіаційного
університету;
Славка А., аспірантка*

ОБ'ЄКТ І ПРЕДМЕТ ІНФОРМАЦІЙНОГО ПРАВА

Без формування сучасної теорії і практики інформаційного права, неможливою видається побудова системи сучасного інформаційного права, права захисного, де захист забезпечений відповідними правовими механізмами, запропонованими теорією та реалізованими у законодавстві та зацементованими теоретичними позиціями.

Кожна наука має свій об'єкт і предмет дослідження. Об'єкт вивчення – той об'єкт, якому, врешті-решт, належать усі характеристики, отримані на різних рівнях породження складного знання, в якому всі вони немовби об'єднуються й проектується [1, с. 107].

У 2008 р. було запропоновано вважати: об'єктом вивчення, проекції, оперування або реальним об'єктом правознавства суспільну діяльність (практику); ідеальним об'єктом – модель або теоретичну модель реального об'єкта, знання про діяльність, пов'язану з правом (теорію) [2].

Основним різновидом суспільної діяльності у інформаційній сфері є інформаційна діяльність, яка потребує правового регулювання і фактично є об'єктом правового регулювання.

Більшість науковців збігаються у думці, що: «Інформаційна діяльність – це сукупність певних дій із застосуванням відповідних способів і методів, пов'язаних зі створенням, одержанням, збиранням, зберіганням, використанням та поширенням, а також охороною та захистом інформації».

Відповідно до ст. 9 Закону України Про інформацію: «Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації» [3].

У інформаційній діяльності за допомогою права можуть визначатися (набувати правової форми) її наступні елементи:

- права та правовий статус суб'єктів;
- дії суб'єктів із перетворення інформації;
- технологія перетворення інформації;
- засоби, за допомогою яких відбувається безпосередній вплив на матеріал діяльності;
- продукт діяльності.

У системі інформаційної діяльності правом одночасно може бути урегульоване матеріал, засіб, норма, технологія, продукт діяльності, й ці комбінації у кооперації різних актів діяльності, де елементом є право, утворюватимуть різні види інформаційної діяльності, які відносять до сфери дії інформаційного права.

Тоді до сфери дії інформаційного права відноситимемо інформаційну діяльність, у якій правом урегульовані хоча б один з перелічених її елементів.

Предметом інформаційного права Кормич Б.А. визначає: «суспільні відносини, що виникають з приводу встановлення режимів та форм обігу інформації, реалізації інформаційних прав і правового статусу суб'єктів інформаційних процесів і формування їх правомірної поведінки і зв'язків» [4].

Такий підхід доцільно застосувати до визначення завдань діяльності, яка потребує правового регулювання у інформаційній сфері (обігу інформації) або інформаційної діяльності.

Виділяють різновиди діяльності, які потребують правового регулювання у інформаційній сфері таким чином: «а) всі види діяльності, пов'язані з інформаційним ресурсом як об'єктом діяльності (продукту інтелектуальної, виробничої, будь-якої іншої соціальної діяльності); б) управління в галузі відносин, пов'язаних з певним інформаційним ресурсом та окремими видами роботи з інформацією; в) використання нових технологій роботи з інформацією – формування і забезпечення сумісності інформаційних систем і систем комунікацій в інформаційних системах та мережах; г) забезпечення безпеки у сфері інформації та інформатизації; д) реалізація юридичної відповідальності в галузі інформації, інформатизації, телекомунікацій» [5, с. 97].

Об'єктом вивчення інформаційного права доцільно вважати інформаційну діяльність, пов'язану з правом, або, іншими словами, теорія й практика правової організації інформаційної діяльності.

Визначення об'єктом правознавства діяльності не суперечить нормативістському підходу до праворозуміння, а поглиблює його, вносячи певні зміни щодо об'єкта “нормування діяльності (як системи) за допомогою нормативно-правових актів”, дозволяє більш системно підходити до дослідження державно-правових явищ і процесів, вийти на нові горизонти щодо організації правової діяльності, використовуючи форми організації діяльності й мислення, викладені в СМД-методології через можливість: формалізувати основні моделі правової практики; дослідити основні зв'язки з іншими видами діяльності, які є визначальними для правової; створювати системи кооперації діяльності, пов'язані з правом, вийти на нові обрії під час досліджень з правової теорії і практики, зокрема використовуючи досягнення праксеології, синергетики, системології тощо [2].

«Предмет державно-правового дослідження – знакова форма частини знань про об'єкт, який утворює ідеальний об'єкт, який заміщає реальний об'єкт, тобто це правова організація діяльності соціальної системи, її механізм, організаційно-правові основи його функціонування та розвитку.

Було визначено, що «категорія «правова організація діяльності» означає упорядкування, узгодження взаємопов'язаних систем норм діяльності й норм права, необхідних для набуття якостей та закріплення закономірностей, які забезпечать результативність і розвиток певної діяльності й відповідної соціальної системи і полягає в організації систем

діяльності з реалізації норм права та організації системи норм, що визначають діяльність.

Правова організація діяльності – це та основа, яка дозволяє по-новому підійти до процесів модернізації соціальних процесів і систем, в якій поєднуються основні підходи до «діяльнісного універсуму», «управління розвитком» та нормування діяльності різного роду в нормах адміністративного права» [6].

Тоді *предметом інформаційного права будемо вважати правові організованості інформаційної діяльності.*

«Подвійне значення інформаційної діяльності виявилось в так званій концепції дуалізму публічного і приватного, яка спочатку застосовувалася щодо сфери засобів масової інформації, але може і в більш широкому розумінні характеризувати ключові принципи регулювання основних видів інформаційної діяльності взагалі» [4, с.238].

Інформаційне право можна поділити за предметами регулювання на діяльність у сфері приватного права та публічного права.

Специфічність сфери публічно-правового регулювання й визначили потребу Шмідта-Ассманна виокремити з інформаційного права інформаційно-адміністративне право, як підгалузь адміністративного [7]. За аналогією можна виокремити сфери інформаційно-публічного та інформаційно-приватного права.

За наведеного підходу до організованостей інформаційної діяльності з використанням технологій IoT, під правове регулювання підпадають такі різновиди діяльності:

- діяльність із створення пристроїв з використанням IoT технологій, які будуть інструментами отримання і передачі даних;
- діяльність із використання інформації, отриманої з використанням IoT технологій для здійснення певної діяльності;
- діяльність із використання пристроїв, що функціонують на основі IoT технології.

Список використаних джерел:

1. Щедровицкий Г. П. Проблемы объекта в системном проектировании / Г. П. Щедровицкий // Вторая всесоюзная конференция по технической кибернетике : тезисы докладов. – М., 1969 // Г. П. Щедровицкий. Избранные труды. – М. : ШКП, 1995. – URL: <http://www.fondgp.ru/gp/biblio/rus/64/>.
2. Кунев Ю. Д. Об'єкт правознавства: системодіяльнісний підхід / Ю. Д. Кунев // Право України. – 2008. – № 3. – С. 35–38.
3. Про інформацію : Закон України, від 02.10.1992, № 2657-XII. – URL : <https://zakon.rada.gov.ua/laws/show/2657-12>.

4. Кормич Б. А. Інформаційне право. Підручник. – Харків: БУРУН і К., 2011. – 334 с.

5. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право / Под. ред. Б. Н. Топорнина. – СПб: Юрид. центр Пресс, 2001.

6. Кунев Ю. Д. Методологія дослідження державно-правових явищ як актуальна проблема / Ю. Д. Кунев // Право України. – 2009. – № 12. – С. 118–123.

7. Шмідт-Ассманн Е. Загальне адміністративне право як ідея врегулювання: основні засади та завдання систематики адміністративного права / Ебергард Шмідт-Ассманн ; [пер. з нім. Г. Рижков, І. Сойко, А. Баканов] ; відп. ред. О. Сироїд. – К. : К.І.С., 2009. – 552 с.

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

Бортник Р., здобувач II рівня вищої освіти, Університет ДФС України

Новицька Н.Б., д.ю.н., доцент кафедри Цивільного права та процесу Університету ДФС України

ПРОБЛЕМИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН В ІНФОРМАЦІЙНОМУ ПРАВІ

Світова глобалізація, інтелектуалізація праці, розвиток та поширення інформаційних технологій (ІТ) призвели до певної віртуалізації економічних та правових відносин. Це створило нову концепцію таких відносин, яка базується на використанні ІТ, різних віртуальних систем та баз даних, які засновані на нематеріальних засобах і створюють відповідні нематеріальні блага, інформацію та трансформують їх в знання. Особливо це стосується сфери інформаційного права, яке регулює різні типи відносин, що стосуються інформації та знань. Актуальності в даній сфері набули технології розподіленої обробки даних. Довгий час такі технології не були досить авторитетними, щоб використовувати їх у правовій діяльності чи застосовувати до них якесь правове регулювання, адже за своєю специфікою вони не впливали на суспільні відносини. Проте з подальшим розвитком даних технологій, виникла технологія розподілених реєстрів, прикладом якої є блокчейн. Блокчейн є технологією, яка швидко впроваджується та стрімко розвивається, здійснюючи вплив на суспільні відносини. Останні пропозиції експертів з даної теми стосуються впровадження блокчейну в фінанси, банківську діяльність, державне управління, оподаткування, земельні відносини та інші сфери, що змушує застосовувати певне правове регулювання з боку держави до даної технології.

На сьогодні питання використання технології блокчейн розглядалися здебільшого іноземними науковцями і в аспекті операцій з криптовалютами. Серед публікацій слід виділити статті таких вчених як Микеш С. [1], Свон М. [2], які досліджували блокчейн у розрізі DLT та використанням «пірингу». Браун Р. [3] досліджував використання блокчейну як бази для існування криптовалюти з економічного та інформаційного аспекту.

Технології розподілених реєстрів (DistributedLedgerTechnology) використовувалися досить давно, але здебільшого на службових комп'ютерах, які не були активні в неробочий час чи вихідні, що не створювало проблем. Розвиток DL-технології був паралельним до розвитку загальної технології побудови комп'ютерних мереж, яка змогла перейти до «пірингової» мережі, відійшовши від стандартного варіанту «клієнт-сервер». Спочатку особливих правових проблем не спостерігалось, проте згодом з'явилися проблеми у захисті інтелектуальної власності при розповсюдженні інформації з використанням «пірингової мережі», що призвело «війни проти торентів», яка і на сьогодні є невирішеною проблемою і в юридичному аспекті також [1, с. 677].

На думку Свон М., розвитку DL-технологій та появі блокчейну сприяв перехід від системи «клієнт-сервер» до однорангового «пірингу», який є основою блокчейну [2, с. 19].

Загалом, блокчейн (англ. blockchain – ланцюг блоків) – розподілена база даних, що зберігає впорядкований ланцюг записів у вигляді блоків, інформація в яких є зашифрованою та обмеженою до доступу. Особливу увагу здобув блокчейн як основа для системи криптовалют, найвідомішою з яких є «Біткоін». Криптовалюта є найбільш захищеною віртуальною валютною системою світу. Електронний вплив заради викрадення даної валюти повинен бути здійснений на рівні кінцевого користувача, а не на рівні обміну даних. Такий криптозахист зробив з даних валют певне «цифрове золото» для інвесторів.

Поняття «блокчейн» та «біткоін» у засобах масової інформації (ЗМІ) використовуються як синоніми. Хоча і увага ЗМІ зосереджена здебільшого на біткоїні, адже за рік свого існування капітальний розмір біткоїн-індустрії становив 35 мільярдів доларів США. Такий швидкий ріст свідчить про спекулятивний характер біткоїн торгівлі. Також сам характер торгівлі не є державно регламентований, а біткоїн як валюта не емітується жодною з країн проте є об'єктом для вільного обміну на валюти інших країн на відповідних біржах [3].

Законодавство країн світу здебільшого не має вагомих актів, що регулюють відносини з використанням криптовалюти. Наприклад, в Ісландії

криптовалюта, відповідно до Закону про валютну біржу, повністю заборонена; відповідно до Німецького закону про банки, криптовалюта є фінансовим інструментом; Центральний банк Фінляндії класифікує програмним забезпеченням, яке виступає товаром; Податкова адміністрація Норвегії визнає криптовалюту активом; Законом про валютне регулювання Японії криптовалюта виконує функцію валюти, але не грошової одиниці. В Білорусії внесено зміни до Декрету Президента №8 «Про розвиток цифрової технології», в якому діяльність, пов'язана з обігом криптовалюти є законною, не потребує ліцензування, звільняється до 2023 року від оподаткування. Сама криптовалюта є законним платіжним засобом за згодою обох сторін угоди.

В Україні існує Проект Закону України «Про обіг криптовалюти в Україні», в якому регламентовано діяльність, пов'язану з використанням блокчейн-технології та криптовалюти. До операцій з криптовалютою застосовуються загальні положення про договір міни (ст. 715, 716 ЦКУ), діяльність не потребує ліцензування, операції є об'єктом оподаткування, криптовалюта не може бути використана проти основ національної безпеки. За порушення даного Закону передбачена цивільно-правова, адміністративна або кримінальна відповідальність. Проте 29.08.2019 законопроект був відхилений [4].

Технологія блокчейну знаходиться у тісній взаємодії з криптовалютами, які здійснюють суттєвий вплив на суспільні відносини, що відповідно породжує юридичні проблеми, які потребують державного регулювання.

Першою проблемою є необхідність ліцензування даного виду діяльності. Звісно у демократичних країнах діяльність приватних осіб, що не порушує закон є легальною, тобто операції стосовно криптовалют дозволів не потребують, бо здійснюються між приватними особами. Проте з'являється аспект стосовно юридичного вирішення їхніх цивільно-правових спорів. А ліцензування обігу криптовалют з боку держави необхідне, адже криптовалюта вже є певним аналогом звичайної національної валюти проте з певним інформаційним характером. Ліцензування необхідне заради протидії шахрайству та інших злочинів, наприклад, легалізація доходів через криптовалюту чи фінансування тероризму таким способом.

Другою проблемою є оподаткування операцій з криптовалютами. Під час таких операцій виникає прибуток: як активний – від продажу, так і пасивний – внаслідок збільшення вартості. В більшості держав існують податки, які можна застосувати до даних ситуацій, а якщо немає, то можна створити нові.

Третьою проблемою є визнання криптовалюти як грошей. Так у таких країнах як Бангладеш, Таїланд, Болівія та В'єтнам криптовалюта є

забороненою, але операції стосовно її обігу не є криміналізованими. Основним питанням в даній ситуації є те, що криптовалюта як аналог світової валюти не має чітко встановленої вартості та емітента через що в операціях пов'язаних з її обміном вона розцінюється на рівні дорогоцінного металу, що змушує вважати такі операції юридично як бартер.

Зважаючи на все вище написане, можна стверджувати, що держава повинна юридично врегулювати аспекти використання технології блокчейну. Особливу увагу повинно звернути на те що дана технологія пов'язана з криптовалютою, а тому повинна регулюватися на основі даного аспекту. Першими кроками повинні стати регулювання інформаційно-правового аспекту, зокрема у визначенні статусу криптовалюти та характеру операцій з нею. Наступними діями держави повинні бути ліцензування та юридичне вирішення спірних цивільно-правових аспектів даної діяльності. Ліцензування необхідне заради забезпечення безпеки даних операцій та їхньої легальності. Також можна звернути увагу і на податкове законодавство, додавши зміни відповідно операцій з криптовалютою. В будь-якому випадку впровадження технології блокчейн на державному рівні потребує суттєвого оновлення законодавства заради вирішення відповідних правових проблем.

Список використаних джерел:

1. KshemkalyaniAjay, MukeshSinghalDistributedComputing. Principles, AlgorithmsAndSystems. Cambridge: UniversityPress, 2008. 756 p.
2. Swan Melanie. Blockchain: Blueprintfor a NewEconomy. Sebastopol CA: O'ReillyMedia. 2015. 152 p.
3. RichBryan. IsBitcoinA Bubble? Forbes: Веб-сайт. URL: <https://www.forbes.com/sites/bryanrich/2017/05/25/why-the-bitcoin-bubble-could-be-dangerous/#2ca5578e11bd>. Дата звернення: 10.11.2019.
4. Проект Закону про обіг криптовалюти в Україні. Верховна рада України: веб-портал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684. Дата звернення: 10.11.2019.

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

*Процишен М., к.ю.н., доцент кафедри
адміністративного права і процесу ДВНЗ
«Київський економічний університет імені
Вадима Гетьмана»*

ЕЛЕКТРОННА КОМЕРЦІЯ З ТОЧКИ ЗОРУ ТЕЛЕКОМУНІКАЦІЙНОГО ПРАВА

В умовах становлення цифрової економіки дедалі більшого розвитку набуває електронна комерція. Так, до кінця 2019 року загальний обсяг

продажів інтернет-магазинів у всьому світі, за прогнозами, повинен досягти позначки в 2 трильйони доларів США. Зростання, порівняно з 2017 роком, складе 6 % [1].

З огляду на важливість електронної комерції для подальшого розвитку інформаційного суспільства чимало науковців, зокрема О.В. Мельник, Т.В. Марусей, С.С. Нестеренко, Ю.О. Володько, В.С. Мілаш розглядали економічні, технічні, правові та інші аспекти комерційної діяльності з використанням мережі Інтернет. Разом з тим, бракує погляду на електронну комерцію з точки зору телекомунікаційного права як інституту інформаційного права.

В широкому розумінні електронна комерція (від англ. Electronic commerce) — це сфера цифрової економіки, що включає всі фінансові та торгові транзакції, які проводяться за допомогою комп'ютерних мереж, та бізнес-процеси, пов'язані з проведенням цих транзакцій. До електронної комерції відносять електронний обмін інформацією (Electronic Data Interchange, EDI), електронний рух капіталу (Electronic Funds Transfer, EFS), електронну торгівлю (E-Trade), електронні гроші (E-Cash), електронний маркетинг (E-Marketing), електронний банкінг (E-Banking), електронні страхові послуги (E-Insurance), тощо [2]. Однак, зовсім інше питання чи можна вважати всі ці види господарської діяльності електронною комерцією в юридичному сенсі.

Незважаючи на наявність низки нормативно-правових актів, які в тій чи іншій мірі фрагментарно регулювали питання організації електронної комерції протягом досить тривалого часу в Україні не було законодавчого акту, який би був повністю присвячений електронній комерції. Як вірно свого часу зазначила В.С. Мілаш, пасивне ставлення вітчизняного законодавця до вирішення питань належного правового забезпечення електронної комерції призвело до гальмування процесу цивілізованого розвитку електронного ринку, адаптованого до сучасних світових умов [3, с.147].

Істотним проривом у питанні щодо врегулювання діяльності підприємств на ринку Інтернет-послуг стало прийняття Закону України “Про електронну комерцію” [4; 5, с.1012]. Водночас слід звернути увагу на те, що попри свою назву цей закон регулює далеко не всі види комерційної діяльності, що здійснюються за допомогою комп'ютерних мереж (електронної комерції).

Так, відповідно до ст.1 цього закону його дія поширюється на відносини у сфері електронної комерції під час вчинення електронних правочинів. При цьому під електронною комерцією розуміються відносини, спрямовані на отримання прибутку, що виникають під час вчинення правочинів щодо

набуття, зміни або припинення цивільних прав та обов'язків, здійснені дистанційно з використанням інформаційно-телекомунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов'язки майнового характеру. Отже, по-суті, головна мета цього закону – врегулювати вчинення електронних правочинів за допомогою інформаційно-телекомунікаційних систем під час будь-якої комерційної діяльності.

Однак, цим же законом встановлені певні обмеження щодо сфери його застосування. Так, відповідно до положень частини другої ст. 1 дія цього закону не поширюється на правочини, що стосуються грального бізнесу, у тому числі парі, тоталізатори та інші азартні ігри, або проведення лотерей, крім не грошових лотерей відповідно до Закону України "Про благодійну діяльність та благодійні організації" та лотерей, визначених Законом України "Про рекламу". Крім того, відповідно до частини другої ст.2 закону України "Про електронну комерцію" порядок надання банківських послуг, випуск та обіг електронних грошей, здійснення переказу коштів не є предметом правового регулювання цього закону і регулюється спеціальним законодавством. До послуг систем дистанційного обслуговування, випуску та обігу електронних грошей, страхування та інших послуг, щодо яких існує спеціальне законодавство, Закон України "Про електронну комерцію" застосовується лише в частині правочинів, вчинених в електронній формі, яка не суперечить спеціальному законодавству, що регулює здійснення послуг із дистанційного обслуговування, випуск та обіг електронних грошей, страхування. Іншими словами, такі види комерційної діяльності як електронний гральний бізнес, електронний банкінг, електронне страхування фактично випадають з поняття електронної комерції в розумінні Закону України "Про електронну комерцію". Отже, в юридичному сенсі електронна комерція в Україні звужується переважно до електронної торгівлі.

У цьому зв'язку слід відзначити, що в Україні саме електронна торгівля поки що залишається основним напрямом електронної комерції. Активний розвиток електронної торгівлі пояснюється тим, що цей вид підприємницької діяльності дозволяє зменшити операційні затрати, а також мінімізувати ризики завдяки розвитку платіжних систем та способів доставки товарів. Дистанційна торгівля дозволяє накопичувати інформацію про продажі та про клієнтів, що дає можливість удосконалити бізнес-процеси, а це є передумовою успішного ведення бізнесу [6, с.33]. Очевидно ці обставини і вимусили законодавця врегулювати в Законі України "Про електронну комерцію" в першу чергу ті суспільні відносини, що пов'язані саме з електронною торгівлею.

Так чи інакше, Закон України "Про електронну комерцію" є системоутворюючим законодавчим актом для цифрової економіки, хоча б

тому, що ним визначаються базові поняття та процедури використання інформаційно-телекомунікаційної інфраструктури в цілях електронної комерції. Серед них слід виділити, зокрема такі терміни як “інформаційні електронні послуги”, “інтернет-магазин”, “комерційне електронне повідомлення”, “мережевий ідентифікатор”, “одноразовий ідентифікатор”, “послуга проміжного характеру в інформаційній сфері”, “реалізація товару дистанційним способом”. Хоча в цілому Закон України “Про електронну комерцію” спрямований на врегулювання вчинення та виконання електронних правочинів, тобто має цивілістичний характер, наведена термінологія є більше характерною для телекомунікаційного права, що є частиною інформаційного права. Це зумовлено тим, що в основі здійснення електронних транзакцій лежить використання інформаційно-телекомунікаційних систем. Тому юридична специфіка дистанційного способу вчинення електронних правочинів в свою чергу зумовлена технічними особливостями функціонування інформаційно-телекомунікаційних систем.

Правове регулювання створення, використання і розвитку телекомунікацій, зокрема інформаційно-телекомунікаційних систем, є завданням телекомунікаційного права. Як інститут інформаційного права телекомунікаційне право має комплексний характер в тому сенсі, що регулює відносини щодо використання засобів телекомунікацій як за допомогою імперативного, так і за допомогою диспозитивного методів правового регулювання. Тому цілком природньо, що відносини у сфері електронної комерції в частині використання інформаційно-телекомунікаційних систем для здійснення електронних транзакцій, входять до предмету правового регулювання телекомунікаційного права. Це жодним чином не суперечить цивільно-правовій природі правовідносин, пов'язаних із вчиненням електронних правочинів дистанційним способом, враховуючи, знову ж таки, комплексну природу телекомунікаційного права, яке об'єднує в собі норми різних галузей права адміністративного, цивільного та ін.

Підсумовуючи викладене, необхідно зазначити, що на сьогодні з точки зору телекомунікаційного права як інституту інформаційного права електронну комерцію слід розглядати як сукупність врегульованих переважно диспозитивним методом суспільних відносин, що складаються у зв'язку з вчиненням та виконанням електронних правочинів за допомогою інформаційно-телекомунікаційних систем насамперед у сфері електронної торгівлі.

В подальшому варто зосередити увагу на правових аспектах процедури вчинення електронних правочинів.

Список використаних джерел:

1. Цікаві факти про інтернет-торгівлю в світі в 2019 році // <https://lemarbet.com/ua/razvitie-internet-magazina/interesnye-fakty-ob-internet-torgovle/>
2. Мельник О.В. Електронна комерція як складова частина електронного бізнесу // <http://intkonf.org/melnik-ov-elektronna-komertsiya-yak-skladova-chastina-elektronnogo-biznesu/>
3. Мілаш В.С. Деякі аспекти правового регулювання торговельної діяльності з використанням мережі Інтернет // Вісник господарського судочинства. – 2015. – № 1. – С.139-148
4. Закон України “Про електронну комерцію” від 03.09.2015 р. № 675-VIII// Відомості Верховної Ради. – 2015. – № 45. – Ст.410
5. Марусей Т.В. Основні тенденції розвитку ринку електронної комерції в Україні // Економіка і суспільство. – 2018. – №14. – С.1011-1015
- Нестеренко С.С., Володько Ю.О. Поява та розвиток дистанційної торгівлі // Економіка, фінанси, право. – 2015. – №7/1. – С.31-33

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

*Рєпіна Є., Устименко О., студентки
Національного авіаційного університету*

ПРАВОВИЙ СТАТУС КРИПТОВАЛЮТИ У СВІТІ

Мало хто задається питанням в повсякденному житті - що таке гроші? Ними користуються щодня, багато говорять і думають про них, але не можуть адекватно пояснити їх сутність. Історично склалося так, що практично скрізь грошима централізовано завідують держави через центральні держбанки, починаючи від їх випуску і закінчуючи правилами поведінки, деномінації і утилізації. Безсумнівно, в цьому є позитивна сторона, але існує і негативна. Ті, кого ці негативні моменти не влаштовують, як правило, не в змозі що-небудь змінити в кращу сторону, тому що це може бути протиправно. При цьому потрібно розуміти, що правові норми вторинні щодо соціальних, які, в свою чергу, з'являються у зв'язку з тими чи іншими явищами, що виникають, по суті, в правовому вакуумі. Так було з появою радіо, автомобілів, Інтернету і багатьма іншими досягненнями науково-технічного прогресу. Те ж саме відбувається зараз з новими альтернативними грошима - криптовалютою - породженнями інноваційних блокчейн технологій. Криптовалюта виникла на стику економіки, криптографії та ідеології. Біткоіни став першою з них, так би мовити, не ініціативою будь-якої держави, а звичайних за своїм статусом людей.

Перед державами стоять нові завдання, пов'язані з проблематичністю регулювання криптовалютних операцій і інших породжень блокчейн

технологій, використанням позитивних сторін з допустимими ризиками, встроюванням цих блокчейн-інновацій в поточну фінансову і правову системи. Заборона або дозвіл, як і повне ігнорування, - лише відмова від відповідальності.

У цьому контексті серйозні зміни очікують не тільки так званий «суспільний договір», а й міжнародну правову систему в цілому. І саме децентралізовані блокчейн-системи є одним з ключових інструментів на шляху до цих незворотних еволюційних змін. Одним з питань держструктур по всьому світу є проблема створення оптимального правового фундаменту для ринку криптовалют [1].

У випадку з окремими країнами історичний зріз яскраво ілюструє повну нездатність більшості держав адекватно і компетентно реагувати на ІТ-інновації та науково-технічну революцію. Єдиної позиції немає ні в одній державі, ключові питання залишаються без відповідей, що створює додаткові проблеми в правовому застосуванні. Через це підвищуються запити соціуму на захист приватності і конфіденційності.

Правовий статус криптовалюти істотно відрізняється в різних країнах. У ряді країн офіційно дозволені операції з криптовалютою. Зазвичай вони розглядаються як товар або інвестиційний актив, і для цілей оподаткування підпорядковані відповідним законодавством. У Німеччині біткоїн визнають в якості розрахункової грошової одиниці, в Японії біткоїн є законним платіжним засобом з податком на покупку.

В даний час в світі відсутній нормативно-правова база, що встановлює еталонні правила, що регулюють проведення криптовалютних операцій. З цього випливає, що немає і механізмів правового захисту як інвесторів, так і осіб, що емітують криптовалюту. Зараз в деяких країнах вже йдуть спроби включення криптоінвестування в правове поле і надання криптовалюті офіційного статусу. Можна розглянути ці спроби в створенні умов регулювання нового інструменту фінансування. Так, в Швейцарії в кінці 2016 року було анонсовано розробка правил, які дозволять залучати до 1 млн швейцарських франків без зобов'язань надання звітності регулятору ринку цінних паперів, що може привернути відповідні компанії.

У стадії розробки власних законодавчих правил регулювання знаходиться Сингапур. Він, як і Китай, довго не звертав уваги на те, що відбувається, поки це не торкнулося його громадян і розробки фінансових заходів боротьби з відмиванням грошей. Показовим прикладом є Японія, яка першою з країн прирівняла цифрові гроші до реальних грошей, легалізувала криптобіржі шляхом розробки правил їх діяльності та, як наслідок, створила базис, але не системний еталон для процедур подібних операцій [2].

Приклад цих країн показав, що визначення правового статусу криптовалюти і процесів первинного розміщення монет створює гарантії для учасників і гравців самого ринку. Звичайно, відсутність правового регулювання надає свободу, проте залучення серйозних гравців потребуватиме певних законодавчих і правових гарантій.

Участь у криптовалютному ринку громадян таких держав, як США, Сингапур, а тепер уже Китай і ряду інших автоматично тягне поширення відповідної юрисдикції. У будь-якому випадку, не варто забувати, що робота в рамках відповідної юрисдикції, який би сприятливою вона не була, тягне за собою застосування норм відповідальності, встановлених цією юрисдикцією[2].

Національний Банк України не визнає криптовалюту ні в якості електронних грошей, ні грошових сурогатів, ні в якості інших законних засобів платежу, але не забороняє використання криптовалюти.

Восени 2017 року група нардепів від НФ і БПП подала в парламент законопроект про обіг криптовалюти в Україні. Він визначає, що криптовалюта - це "програмний код, який може виступати засобом міни". Закон передбачає створити криптовалютні біржі, а з боку держави контролювати обмін буде Нацбанк. Проте в серпні 2019 року проект був відкликаний [3].

У другому законопроекті, який подав у ВР голова комітету з питань фінполітики Сергій Рибалка, дається інше визначення криптовалюти: "децентралізований цифровий вимір вартості, що може бути виражений в цифровому вигляді та функціонує як засіб обміну, збереження вартості або одиниця обліку, що заснований на математичних обчисленнях, є їх результатом та має криптографічний захист обліку.". Прописано там і створення криптобіржі - нею може стати будь-яка фінансова установа, статутний капітал якого не менше 5 млн грн. Засновниками кібербірж, згідно із законопроектом, можуть стати держоргани, пересічні українці і навіть іноземці. При цьому мінімум 51% статутного капіталу повинно належати громадянам України. Для управління ринком цифрових грошей пропонується створити окремий державний орган, який буде видавати ліцензії криптобіржам і криптообмінникам, а також регулювати їх роботу [4].

Поки йдуть регуляторні дискусії в Україні вже з'явився власний «криптокарбованець» (Karbo) - децентралізована однорангова пірінгова обмінна мережа, яка не має централізованого управління і емітента, забезпечує конфіденційність і анонімність операцій без посередників і регуляторів. "Карбованець" - це криптографічно захищена (зашифрована) інформація, а карбованці - це одиниці обміну, тобто одиниці інформації. Вони захищені від

копіювання та підробки технологією блокчейн нового покоління на основі протоколу Cryptonight [5].

Можна зробити висновок, що існує ризик пов'язаний з законодавством про протидію відмиванню коштів, одержаних злочинним шляхом. Необхідно бути готовим до того, що надходження грошових коштів, особливо від фізичних осіб, потребують пояснень їх легального походження. Відповідно будь-якому проєкту необхідно враховувати цей аспект при первинному розміщенні монет. Однак наявність законодавства про протидію відмиванню коштів, одержаних злочинним шляхом, і відсутність законодавчого регулювання криптовалютних процесів швидше створюють ґрунт для зловживань контролюючими органами, але не створюють перешкод для відмивання.

Список використаних джерел:

1. The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT – URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp1_50128en.pdf

2. Запуск криптовалюти в Сингапуре: опыт запуска и достоинства юрисдикции. – URL: <https://internationalwealth.info/offshore-investments-abroad/launch-cryptocurrency-singapore-experience-and-benefits-jurisdiction/>

3. Проект Закону про обіг криптовалюти в Україні. – URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684

4. Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні. – URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710

5. Електронний карбованець. – URL: <https://karbo.io/ru/>

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

***Текєджанова К., студентка
Національного авіаційного
університету***

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ КРИПТОВАЛЮТ В УКРАЇНІ

Беззаперечно, що ХХІ століття – це століття інформаційних технологій. Процеси глобалізації, динамічний розвиток інтернет-ринку, розвиток інформаційних технологій призводить до появи нових інститутів, фінансових інструментів та нових форм взаємодії в суспільстві. Одним із таких напрямів є обіг криптовалюти.

Доречно зауважити, що Україна входить в десятку світових країн за рейтингом користування біткойн-гаманцями. При тому ж, Україна посіла 4-те місце за кількістю відвідування сайту Blockchain.info [4].

Однак, станом на сьогодні правовий статус криптовалюти в Україні, операцій з нею та оподаткування не визначений, тому, що методологічна та юридична база регулювання відсутні, як наслідок маємо, компанії які здійснюють криптовалютну діяльність офіційно не зареєстровані, та не прогнозовані дії органів державної влади та контрагентів у відносинах із суб'єктом ринку криптовалюти створюють перепони у криптовалютній діяльності. Зокрема, це ризики визнання даної діяльності незаконною, проблеми із банківським обслуговуванням, невизнання смарт-контрактів тощо.

Так, були здійснені спроби законодавчого врегулювання відповідної сфери, зокрема, у Верховній Раді України було зареєстровано Проект Закону про обіг криптовалюти в Україні № 7183 від 06.10.2017 [1].

Крім того, у 2014 році Національний банк України (далі – НБУ) у своєму документі «Роз'яснення щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» Bitcoin» зробив першу спробу визначити правовий статус, який був прирівняний до грошового сурогату, але вже у 2018 році НБУ дійшов висновку, що криптовалюта не може бути визнана грошовим сурогатом, залишивши біткоїн у сірій зоні українського законодавства (Лист від 22.03.2018 р. №40-0006/16290).

Державна фіскальна служба Україна (далі — ДФС) у своїй ІПК від 25.01.2019 р. №282/К/99-99-13-01-02-14/ІПК «Щодо порядку оподаткування доходів деяких операцій» дублює позицію НБУ, Національної комісії з цінних паперів та фондового ринку і Національної комісії, що здійснює регулювання у сфері ринків фінансових послуг. ДФС зазначає, що «природа криптовалют не дозволяє визнати їх ні грошовими коштами, ні валютою і платіжним засобом іншої країни, ні валютною цінністю, ні електронними грошима, ні цінними паперами, ні грошовим сурогатом». Також ДФС повідомляє, що оскільки порядок оподаткування операцій з криптовалютою не встановлений нормами податкового законодавства, то надання індивідуальної податкової консультації з питань практичного застосування вказаних вище норм є неможливим [3].

Проблема правової регламентації обігу криптовалют, що породжена сучасним глобалізованим світом, має досить складний комплексний характер. Намагання вирішити її традиційними способами є марними, враховуючи соціально-економічні фактори сучасного глобалізованого світу та конфлікти юрисдикцій і застосування національного права різних країн до відносин, які виникають під час обігу криптовалют.

Водночас, значний суспільний інтерес до проблеми зумовлює необхідність пошуку адекватного механізму правового регулювання, оскільки існуючі способи саморегулювання не захищають права власності та законних інтересів.

У цьому випадку доречно погодитися з думкою Дороніна І.М., який зазначає, що державний вплив на відносини, що складаються у сфері обігу криптовалют, має відбуватись у певних зонах впливу, до яких можливо віднести наступні:

- зона регламентації обігу криптовалюти на біржах та її використання у платіжних системах;
- зона відповідальності за збереження криптовалюти (насамперед, шляхом технічного захисту інформації);
- зона застосування криптовалют для спільного інвестування;
- зона використання криптовалют у цивільно-правових відносинах.

Окрім цього, повинні бути розроблені ефективні міждержавні механізми взаємодії у сфері обігу криптовалют насамперед в інтересах протидії злочинності та юридичної відповідальності за вчинення правопорушень економічного характеру (зокрема, фінансового шахрайства) [2, с. 92].

Таким чином, Україна потребує відповідне законодавство у сфері обігу криптовалют, так як будь-яка діяльність, що не має чітко визначених правил, не особливо приваблива для інвесторів і підприємців. Тому, важливо, щоб закон не обмежував інновації. Також слід пам'ятати, що нові напрямки в блокчейн-технологіях можуть бути безпосередньо і не пов'язані з криптовалютою, але наприклад, фінансування таких проектів буде пов'язано з зазначеною сферою.

Список використаних джерел:

1. Про обіг криптовалют в Україні: проект Закону України № 7183 від 06.10.2017 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684
2. Доронін І.М. Криптовалюти: соціально-економічні фактори, право та функції держави. Інформація і право. 2017. № 3. С. 85-93.
3. Загрядська М. Криптовалюти в Україні URL: <http://yur-gazeta.com/publications/practice/podatкова-praktika/kriptovalyuti-v-ukrayini.html>
4. Кубай В.В. Чим є криптовалюта в Україні? Проблеми правового регулювання криптовалют URL: <http://aphd.ua/publication-569/>

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

***Маньгора В. В., к.пед.н., доцент,
професор кафедри права ПрАТ «ВНЗ
«МАУП» Вінницький інститут***

ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ГОСПОДАРСЬКИХ ДОГОВОРІВ

Розвиток торгівлі, збуту промислової продукції, постачання господарюючим суб'єктам необхідної сировини, матеріалів й устаткування, надання фізичним і юридичним особам різноманітних послуг у сфері

обслуговування потребує регулювання договірних відносин, господарський договір є основним правовим документом, який регулює відносини сторін, учасників господарських правовідносин та є однією з основних підстав виникнення господарських зобов'язань.

З метою удосконалення нормативно-правового регулювання електронного документообігу з метою наближення умов його застосування до документообігу на паперових носіях Верховна Рада України прийняла 5 жовтня 2017 р. Закон України «Про електронні довірчі послуги»[1]. Закон України «Про електронний цифровий підпис» втратив чинність [2].

7 листопада 2018 р. в Україні набув чинності Закон України «Про електронні довірчі послуги», який передбачає: якщо відповідно до законодавства на паперовому документі не потрібен власноручний підпис сторін, при електронному документообігу можна використовувати електронні дані або ж ні - за домовленістю сторін.

Прийняття Законів України «Про електронну комерцію» та «Про електронні довірчі послуги», внесення змін до діючих нормативно-правових актів значно розширило можливості суб'єктів господарювання використовувати в своїй діяльності електронні господарські договори. Проте, інформаційно-телекомунікаційні системи постійно розвиваються і потребують прийняття нових підзаконних нормативно-правових актів для повноцінного впровадження Законів України «Про електронну комерцію» та «Про електронні довірчі послуги» та внесення змін до них.

Основними законодавчими актами, що регулюють відносини щодо електронних договірних відносин в господарюванні є Господарський кодекс України від 16 січня 2003 р., Цивільний кодекс України від 16 січня 2003 р. та Закон України «Про електронну комерцію» від 26 квітня 2017 р.

Відповідно до п. 5 ч. 1 ст. 5 Закону України «Про електронну комерцію» електронний договір - домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав і обов'язків та оформлена в електронній формі [3].

В сучасній правовій науці існують різні точки зору щодо форми електронних договорів. Одні поділяють думку західних вчених, що електронна форма правочину є окремою формою правочину. На думку представників іншої позиції, зокрема І. Спасибо-Фатєєвої, А. Чучковської та О. Гудзь, правочин, вчинений з використанням електронних засобів зв'язку, є різновидом письмової форми [4].

Згідно з ч. 1 ст. 181 Господарського кодексу України господарський договір за загальним правилом викладається у формі єдиного документа, підписаного сторонами та скріпленого печатками. Допускається укладення

господарських договорів у спрощений спосіб, тобто шляхом обміну листами, факсограмами, телеграмами, телефонограмами тощо, а також шляхом підтвердження прийняття до виконання замовлень, якщо законом не встановлено спеціальних вимог до форми та порядку укладення даного виду договорів [5].

Закон України «Про електронну комерцію» доповнив частину другу статті 639 Цивільного кодексу України абзацом другим такого змісту: «Якщо сторони домовилися укласти договір за допомогою інформаційно-телекомунікаційних систем, він вважається укладеним у письмовій формі». Відповідно до ст. 205 Цивільного кодексу України правочин може вчинятися усно або в письмовій (електронній) формі. Стаття 207 Цивільного кодексу України визначає що правочин вважається таким, що вчинений у письмовій формі, якщо його зміст зафіксований в одному або кількох документах (у тому числі електронних), у листах, телеграмах, якими обмінялися сторони [6]. Отже, Господарський кодекс України та Цивільний кодекс України, визначають, що договори укладені в електронній формі, є такими, що укладені у письмовій формі. Проте, на нашу думку, потрібно електронні договори винести в окрему групу договорів, так як вони мають свої особливості укладання і відрізняються від усних та письмових договорів. Вирішення даної проблеми буде зумовлено правозастосовною практикою, яка вимагає чіткого механізму регулювання господарських електронних договорів при вирішенні питань щодо спорів між особами, що уклали електронний договір.

Винесення електронних договорів в окрему групу договорів передбачає внесення змін до Цивільного кодексу України. Для цього необхідно Ч.1 ст. 205 Цивільного кодексу України викласти в такій редакції: «Правочин може вчинятися усно, в письмовій, електронній формі. Сторони мають право обирати форму правочину, якщо інше не встановлено законом». Виділення електронних договорів в окрему форму дасть можливість чітко визначити істотні умови договору, зменшить кількість випадків коли договір визнається неукладеним або недійсним.

Список використаних джерел:

1. Про електронні довірчі послуги»: Закон України від 5.10.2017 р. № 2155-VIII *Відомості Верховної Ради України*. 2017. № 45. Ст. 400.
2. Про електронний цифровий підпис»: Закон України від 22.05.2003 р. *Відомості Верховної Ради України*. 2003. № 36. Ст. 236.
3. Про електронну комерцію»: Закон України від 03.09.2015 р. № 675-VIII. *Відомості Верховної Ради України*. 2015. № 45. Ст. 410.
4. Жуткова С.М. Особливості укладання угод через мережу Інтернет. *Молодий вчений*. 2017. № 11(51). листопад. - С. 876.

5. Господарський кодекс України: Закон України від 16.01.2003 р. № 436-IV *Відомості Верховної Ради України*. 2003. № 18, № 19-20, № 21-22. Ст. 144.

6. Цивільний кодекс України: Закон України від 16.01. 2003 р. № № 435-IV *Відомості Верховної Ради України*. 2003. №№ 40-44, Ст. 356.

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

*Високос В. Р., магістр кафедри ІППІВ
КПІ ім. Ігоря Сікорського*

*Науковий керівник: Яшарова М. М.,
доцент кафедри ІППІВ КПІ ім. Ігоря
Сікорського, к.т.н., с.н.с.*

КОМП'ЮТЕРНА ПРОГРАМА ЯК ОБ'ЄКТ ІНТЕЛЕКТУАЛЬНОГО ВЛАСНОСТІ

Судові спори у сфері інтелектуальної власності є складними тому що мають у наявності специфічний об'єкт, сторони, методи доказування. Також комп'ютерні програми можуть складатися з декількох об'єктів авторського, інтелектуального та патентного права (музика, зображення, алгоритми, комп'ютерні коди). Зважаючи на вище викладене в Україні вводиться Вищий суд з питань інтелектуальної власності, який розглядатиме справи цієї категорії.

У Законі України «Про авторське право та суміжні права» у статті 1 сказано «Комп'ютерна програма - набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах)»

У законодавстві сказано що комп'ютерна програма захищається як літературний твір однак не всі науковці погоджуються з цим. На нашу думку, порівняння комп'ютерних програм із літературними творами є не зовсім коректним. На відміну від літературних творів, текст комп'ютерної програми (вихідний чи об'єктний код) не мають самостійної цінності без можливості їх застосування в комп'ютері. Отже, сприйняття комп'ютерної програми, тобто власне кажучи її тексту, відбувається не безпосередньо людиною, а опосередковано, за допомогою комп'ютера С. Петренко²³

²³ Петренко С. А. Правова охорона комп'ютерної програми як об'єкта інтелектуальної власності: шляхи розвитку / С. А. Петренко [Електронний

зауважує, що порівняльний аналіз такого об'єкта авторського права як комп'ютерна програма, з таким класичним об'єктом авторського права як літературний твір, надає змогу зробити висновок про те, що програма також характеризується змістом, внутрішньою та зовнішньою формами. При цьому елементи змісту, внутрішньої та зовнішньої форм не є сталими і залежать від виду та призначення комп'ютерної програми. Програма прикладного характеру подібна до літературного твору наукового жанру, а ігрового характеру – до мультимедійних творів.²⁴ Погоджуємося з думкою В. Дмитришина, який вказує, що вибір на користь авторського права для правової охорони комп'ютерних програм пояснюється тим, що найбільш високий рівень охорони в умовах масового виробництва програм може дати тільки визнання комп'ютерних програм об'єктом захисту як результату творчої діяльності, тобто як об'єкту авторського права.²⁵

Автор наводить фактори, що свідчать про належність комп'ютерних програм до об'єктів авторського права:

- вихідний текст комп'ютерної програми має риси письмового літературного твору (подібність з літературним твором доповнює й те, що текст комп'ютерної програми може бути написаний різними мовами програмування – Асемблері, С++, Java, Паскалі, Qbasic тощо, як і будьякий літературний твір – українською, російською, англійською чи іншою мовами);

- алгоритми, методи, ідеї, теорії, формули, використані при розробці комп'ютерної програми, додають їй риси наукового твору, тобто галузеву належність до об'єктів авторського права;

- аудіовізуальні відображення, анімація і графіка, створювані комп'ютерною програмою, мають риси музичного (з текстом і без тексту), аудіовізуального, твору образотворчого мистецтва, твору, виконаного способами, подібними до фотографії, художнього твору, що також дає підстави віднести їх до творів у галузі мистецтва.

ресурс]. – Режим доступу: http://irbis-nbuv.gov.ua/cgibin/irbis64r_81/cgiirbis_64.exe?C21COM=2&I21DBN=AD&P21DBN=ARD&Z21ID=&Image_file_name=DOC/2010/10psavsr.zip&IMAGE_FILE_DOWNLOAD=1

²⁴ Закон України «Про авторське право і суміжні права» Закон від 26.04.2017 № 3792-12 // База даних «Законодавство України» / ВР України. [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/3792-12>

²⁵ Дмитришин В. С. Інтелектуальна власність на програмне забезпечення в Україні / В. С. Дмитришин, В. І. Березанська. – К.: Вірлен, 2005 – 304 с.

Авторське право на комп'ютерну програму не поширюється на закладені в ній ідеї, процеси, методи діяльності або математичні концепції як такі, на яких базується комп'ютерна програма (включаючи сполучення, іншими словами, авторським правом захищається текст (код) програми, а не функції, які вона виконує. Для усунення цього недоліку авторського права останнім часом усе частіше й частіше в Україні подаються заявки на отримання патенту на винахід (корисну модель) із метою охорони й захисту алгоритму (способу) роботи комп'ютерної програми щодо розв'язання конкретної задачі. Патент на винахід дозволяє захистити змістовий бік програмного забезпечення, патентна охорона поширюється на сутність, утілену в алгоритмі, яка є основною ідеєю програми. Крім того, патент дає виключне право власності на саму ідею (якщо вона відображена в істотних ознаках формули винаходу) і запобігає її несанкціонованому використанню.

Також деякі фахівці критикують цей термін тому що він не сходиться із технічним терміном. У науковій літературі слушно наголошують на те, що законодавче визначення марно піддано критиці фахівцями у цій сфері, оскільки у ньому зазначено більше ознак, ніж у її технічному визначенні, що вживається на практиці.²⁶ Комп'ютерна програма з технічної точки зору є описом процесу оброблення інформації; такий опис має зчитуватися комп'ютером та приводити його у дію для вирішення конкретної задачі. Зокрема, йдеться про обробку інформації, виконання певної функції, досягнення певного результату тощо. Дати правове визначення комп'ютерної програми без фахових знань у цій сфері неможливо, оскільки складно відобразити правовою термінологією певні технічні процеси. Враховуючи можливе тлумачення законодавчих визначень, зокрема і комп'ютерної програми, може бути встановлено, що певний програмний продукт не містить однієї чи двох ознак, що містяться у законодавчому визначенні, а відтак його не можна вважати комп'ютерною програмою.

Отже на нашу думку слід переглянути терміни які стосуються комп'ютерних технологій. Та співпрацюючи із науковцями цієї технічної сфери дійти спільного консенсусу за для того, щоб ці терміни відповідали

²⁶ Петренко С. А. Правова охорона комп'ютерної програми як об'єкта інтелектуальної власності: шляхи розвитку / С. А. Петренко [Електронний ресурс]. — Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis64r_81/cgiirbis_64.exe?C21COM=2&I21DBN=A&P21DBN=ARD&Z21ID=&Image_file_name=DOC/2010/10psavsr.zip&IMAGE_FILE_DOWNLOAD=1

технічній дійсності. Так як існує ще декілька термінів які у практиці важко застосовувати та створюють проблеми при вирішенні спорів у цій сфері.

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

*Кривобок І. О., магістр кафедри
ІППІВ, КПП ім. Ігоря Сікорського
Яшарова М. М., доцент, к. ю.н., КПП
ім. Ігоря Сікорського*

ДОСВІД США ЩОДО ПРАВОВОЇ ОХОРОНИ ДИЗАЙНУ ОДЯГУ ЯК РЕЗУЛЬТАТУ ІНТЕЛЕКТУАЛЬНОЇ ДІЯЛЬНОСТІ

Нагальна необхідність ефективної правової охорони та захисту прав інтелектуальної власності для України зумовлюється обраною нею стратегією побудови цивілізованих ринкових відносин і тому законодавство з охорони інтелектуальних прав має відповідати духу часу і потребам ринку. Актуальність обраного дослідження зумовлено з розвитком сучасної української моди, а тому виникає необхідність охорони та ефективного захисту інтелектуальної власності на такі об'єкти, як одяг, взуття, аксесуари.

Слідуючи тенденціям сучасної моди, вона завжди піддавалася швидкому старінню, однак наразі цей процес прискорився в рази, наприклад якщо раніше підприємство, яке працювало в сфері виготовлення одягу, випускало дві колекції в рік, то сьогодні деякі підприємства пропонують в чотири рази більше колекцій на рік.

Розвиток правового регулювання суспільних відносин в цій сфері безпосередньо залежить від виникнення відповідної потреби в такому правовому регулюванні, а саме дизайну одягу, взуття, аксесуарів.

Правова охорона дизайну взагалі і дизайну одягу в різних країнах світу має свої особливості, але в той же час спирається на міжнародні стандарти охорони, закріплені в міжнародних угодах.

Перш ніж звернутися до проблем правової охорони дизайну одягу, слід уточнити поняття дизайну одягу, виявити характерні риси, що визначають вимоги до його правову охорону.

Згідно міжнародному законодавству питання правової охорони прикладного мистецтва врегульовано, зокрема, в п. 7 ст. 2 Бернської конвенції щодо охорони літературних і художніх творів, прийнятої в 1886 році. Тобто ми бачимо, що у зазначеній нормі передбачена можливість вибору правової охорони країною-учасницею, або це твори прикладного мистецтва можуть і охоронятися як авторське право або отримати

спеціальну охорону, як охорона в межах промислового зразка. Таким чином, розробники Бернської конвенції надали вибір режиму охорони творів дизайну країнам-учасникам.

Аналізуючи угоду ТРІПС, ми бачимо, що якщо право країни не передбачає авторсько-правову охорону для дизайну одягу, то країна може передбачити таку охорону нормами як промисловий зразок, виключаючи при цьому адміністративні процедури з перевірки охороноспроможності результату інтелектуальної діяльності для надання такої охорони. Перераховані особливості патентно-правової охорони призводять до відсутності охорони дизайну одягу в країнах, де їх авторсько-правова охорона не передбачена.

Таким чином, на підставі вище зазначених міжнародних угод можна зробити висновок, що на міжнародному рівні теж відсутнє регулювання питань правової охорони дизайну. Наявне правове регулювання носить загальний, фрагментарний характер, залишаючи рішення таких важливих питань на розсуд країн-учасниць, що породжує різноманітність підходів до правового регулювання дизайну одягу.

На національному рівні питання правового регулювання творів дизайну вирішується по-різному. В одних країнах передбачена можливість тільки патентно-правової охорони (США, Канада). В інших допускається одночасне застосування авторсько-правового та патентно- правового режиму (Франція, Німеччина), по-третє передбачається вибір одного із зазначених режимів (Італія, Великобританія).

Розглянемо більш докладно на прикладі правової охорони дизайну одягу США, вибір зазначених країни для дослідження пов'язаний з різними правовими підходами до регулювання охорони дизайну в загальному і дизайну одягу взагалі.

Дизайн одягу може охоронятися в рамках як авторського, так і патентного права. Відповідно до законодавство США , яке орієнтоване на патентно правову охорону дизайну одягу, але незважаючи на те що прямої заборони в законодавстві на авторсько-правову охорону дизайну не передбачено, отримати таку охорону практично важко. Відповідно до Закону про авторське право США 1976 роки (17. U.S.C. §§ 101et seq.)²⁷ в якості об'єктів авторського права охороняються оригінальні результати інтелектуальної діяльності, виражені в певній матеріальній формі, що дозволяє здійснювати відтворення, копіювання, переробку цих результатів. Крім цього, застосовується вимога «окремого існування», мається на увазі,

²⁷ Закон США «Об авторском праве» 1976 года, 17. U.S.C. §§ 101 et seq. URL: <http://www.wipo.int/wipolex/ru/details.jsp?id=5405> (дата обращения: 13.06.2015).

що дизайн повинен являти собою образотворчу, скульптурну або графічну роботу, яка може розглядатися окремо від утилітарної складової виробів.²⁸ Виконаний дизайнером малюнок одягу визнається об'єктом авторського права, що не можна сказати про дизайн, втіленому у виробі.

Наприклад, у справі *Jovani Fashion Ltd. v. Fiesta Fashions*, 2d Cir., No.12-598-cv, 10/15/12 про порушення авторського права на дизайн випускної сукні з блискітками, окружний суд США відмовив позивачеві у наданні охорони в рамках авторського права на підставі того, що декоративні елементи сукні - блискітки і кристали, що покривають ліф сукні, а також багатошарова спідниця не можуть бути відокремлені від утилітарної складової виробу і служать для виконання утилітарних функцій.²⁹ Висновок суду є неоднозначним, оскільки декоративне оформлення ліфа сукні блискітками і кристалами навряд чи може бути пов'язано з функціями сукні як виробу, що покриває тіло людини, оскільки при їх виключенні утилітарна функція сукні не зміниться. Але з іншого боку, відокремлене використання спірного елемента (не стосовно сукні) викликає великі сумніви.

Якщо брати до уваги справу про декоративне оформлення пряжки ремня, то малюнок, який там зображений може бути використаний для інших виробів, сам факт застосування блискіток і кристалів для оформлення інших виробів можливий, але зазначений дизайнерський винахід не може охоронятися, так як застосування блискіток і кристалів не є оригінальним. Якби мова йшла про візерунок або малюнок, то в такому випадку це все охоронялося б законом.

Маскарадні костюми неодноразово виступали предметом розгляду судових справ. А саме, у таких справах, як *National Theme Productions, Inc. проти Jerry B. Beck, Inc. і Whimsicality, Inc. v. Rubie's Costumes Co. Inc.*, вирішувалося питання про отримання охорони у рамках авторського права. Після розгляду цих справ, суд дійшов висновку, що призначення маскарадних костюмів відрізняється від функцій звичайного одягу, тим що вони виконують ігрову функцію, при цьому приховуючи особу людини. Крім того, свобода творчості дизайнера не обмежена функціональністю речі. Суд відхилив необхідність застосування критерію роздільності, мотивуючи це тим, що в даному випадку провести таке виділення не можливо, зважаючи на естетичну

²⁸ Silverman I. Copyright and fashion: friends at last? // E.R.P.R. 2013. V. 35. № 11. P. 637-

645.

²⁹ Silverman I. Copyright and fashion: friends at last? // E.R.P.R. 2013. V. 35. № 11. P. 637-

645.

спрямованість результату творчої діяльності. Таким чином, судом було вирішено, що карнавальні костюми підлягають охороні.³⁰

Отже, на підставі вище викладеного можна зробити висновок, що теорія концептуальної роздільності недостатньо розроблена в правозастосовній практиці і вимагає додаткового опрацювання.

Складність полягає в тому, що виділення критеріїв розмежування утилітарних і функціональних рис є практично неможливим, оскільки основне завдання дизайнера- добитися раціонального поєднання вказаних функцій. Іншими словами, завдання дизайнера протилежне до завдання суду, при вирішенні питання про їх розмежування.

Зробивши проміжний підсумок, можна сказати, що авторське право США не надає правову охорону дизайну одягу, за рідкісним винятком є охорона окремих високохудожніх елементів дизайну, які можуть бути відособлені від функціональних рис дизайну.

Патентно-правова охорона дизайну одягу може бути надана в США згідно розд. 35(§171-173) Зведення законів США від 19 липня 1952р.³¹ при відповідності наступним умовам: новизні, неочевидності, оригінальності і декоративності.

Дизайн визнається таким, що відповідає умові новизни, якщо він сприймається звичайним спостерігачем, відмінним від зареєстрованого промислового зразка (прототипу), а не в якості його модифікованого різновиду. Так, у справі L. A. Gear, Inc v. Thom McAn Shoe Co суд вказав, що промислові зразки не мають бути абсолютно однаковими, досить збігу в рисах.³²

Під оригінальністю дизайну розуміють створення дизайну за допомогою незалежної творчої діяльності і за відсутності прямого копіювання. У рамках судового розгляду це зводиться до порівняння заявленого дизайну з раніше

³⁰ Schalestock P.K. Forms of Redress for Design Piracy: How Victims Can Use Existing

Copyright Law. URL:

<http://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1523&context=sulr> (дата обращения: 05.01.2015).

³¹ U.S. Patents Act (Designs) 35 U.S.C. §§ 171-173 and 289 and Code of Federal Regulations,

37 C.F.R. 1. URL: <http://www.wipo.int/wipolex/ru/details.jsp?id=3925> (дата обращения:

13.06.2015).

³² Shickl L. Protection of industrial design in the United State and in the EU: different concept

zareestrovanim promislivim zrazkom z pozicii spozivacha, pri c'omu vidminnosti majuť buti duzhe istotnymi v porivnanni iz zvichaynim rezul'tatom praci dizajnera. Takim chinom, pri viznachenni yak novizni i neochovidnosti, tak i orihinalnosti promislivogo zrazka neobkhidno виявити міру відмінності заявленого дизайну від раніше zareestrovanih promislivih zrazkiv.

Pri c'omu novizna i neochovidnist', na nash poglyad, e detal'nishim analizom z toчки zoru vidpovidalnosti заявленого дизайну, krugu naybil'sh bliz'kih analogiv, todi yak orihinalnist' spriamovana na usunen'nia kopiuvannya. Varto vidmititi, sho borot'ba za oхорону дизайну одягу в США має тривалу історію і розгортається в області авторського права.

У 2006 році в Конгрес був внесений законопроект про захист дизайну одягу Design Piracy Prohibition Act, sho peredbachae vnesennia zmin do glavi 13 Zakonu США pro avtors'ke pravo. У законопроекті пропонувалося надати правову охорону дизайну одягу у рамках авторського права протягом 3 років за умови реєстрації у Бюро охорони авторських прав США (U.S. Copyright Office) vprodovzh 3 misyatsiv z momentu perшого pублічного prodazu. Однак вказаний законопроект так і не був ухвалений.

Otze, можна зробити висновок про відсутність ефективної правової охорони дизайну одягу в США. Охорона нормами авторського права може бути надана тільки художнім елементам дизайну, sho виключає з сфери правової охорони дизайн одягу як такого, a патентно-правова охорона в США не є ефективною зважаючи на тяжкі умови охороноздатності, тривалість реєстрації, фінансових витрат, високих ризиків визнання патенту недійсним в судовому порядку.

Zrobivshi zagal'nі підсумки doslidzhennia правової охорони дизайну в США, v porivnanni z іншими країнами ЄС, вона виявляється найбіл'sh не пристосованою для охорони дизайну одягу, oskil'ki avtors'ke pravo виключає охорону промислових виробів, a патентне право вимагає тривалої реєстрації, неприйнятної для ефективної охорони. Але особливий інтерес doslidzhennia v цій сфері викликає законодавство ЄС, де використовується новий перспективний механізм охорони промислових зразків, sho виключає необхідність реєстрації, який дозволяє отримати ефективну охорону без дотримання формальностей.

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

*Шарудило Д. О., магістрант кафедри
ІППІВ КІІ ім. Ігоря Сікорського
Науковий керівник: Яшарова М. М.,
доцент кафедри ІППІВ КІІ ім. Ігоря
Сікорського, к.т.н., с.н.с.*

ПРАВОВИЙ СТАТУС СУБ'ЄКТІВ АВТОРСЬКОГО ПРАВА НА ТВОРИ АРХІТЕКТУРИ

Людина з давніх – давен будує різні споруди з метою фізичного захисту свого життя. Однак сьогодні, архітектурна діяльність є одним із найбільш важливих аспектів міжнародного правового регулювання, оскільки сучасні тенденції життя роблять архітектуру вкрай вразливим, з точки зору порушення права, об'єктом. Історія розвитку законодавчих актів щодо прав суб'єктів інтелектуального права активно розвивалася протягом сторіч, і такий процес значно вплинув на сьогоdnішній статус суб'єктів авторського права на твори архітектури як на міжнародному рівні так і в окремо взятих національних системах законодавства.

Однією із важливих особливостей визначення авторського права та суб'єктів авторського права на твори архітектури є формування кола учасників процесу створення архітектури. Адже якщо, наприклад, твори літератури можуть писатися однією особою, то процес будівництва передбачає залучення великої кількості суб'єктів. Тому, питання чіткого визначення суб'єктів авторського права в архітектурі є важливим елементом забезпечення правового захисту.

Втім, проблематика даного питання також полягає в низькому рівні наукового дослідження, оскільки наявні роботи лише надають загальну характеристику класифікації суб'єктів авторського права на твори архітектури та практично не досліджують особливостей специфіку архітектурної діяльності.

До визначення проблематики чіткого визначення суб'єктів авторського права на твори архітектури належать роботи Є.А. Грекова ³³, Є. Ю. Гнатченка³⁴. У цих роботах автори намагаються розглянути проблематику визначення суб'єктів авторського права на твори архітектури, однак

³³ 1. Проблеми застосування в законодавстві України поняття твору архітектури як об'єкта авторського права. Є. А. Греков - Вісник Харківського національного університету внутрішніх справ. - 2006. - № 34. - С. 258-265

³⁴ 1. Маркетингова стратегія підприємств будівельного комплексу. Є. Ю. Гнатченко, Н. В. Дріль, Науковий вісник Херсонського державного університету. Сер. : Економічні науки. - 2014. - Вип. 7(2). - С. 162-164.

проблематика порушена лише частково і не охоплює усієї специфіки визначення суб'єктів права в архітектурній діяльності.

Важливим елементом у визначенні класифікації суб'єктів авторського права є виокремлення осіб, що безпосередньо задіяні у створенні інтелектуальної власності та осіб, що є лише учасниками суспільних відносин у сфері архітектури та будівництва. У відповідності до чинного законодавства, а саме ст.29 Закону України «Про архітектурну діяльність», зазначається, що особи які не створюють об'єкту інтелектуальної власності – не можуть бути співавторами або авторами. Отже, особи які є учасниками суспільних відносин у сфері архітектури та будівництва це загальне поняття, що характеризує осіб, які приймають пряму чи опосередковану участь у створенні творів архітектури та об'єктів архітектури. Натомість, суб'єктом авторського права на твори архітектури визначаються особи, які шляхом творчої діяльності створюють об'єкти архітектури. Фактично, в першому випадку до суб'єктів архітектурної діяльності відносяться усі особи, що приймають участь у створенні об'єкту архітектури: підрядники, замовники, державні установи, юридичні особи, тощо. А в другому випадку, автором та суб'єктом авторського права на твори архітектури визнаються лише особи, які шляхом саме творчої діяльності створюють об'єкти архітектури.

До таких осіб відносяться такі, що створюють твори архітектури, наприклад корисну модель або винахід, що застосовуються у процесі будівництва або відповідну проектну документацію, ескіз, тощо.

Також, до суб'єктів авторського права на твори архітектури можуть належати особи за якими, у відповідності до договорів або умов праці, зазначаються майнові права на твір архітектури.

Таким чином, можливість визначення суб'єкту права виходить із приналежності майнових прав, які можуть виникати як на момент створення об'єкту архітектури так і у відповідності до укладених договорів. На жаль, в чинному законодавстві не має такого розподілення, але важливим нюансом визначення суб'єктів авторського права на твори архітектури за причиною виникнення майнових прав : первинні та вторинні. Оскільки, за умови відсутності такого визначення виникає проблематика у майнових спорах між первинними та вторинними суб'єктами авторського права на твори архітектури. Також, важливим фактором є визначення проблематики приналежності майнових прав юридичним особам, та умови визначення юридичних осіб суб'єктами авторського права на твори архітектури. З одного боку, юридичні особи можуть знаходитися у співавторські за умови складання трудового договору або умови придбання майнових прав на твір архітектури. Втім, з іншого боку, за певних обставин

юридичним особам необхідно надавати первинні авторські права та визнавати їх суб'єктом авторського права на твори архітектури. У своїх працях правознавець Ю.Басін визначає³⁵, що первинним суб'єктом авторського права можуть бути лише фізичні особи, які безпосередньо шляхом творчої діяльності створюють об'єкти архітектури. Зазначаючи, що за умови використання юридичною особою майнових прав на твір архітектури, обов'язково необхідно зазначати автора.

Мотивація такого підходу до визначення правового статусу суб'єктів авторського права на твори архітектури визначається роллю людини у створення об'єктів архітектури, адже юридичні особи є лише представниками майнових прав та виокремлюють можливість використання таких прав задля отримання матеріального зиску. Натомість фізичні особи – автори, в першу чергу, є носіями нематеріального права та є суб'єктами авторського права, оскільки за умови володіння майновими правами – юридичні особи не стають авторами.

Проте, юридичні особи можуть первинно володіти торгівельними марками, найменуваннями та іншими позначеннями комерції. Така класифікація ознак приналежності елементів інтелектуальної власності визначає специфіку визначення індивідуального суб'єктивного складу для кожного об'єкту інтелектуального права в аспекті процесу будівництва та створення архітектурних творів. Важливого значення набуває також отримання авторського права спадкоємцями які також можуть бути суб'єктами авторського права на твори архітектури.

У відповідності до ч.1 ст.1218 Цивільного кодексу України³⁶ до складу спадщини входять усі права та обов'язки, що належали спадкодавцеві на момент відкриття спадщини і не припинилися внаслідок його смерті. При цьому, не входять до складу спадщини права та обов'язки, що нерозривно пов'язані з особою спадкодавця.

Отже, досліджуючи законодавчі норми, стає зрозуміло що спадкоємці отримують лише спектр майнових прав, не отримуючи немайнових. Можна відмітити, що законами України «Про архітектурну діяльність» та законом України «Про авторське право і суміжні права» унормовано питання створення об'єкту права інтелектуальної власності в сфері будівництва за замовленням. Так згідно ст. 31 закону України «Про архітектурну діяльність» вказано, що Особистими немайновими правами інтелектуальної власності автора (співавторів) об'єкта архітектури як об'єкта

³⁵ Басин Ю.Г., Грешников И.П. Избранные труды по гражданскому праву,. Сборник научных трудов. - СПб.: Юридический центр-Пресс, 2003. - 591 с.

³⁶ Цивільний Кодекс України// закон від 16 січня 2003 року № 435-IV// База даних «Законодавство України»/ ВР України. URL: <https://zakon.rada.gov.ua/laws/show/435-15>

авторського права є відповідні права, визначені Цивільним кодексом України, Законом України "Про авторське право і суміжні права" та зокрема:

- право фотографувати, здійснювати відеозйомку відповідного об'єкта архітектури як об'єкта авторського права, крім випадків, визначених законом;

- право вимагати визнання свого авторства (співавторства) шляхом зазначення належним чином свого імені на об'єкті архітектури як об'єкті авторського права, якщо це практично можливо.

Особисті немайнові права на об'єкт архітектури як об'єкт авторського права належать його автору (співавторам) незалежно від умов договору (контракту) між автором та замовником або юридичною чи фізичною особою, де або в якій він працює. Отже у разі створення об'єкту архітектури за замовленням, очевидним є те, що особисті немайнові права залишаються за автором.

Особисті немайнові права на об'єкт архітектури як об'єкт авторського права належать його автору (співавторам) незалежно від умов договору (контракту) між автором та замовником або юридичною чи фізичною собою, де або в якій він працює.

При цьому, майнові права на об'єкт архітектури як об'єкт авторського права, створений за замовленням, належать творцеві цього об'єкта або замовникові спільно, якщо інше не встановлено договором. Таким чином, договором можуть врегульовуватись питання розподілу майнових прав інтелектуальної власності і тільки вони. Взагалі, цілісність аспектів створення об'єктів інтелектуального права в сфері будівництва визначається низкою трудових договорів, які передбачені законодавством України та визначають умови передання майнових прав на об'єкти авторського права у сфері архітектурних творів. Основні закони, що регулюють правове врегулювання авторського права в секторі архітектурної діяльності:

- 1) Закон України «Про авторські права та суміжні права»;
- 2) Закон України «Про архітектурну діяльність».

У відповідності до вищезгаданих законів, немайнові права залишаються за суб'єктами авторського права на твори архітектури, а майнові можуть передаватися як фізичним так і юридичним особам у відповідності до трудового договору або заповіту.

Таким чином, немайнові та майнові права автора є первинними та виникають на момент створення твору архітектури, а майнові права, що передаються від автора іншим особам є вторинними та виникають внаслідок відповідних правочинів.

Втім, визначаючи специфіку процесу будівництва – виникає низка

унікальних умов передачі майнових прав серед осіб, тому кожна ситуація повинна розглядатися індивідуально з метою максимально об'єктивного та неупередженого захисту авторських прав.

Так, у відповідності до ст.7 Закону України «Про авторські право та суміжні права»³⁷ - суб'єктами авторського права є автори творів, зазначених у частині першій статті 8 цього Закону, їх спадкоємці та особи, яким автори чи їх спадкоємці передали свої авторські майнові права. Однак, в аспекті визначення суб'єктів авторського права саме на твори архітектури, необхідно зазначити, що у відповідності до ст. 29 Закону України «Про архітектурну діяльність»³⁸ - об'єктами авторського права в галузі архітектури є твори архітектури, містобудування і садово-паркового мистецтва, а також плани, креслення, пластичні твори, ілюстрації, карти та ескізи, що стосуються архітектури.

Особа (особи), творчою працею якої (яких) створено об'єкти архітектури як об'єкти авторського права, вважається автором (співавторами) цих об'єктів.

Співавторами не можуть бути особи, які подають автору об'єкта архітектури технічну, консультаційну чи організаційну допомогу або такі, що здійснюють організацію проектування і будівництва (реконструкції, реставрації, капітального ремонту), контроль за виконанням зазначених робіт.

Отже, згідно чинного законодавства, суб'єктами авторського права на твори архітектури виступають лише ті особи, які приймали або приймають безпосередню участь у створенні об'єкту архітектури. Тому, якщо інше не передбачено відповідним договором, визнання суб'єктом авторського права на твори архітектури намагається максимально зменшити діапазон можливих власників такого права. Оскільки, специфіка створення об'єктів архітектури та творів архітектури, майже унеможливорює створення таких об'єктів та творів одноособово, і тому законодавство чітко розмежовує важливість ролі особи у створенні того чи іншого виду об'єктів архітектурної діяльності. І хоча законодавча база чітко розмежовує поняття суб'єктності, певні положення потребують редагування та доповнення з метою розкриття більш конкретних формулювань визначень з метою

³⁷ Закон України “Про авторське право і суміжні права”// Закон від 23 грудня 1993 року № 3792-XII//База даних «Законодавство України»/ ВР України. URL: <https://zakon.rada.gov.ua/laws/main/3792-12/> (Відомості Верховної Ради України (ВВР), 1994, № 13, ст.64)

³⁸ Закон України “ Про архітектурну діяльність”// Закон від 20 травня 1999 року № 687-XIV //База даних «Законодавство України»/ ВР України. URL: <https://zakon.rada.gov.ua/laws/main/687-14/> (Відомості Верховної Ради України (ВВР), 1999, № 31, ст.246)

підвищення правового рівня захисту авторських прав та регулювання суспільних відносин з суб'єктами авторського права.

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

*Третякова П. О., магістр кафедри
ІППІВ КПІ ім. Ігоря Сікорського
Науковий керівник: Яшарова М. М.,
доцент кафедри ІППІВ КПІ ім. Ігоря
Сікорського, к.т.н., с.н.с.*

ОЗНАКИ ТЕАТРАЛЬНОЇ ПОСТАНОВКИ ЯК ОБ'ЄКТА АВТОРСЬКОГО ПРАВА

Умови глобалізації, поглиблення інформаційних потоків, ускладнення відносин у суспільстві, стрімкий розвиток науки і техніки, який відкрив людству нові можливості щодо створення, фіксації, відтворення та розповсюдження об'єктів права інтелектуальної власності стимулюють розвиток креативних індустрій в Україні. Зокрема, розвивається театральне мистецтво. Театральні постановки стають складнішими, синтезуючи у собі все більше творів — складових частин, з'являються нові види театральних постановок з використанням сучасних сценічних технік та театральних явищ, схожих на театральні постановки, але з певними відмінностями. Суспільні відносини у театральній сфері стають все складнішими, розгалужуються, що зумовлює необхідність їх усестороннього дослідження. Незважаючи на наявність праць, які висвітлюють правові дослідження у сфері театральної діяльності, тема не є повністю розробленою і потребує подальшого дослідження. До цього часу науковці не прийшли до єдиної думки стосовно ознак театральної постановки як об'єкта авторського права. Це пов'язано зі специфікою об'єкта, що виражається у його складності, наявності прогалин законодавчого регулювання, проблематикою правового статусу авторів та виконавців, численними складнощами у їх взаємодії і правозастосуванні.

Відповідно до ст. 1 спеціального Закону України «Про театри і театральну справу», театральна постановка — твір театального мистецтва, створений на основі драматичного, музично-драматичного або літературного твору, що має єдиний задум та конкретну назву.³⁹

³⁹ Закон України «Про театри і театральну справу» від 31.05.2005 р. № 2605-IV// Відомості Верховної Ради України. — 2005. — №36. — Ст. 350 [Електронний ресурс]. — Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2605-15>.

Варто виокремити 4 ознаки театральної постановки з наведеного законодавчого визначення: вид твору (зокрема, твір театального мистецтва), похідний характер (створена на основі іншого твору, зокрема, драматичного, музично-драматичного або літературного), єдиний задум і конкретна назва. Використання саме цих характеристик для закріплення поняття «театральної постановки» свідчить про те, що саме вони визнаються законодавцем фундаментальними і більш важливими у порівнянні з іншими.

Розглянемо більш детально. По-перше, театральна постановка – твір театального мистецтва. Нормотворець завбачливо визначив театральне мистецтво як «вид мистецтва, особливістю якого є художнє відображення життя за допомогою сценічної дії акторів перед глядачами». У законі дуже доречно використовує не поняття «гра акторів», а більш широке – «сценічна дія». Оскільки останнє може вміщувати танець, спів, використання спеціальних приладів, інструментів, створення технічних ефектів тощо, а не просто гру у класичному розумінні. Окрім цього сценічна дія включає в себе використання ляльок, масок, тіней тощо.

Також відповідно до наведеного у законі визначення, сценічні дії спрямовані на художнє відображення життя. На мою думку, такий підхід є неповним, - це лише один з можливих напрямів, адже є фантазійні, абстрактні твори, що прагнуть створити певний емоційний ефект, змодельовати іншу реальність, не прив'язуючись до зображення життя.

В протигагу цьому безумовною позитивною рисою цього визначення є вказівка на взаємодію акторів з глядачами. Аудиторія є обов'язковим складником театального мистецтва, адже специфіка театру полягає в його існуванні лише за наявності глядацької уваги. Театральне мистецтво загалом прагне до створення інтерактивної ситуації для глядача, а композиція твору передбачає участь глядачів у виставі, що формує ефект інтерактивності дії.

По-друге, законодавче визначення вказує на похідний характер театральної постановки, оскільки вона створюється на основі іншого самостійного твору. Такої думки дотримуються більшість науковців, зокрема, С. Холодинська, яка зазначає, що у театральній постановці здійснюється задум, вже даний в іншому творі, а саме – у драматургічному.⁴⁰

Нормотворець у ЗУ «Про театри і театральну справу» у якості основи театральної постановки виділяє лише драматичний, музично-драматичний чи

⁴⁰ Холодинська С. М. Естетико-художні особливості театру як поліфонічного виду мистецтва / С. М. Холодинська// Вісник МДУ. Серія «Філософія, культурологія, філософія». -- 2011. -- Вип. 1. -- С. 140-146.

літературний твір.⁴¹ Відповідний законодавчий перелік є вичерпним, однак це не відповідає практиці театральної діяльності. Сучасні театральні постановки можуть бути побудовані на основі хореографічних або інших творів.

На мій погляд, слід відмовитися від закріплення похідності театральної постановки від драматургічного, музично-драматургічного чи літературного твору. Краще вказати на рису синтетичності, що полягає у гармонійному поєднанні різних видів мистецтва у єдиний, цілісний твір.

Цікавим у цьому розрізі є підхід О. Жилінкової. Дослідниця у своїх працях описала юридичну концепцію складного твору, відповідно до якої складний твір вважається об'єктом авторського права, який:

а) поєднує два або кілька самостійних об'єктів авторських прав, що належать до різних видів мистецтва;

б) містить окремі частини, жодна з яких не є головною порівняно з іншими; в) поєднує частини, кожна з яких може використовуватись як разом з іншими частинами, так і окремо від інших.⁴²

Третя ознака, яку можна виокремити з законодавчого визначення, - наявність основної ідеї твору, на розкриття якої спрямовані сценічні дії, засоби виразності та уся постановка у цілому. Нормотворець використовує поняття «єдиний задум» як ознаку театральної постановки. Поняття задуму твору є мистецтвознавчою категорією, але у даному випадку через використання у нормативно-правовому акті вона набуває правового значення, і тому має бути розкрита з юридичної точки зору. Деякі автори вважають, що творчий задум – це думка митця, яку він доніс до аудиторії через твір. Я розглядаю задум як певну ідею, ще не втілену у конкретному творі. У зв'язку зі своїм ідеальним динамічним станом, ця вихідна ідея може здійснити метаморфози під час підготовки твору, тобто цілком можливо, що задум у процесі побудови твору зміниться та набуде нових рис. Отже, задум ніби передують формуванню основної думки твору. Таке розуміння задуму театральної постановки не дозволяє йому бути юридично значущою ознакою цього об'єкту. Втілений задум є фактично основною ідеєю твору – саме її можна виокремити із готового твору, проаналізувавши театральну постановку на предмет єдності та цілісності, наявності основної думки. Тому вважаємо, що було б зручніше

⁴¹ Закон України «Про театри і театральну справу» від 31.05.2005 р. № 2605-IV// Відомості Верховної Ради України. – 2005. – №36. – Ст. 350 [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2605-15>.

⁴² Жилінкова О. В. Договори в сфері реалізації майнових прав на музичний твір [Текст] : дис. канд. юрид. наук: 12.00.03 / Жилінкова Олена Вячеславівна ; Інститут держави і права ім. В.М.Корецького НАН України. - К., 2007. - 224 арк. - арк. 209-224

легальне поняття театральної постановки все ж будувати, виходячи з існування обов'язкової характеристики – основної думки твору.

Четверта ознака, яку можна виокремити, - наявність власної назви. Вважаємо, що більш доцільно використовувати саме формулювання «власна назва», замість законодавчого «конкретна назва», адже конкретність є лише однією з характеристик назви театральної постановки. До того ж «власна назва» є загальновживаним науковим терміном для визначення назви окремих художніх творів. Що стосується назви театральної постановки, то слід звернути увагу, що назва розглядається як частина твору. Як звертають увагу науковці, стаття 9 Закону України «Про авторське право і суміжні права» закріплює, що частина твору, яка може використовуватися самостійно, зокрема, оригінальна назва твору, розглядається як твір і охороняється відповідно до зазначеного Закону.⁴³

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

**ТЕЗИ ВИСТУПІВ СТУДЕНТІВ НТУУ «КПІ ім. ІГОРЯ СІКОРСЬКОГО»
НА ДРУГОМУ УКРАЇНСЬКОМУ МОЛОДІЖНОМУ ФОРУМІ З
УПРАВЛІННЯ ІНТЕРНЕТОМ**

*Сазонова К. М., студентка ФБІ КПІ ім.
Ігоря Сікорського*

*Науковий керівник: Фурашев В. М.,
доцент кафедри ІППІВ КПІ ім. Ігоря
Сікорського, к.т.н., с.н.с.*

**СОЦІАЛЬНІ МЕРЕЖІ: КІБЕРЗАЛЕЖНІСТЬ ЧИ КОМУНІКАЦІЯ
МАЙБУТНЬОГО?**

Давайте уявимо наше життя без соціальних мереж та Інтернету. Що, складно? А наші батьки в молодості з електронних пристроїв знали тільки телевізор, радіо та магнітофон. З появою персональних комп'ютерів та Інтернету набагато більше речей стало робити легше ніж раніше. Знайти потрібний рецепт, подивитися дорогу за допомогою електронних карт, передивитися улюблений фільм, прочитати нову книгу, а особливо, технічний прогрес спростив процес спілкування.

Тепер можна листуватися з друзями по всій планеті – підтримувати контакти зі старими товаришами і знаходити нових. Лише кілька кліків і друг чи подруга – на дроті або правильніше сказати он-лайн. І все це завдяки

⁴³ Про авторське право і суміжні права: Закон України від 23.12.1993 № 3792-ХІІ (у чинній редакції від 26.04.2017). Відомості Верховної Ради України. 1994. № 13. Ст. 64.

соціальним мережам. Але що таке, ці соціальні мережі, насправді вони є кроком у майбутнє, а не причиною деградації та залежності?

У наш час, соціальні мережі – основний спосіб розповсюдження новин. За даними дослідження, проведеного каналом CNN, було виявлено, що 43% новин поширюються через такі соціальні сайти як Фейсбук, Твітер, MySpace, YouTube. Це дуже зручно, бо вони забезпечують швидку та дешеву комунікацію, оперативний обмін інформацією, можливість побути у центрі уваги та здобути нові знайомства. Також, це непоганий «тренувальний майданчик», для людей, що погано почувають себе у соціумі і не можуть реалізуватися у справжньому житті, там, вони вчаться цьому і створюють певний, бажаний для себе образ, який потім можуть втілити у реальність.

Соціальні мережі – це не лише місце для спілкування із друзями. Вони можуть бути використані для проведення семінару чи конференції. На сьогодні вони стали потужним освітнім засобом. Наприклад, викладачі можуть відправляти домашнє завдання, конспект лекції, питання на залік чи результати контрольних через соціальні мережі. Також, якщо якийсь питання тебе непокоїть, то немає необхідності шукати викладача десь на кафедрі, а можна просто написати йому електронного листа або повідомлення .

Крім того, соціальні мережі допомагають мозку працювати. За даними BBC NEWS групі вчених з США, під час проведення спеціалізованого дослідження вдалося виявити невелику за розмірами ділянку головного мозку, яка відповідає за організацію соціального життя. В тих людей, які надають перевагу активному способу соціальної поведінки, ця частина головного мозку розвинена набагато краще, ніж у решти населення.

Протягом останніх 5 роки соціальні мережі стали невід’ємною частиною життя більшості українців. Мабуть, одним із найяскравіших підтверджень даної тези є те, що Папа Римський, Бенедикт XVI, зазначив, що спілкування в соціальних мережах допомагає встановити нові знайомства, сприяє обміну знаннями, діалогу культур [1].

А тепер поговоримо про недоліки. Як я вже зазначала раніше, соціальні мережі допомагають соціально невпевненим людям спілкуватися: спочатку онлайн, а потім у реальному житті. Але, що ми бачимо зараз? Спілкування онлайн заміняє реальні відносини між людьми, хоча це навіть спілкуванням не назвеш, бо люди відправляють один одному лише «смайлики», бо їм навіть ліньки писати слова. Від такого «спілкування» втрачаються міжособистісні навички і спроможність адекватного ставлення та реакції на людей та життєві ситуації. У віртуальності в тебе може бути понад 1000 друзів, але близько спілкуватися у реальному житті ти будеш з меншою кількістю. Не без допомоги соціальних мереж поняття «дружби» втрачається, спотворюється, бо

дружба – це відданість, щирість, довіра чи може вона у такому розумінні буди забезпечена он-лайн?

Крім того, соціальні мережі спричиняють проблему з концентрацією, бо коли ти чимось зайнятий: роботою, навчанням, тощо і тобі приходить повідомлення, ти маєш відриватися від своєї справи и переключатися, щоб зрозуміти, що саме від тебе хоче твій віртуальний співрозмовник. Це дуже сильно впливає на якість виконання роботи і спричиняє виникнення помилок. Звісно, рішенням такої проблеми є вимкнення звуку на телефоні, або комп'ютері, але не всі погодяться з таким способом, бо їм необхідно відповісти на повідомлення попри усе. Були проведені дослідження по цьому питанню в Нідерландах професором Кіршнером. Дослідження показали, що оцінки учнів, які готуються до занять за комп'ютером, не відключаючись від соціальної мережі, на 20% нижчі, ніж у тих, хто не проводить час в Фейсбук. Також виявилось, що останні приділяють навчанню на 88% більше часу (мається на увазі самостійна підготовка).

Вчені вже не раз стверджували про психічні захворювання, спричинених соціальними мережами. Найбільший вплив вони мають на підлітків, які ще не мають доцільного розуміння, як все працює у цьому світі. Крім того, місце має булінг у соціальних мережах, це стосується не тільки звичайних людей, а й зірок, які можуть зробити, щось, що спричинить суспільний осуд та на них виліється купа гнівних коментарів, не кожен спроможне таке витримати. Основний принцип більшості психологічних захворювань – це піраміда за принципом Маслоу, згідно з якою основний ступінь потреб займає самовираження. Згідно з даними дослідження американської вищої Школи медицини «Case Western Reserve School» активні користувачі соціальних мереж в 2 рази частіше вживають алкоголь, на 40% більше палять тютюн та на 55% більше б'ються [1].

Мало хто замислюється, що інформація про себе несе загрозу, у першу чергу - користувачеві. Адже почастишали випадки, коли при пограбуванні квартир чи викраденні авто злочинці використовували інформацію, отриману з соціальних мереж. Також, детальна інформація стає здобиччю спецслужб (в США за допомогою соціальних мереж з боржників «вибивають» борги та кредити). У Німеччині теж не вщухає суспільна дискусія про безпеку даних в Інтернеті. Незалежна організація Stiftung Warentest провела перевірку і знайшла суттєві недоліки. Ця компанія звернулася до адміністраторів соціальних мереж з проханням дати дозвіл на «тестову атаку». Результати виявилися сумними: інформація користувачів дуже погано захищена. Для сторонніх осіб доступ до приватної інформації є фактично відкритим. Отже, даними можна зловживати та маніпулювати.

Соціальні мережі становлять загрозу і для сім'ї. За результатами опитування, проведено з нагоди Національного тижня сім'ї в Британії, виявилось, що четверта частина 15-річних підлітків вважають соціальні мережі найважливішим, що є в їхньому житті.

Співробітник Массачусетського технологічного інституту завершив дослідження, присвячене негативному впливу соціальних мереж на здоров'я. Вони негативно впливають і на роботу імунної системи організму, роботу артерій і процеси мислення. У результаті – підвищення ризику появи раку та серцево-судинних захворювань. На думку великобританського біолога Аріка Сігмана ця загроза пов'язана з тим, що фізіологічні процеси в організмі людини відбуваються по різному залежно від того, знаходиться людина наодинці, або в чиємусь товаристві чи у віртуальній реальності. Є й інші мінуси – порушення зору, викривлення хребта тощо [1].

Провідні соціологи вважають, що безперервне спілкування в соціальних мережах є нічим іншим, як сучасна форма божевілья. Вони пояснюють це тим, що через подібні сайти люди ізолюються від реальності і стають менш людяними. Ілюзія підвищення зручності спілкування насправді відбирає у нас «живу» взаємодію і лише створює імітацію реального світу. Зараз ми вже не можемо уявити собі і дня без спілкування он-лайн, а якщо у тебе зламався телефон, або раптово зник Інтернет, то все – ти відрізаний від соціуму, самотній, розгублений, не знаючий, що тобі робити далі.

Насамкінець, хочу зазначити, з одного боку, соціальні мережі є безцінним винаходом. Але ставши прогресом для людства, вони стають регресом для кожної окремої людини.

Список використаних джерел:

1. Андрейко П. Позитивний та негативний вплив соціальних мереж [електронне джерело] // SITES.GOOGLE.COM: зібрання інформації про соціальні мережі, 2016. URL: [https://sites.google.com/site /socialnimeregi/ pozitivnij-ta-negativnij-vpliv-socialnih-merez](https://sites.google.com/site/socialnimeregi/pozitivnij-ta-negativnij-vpliv-socialnih-merez) (дата звернення: 14.10.2019)

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

*Мнишенко М. О., студент ФСП КПІ
ім. Ігоря Сікорського*

*Науковий керівник: Фурашев В. М.,
доцент кафедри ІППІВ КПІ ім. Ігоря
Сікорського, к.т.н., с.н.с.*

ПРАВА ЛЮДИНИ ТА РОЗШИРЕННЯ РОЛІ ІНТЕРНЕТУ, ЯК ЗАСОБУ МАНІПУЛЯЦІЇ СУСПІЛЬСТВОМ

Темою мого сьогоднішнього виступу є "Права людини та розширення ролі інтернету, як засіб маніпуляції суспільством".

Звісно ж таке формулювання є доволі специфічним враховуючи що всіх намагаються переконати в непорушності концепції прав людини, що були закладені в ООН, а точніше її декларативних актах.

Окрім цього популяризується й вседоступність інформації та доступу до інтернету з перенесенням життя суспільства та держави у віртуальну площину. Неймовірно, дехто навіть закликає розробляти концепції такі як держава в смартфоні або "інтернет речей". (Інтернет речей — концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку.)

В контексті даного виступу я висуну тезу, що той хто пропонує надати найбільше прав і свобод, той врешті-решт найбільше їх і обмежить. Надання людині більших прав та привілеїв призводить до невизначеності і надмірного індивідуалізму, коли втрачається справжня цінність особистості і створюється культ "важливого індивіда" - розмитого невизначеного поняття, яким можливо маніпулювати як завгодно, бо якщо здорове колективне суспільство формують особистості, що займають своє визначене місце, то біомасу формують такі ж самі розмиті індивіди, що піддаються на лестоці та найпростішу брехню.

Коли в ці відносини додається інтернет, то ми бачимо ще більший вплив інформації та так званих лідерів думок в інтернеті на індивідів та деградацію особистості. Інтернет є офіційно непідконтрольною системою з точки зору фільтрації інформації, але при цьому надсилати туди необхідні месенджі мають найкращу можливість саме ті, хто і до цього здійснював інформаційний контроль над суспільством.

Тому підбиваючи підсумки, знову ж таки зазначемо, що концепція прав людини та інтернет розвитку є одним із елементів маніпуляції свідомістю та

переходу до справжньої диктатури, отже на мою думку слід переглянути концепцію прав людини, доцільність існування ООН та її декларацій.

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

Єрмак Я. М., студент ФСП КПІ ім. Ігоря Сікорського

Науковий керівник: Фурашев В. М., доцент кафедри ІППІВ КПІ ім. Ігоря Сікорського, к.т.н., с.н.с.

ДОСТУП ДО ІНТЕРНЕТУ В СЕЛАХ, СЕЛИЩАХ, СМТ

В 2018 році Україна посіла 9 місце в Європі (у звіті про стан європейської технічної індустрії State of European Tech) , за кількістю ІТ-розробників . Ми обігнали Швецію, Туреччину, Австрію, Норвегію, та багато інших маленьких країн. З одного боку, можемо пишатись, що їх так багато - приблизно 185 000, з іншого - якщо ми візьмемо країни, які йдуть зверху в списку, то побачимо, що ми непогано так відстаємо. В Нідерландах, де населення приблизно в 2 рази менше, ІТ-розробників приблизно в 1,5 рази більше . І це є нормальним явищем, бо кожна країна має свої вектори розвитку, я впевнений, що в агро-секторі з нами не можуть позмагатись більшість Європейських країн.

Тому, в цьому звіті нас більше цікавить, не кількість розробників в сфері ІТ, а їх місцезнаходження... На другому графіку зображено процент ІТ-developer-ів певної країни, в великих містах, від загальної їх кількості. В Києві знаходиться 41 відсоток, від усіх ІТ-developer-ів України. В Москві - 40 %, в Брюсселі - 84 %. В Німеччині, в якій більше за всіх ІТ-розробників в Європі (850 000), вони децентралізовані, лише Кельн має 19 відсотків від усіх німецьких девелоперів.

Ця статистика, спонукає задуматись, наскільки реально в Україні децентралізувати будь-яку ІТ - сферу, та взагалі, будь-яку галузь пов'язану з використанням комп'ютерних технологій, та найголовніше - інтернету. Бо на сьогоднішній день, інтернет - засіб надавати робочі місця мільйонам людей дистанційно. Доступ до інтернету по всій Україні може:

- Залишити села, селища, смт живими - залишити в них мешканців. Тим самим врятувати міста, від переповнення.
- Покращити юридичне та соціальне становище села (Інформація про існуючі та затверджені закони, буде надходити швидше, що призведе до тиску на місцеву владу з боку населення, на дотримання своїх прав та свобод).
- Допоможе привернути увагу, до існуючих проблем (За прикладом можна звернутись до проєкту Ukrainer, на сайті якого ви зможете знайти статті

і відео, як заброшені заводи, ставали місцевими хабами, ставали спортивними зонами, тощо .

- **Покращить рівень освіти сільського населення, надасть можливість дистанційного навчання.**

Абсолютно вірним аналізом моїх досліджень буде думка, що: “Інтернет же в селах є, і їм користуються”. І ви не помиляєтесь, просто питання в кількості людей які користуються їм, і як вони його використовують!

Дослідницький холдінг Factum Group Ukraine, провів ряд досліджень, під назвою “Проникнення інтернету в Україні” в лютому місяці 2019 року . І надав статистику щодо кількості користувачів інтернету в Україні:

21,09 мільйонів громадян України - регулярно користуються інтернетом. Без тимчасово окупованих Криму та Донбасу, це приблизно 64% населення віком 15+ років. А інтернет вдома є у 65% населення.

В селах, інтернет є тільки у 54% мешканців. Чи може це бути достатнім для найбільшої країни в Європі? Питання риторичне.

Як вирішити проблему? Провести інтернет, в кожний будинок насильно/примусом - не раціонально. Тим паче, наявність просто інтернету, без обладнання (в нашому випадку - ПК) - нічого не змінить. На мою думку, правильним рішенням буде - забезпечити обладнанням “Сільські Ради”, бо деякі будинки минулих сільських рад, після децентралізації (Сільські ради створили ОТГ (об'єднані територіальні громади)) , чи покинуті, чи не використовуються на 100%. Логіним є, що певне місце теж звільнилось. Місце знайдено, залишається знайти бюджет, та людський ресурс, який допоможуть втілити план в життя.

Бюджет - найскладніша частина, тут на жаль, сподіватись на відсоток від державного бюджету не приходить, тому основне джерело капіталу я бачу в Європейських грантах, залучення іноземних коштів. Як показує практика, це достатньо реально, багато проектів в Україні, зокрема малий/середній бізнес, наукові проекти, тощо. були спонсоровані такими організаціями/фондами.

Зокрема треба звернути увагу на European Agricultural Fund for Rural Development - Європейський сільськогосподарський фонд розвитку сільської місцевості, який спонсорує схожі проекти в Європі.

Люди - не менш важка частина. Бо знайти людей, які будуть навчати населення сіл та селищ, користуватись інтернетом “з розумом”, навчати знаходити відповідну інформацію в інтернеті, а молоде населення буде навчати, займатись дистанційною освітою - важко.

Тому тут є пропозиція залучити три пласти населення:

- 1) Волонтери (Залучення певних волонтерських організацій, для початкової фази проекту);

2) Студенти педагогічних ВНЗ (за принципом випускників-бюджетників медичних ВНЗ, під час практики, студенти будуть відточувати свої соціальні навички в даному проекті);

3) Соціальні робітники (Так само під виглядом практики, чи державних відробіток).

Моя праця з впливом часу буде розвиватись, та набувати нових думок та компромісів у вирішенні даної проблеми, але все ж головною тезою моєї праці є: Доступ до інтернету - доступ до розвитку!

Список використаних джерел:

1.URL:https://www.google.com/url?q=https://2018.stateofeuropeantech.com/chapter/europes-got-talent/article/people-power/&sa=D&ust=1570560829873000&usg=AFQjCNG1GLw5TZ_KSmLowabjz5afTxLTVw

2.URL:<https://www.google.com/url?q=https://uk.wikipedia.org/wiki/%25D0%259D%25D1%2596%25D0%25B4%25D0%25B5%25D1%2580%25D0%25BB%25D0%25B0%25D0%25BD%25D0%25B4%25D0%25B8&sa=D&ust=1570560829873000&usg=AFQjCNHDzg4sTxi4QWnO67rlSlcClChrgQ>

3.URL:<https://www.google.com/url?q=https://ukrainer.net/thread/peretvorennyaprostoriv/&sa=D&ust=1570560829868000&usg=AFQjCNFsFwV7dE9GhzYeDDo5o7DvF5zIoQ>

4.URL:https://www.google.com/url?q=https://inau.ua/sites/default/files/file/1903/dani_ustanovchyh_doslidzhen_za_1-y_kvartal_2019_0.pdf&sa=D&ust=1570560829872000&usg=AFQjCNHAdFNzVflmQFURp1cg5YDK3r_qqw

5.URL:https://www.google.com/url?q=https://ec.europa.eu/regional_policy/en/policy/what/glossary/e/european-agricultural-fund-for-rural-development&sa=D&ust=1570560829874000&usg=AFQjCNH7a0E8UuawW0IsvRc_dXRNgmYzww

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

Климчук М., студентка БФ КПП ім Ігоря Сікорського

Науковий керівник: Фурашев В. М., доцент кафедри ІППІВ КПП ім. Ігоря Сікорського, к.т.н., с.н.с.

ШАХРАЙСТВО В ГЛОБАЛЬНІЙ МЕРЕЖІ ІНТЕРНЕТ

На сьогоднішній день в сучасному інформаційному суспільстві відбувається дуже активний розвиток різноманітних інформаційних технологій і у зв'язку з цим значного розвитку зазнала і глобальна мережа Інтернет.

28 років тому, 12 березня Тім Бернес Лі заснував всесвітню паутину Інтернет. Він прагнув створити відкриту платформу, якою зможуть

користуватися люди з будь-яких куточків світу. З того часу багато, що змінилося. Так, ніхто наразі і уявити собі не може життя без Інтернету, але на жаль, не всі ми знаємо і розуміємо, яку небезпеку ця мережа може принести. Яка небезпека може нас спіткати під час користування цією мережею [1].

Кількість користувачів мережею Інтернет зростає з кожним днем, а от, що стосується безпеки персональних даних, розповсюдження хибної інформації, політичної пропаганди, шахрайства – залишаються відкритими серйозними проблемами.

Я б хотіла найбільш широко розкрити проблему, яка пов'язана саме з шахрайством, бо Інтернет – це не тільки мережа, в якій ми можемо комунікувати один з одним, ділитися світлинами, вести блоги, але це й ще чудова мережа, в якій можна непогано заробити злочинним способом.

Перше, і найбільш сумне, це коли шахраї під виглядом благодійних фондів, приватних зборів на лікування, намагаються видурити у людей кошти. Тому аби якимось чином захистити себе від такого обману, потрібно перш ніж віддавати комусь свої кошти впевнитися, що той чи інший фонд дійсно займається допомогою людям. Потрібно завжди перевіряти інформацію про те, куди підуть ваші кошти, дізнаватись про детальні звіти про надходження і витрати компаній, а також знайти детальну інформацію про людину чи благодійний фонд. Якщо це буде приватна організація, вона завжди розповість вам про себе і про свій рід діяльності, на відміну від шахраїв, які просто здійснюють шум навколо і при цьому не надають жодної інформації про організацію.

Наступна область в якій найчастіше оперують шахраї це інтернет магазини та розіграші в різних соціальних мережах. В даному випадку, щоб якимось чином захистити себе та своїх рідних, потрібно уникати підозрілі сайти з гарною рекламою, низькими цінами та вигідними пропозиціями, адже є чудова приказка, що скупий платить двічі.

Різноманітні повідомлення типу – «Ваш акаунт заблоковано» або «Ваш акаунт зломали», теж найчастіше є ділом рук шахраїв. Вони відразу починають пропонувати відновити ваш акаунт за гроші, або користуючись довірою близьких людини, починають вигадувати різноманітні історії. Ні в якому разі не можна довіряти такому роду повідомленням і пересилати кошти, поки ви не поспілкуєтесь з людиною особисто.

Використання електронних гаманців дуже зручно в наш час, так як можна здійснювати покупки не виходячи з власного будинку, але і тут підстерігають шахраї. В даному випадку потрібно просто розуміти, що жодна платіжна система не спроможна втратити ваші облікові записи, тому якщо вам

приходить смс, в якій вас просять надати детальну інформацію, то це вже повинно служити дзвіночком про те, що вас хочуть обдурити.

Ще одним розповсюдженим видом шахрайства є так званий фішинг, при якому данні користувача знаходяться у небезпеці через фальшиві шахрайські сайти чи мобільні додатки. В більшості випадках зловмисники створюють копії сайту і розповсюджують його за допомогою посилань. Тож аби захистити себе потрібно, перед тим як переходити кудись за посиланням перевіряти коректність адреси.

Тому, можна дійти до висновку, що Інтернет це глобальна мережа, якою користується кожна друга людина в усьому світі. Ми не можемо уявити собі жодного дня без соціальних мереж, без перегляду стрічки новин. Інтернет дав нам змогу не виходячи з дому здійснювати покупки, чи поповнювати рахунок. Але якщо поглянути на інший бік медалі, то за мережею Інтернет криється чимало небезпеки, про яку багато з нас навіть не замислюється і однією з них є проблема шахрайства. Отже, потрібно вміти відрізнити де правдива інформація, а де вас намагаються обдурити і поцупити ваші кошти.

Список використаних джерел:

1. <https://utmagazine.ru/posts/20358-tim-berners-li-osnovnye-problemy-globalnoy-seti-internet>
2. <https://sales-generator.ru/blog/vidy-moshennichestva-v-internete/>

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

Фарадж Д. Ю., студент ФСП КПІ ім. Ігоря Сікорського

Науковий керівник: Фурашев В. М., доцент кафедри ІППІВ КПІ ім. Ігоря Сікорського, к.т.н., с.н.с.

НЕГАТИВНИЙ ВПЛИВ ІНТЕРНЕТУ НА ПІДРОСТАЮЧЕ ПОКОЛІННЯ

На сьогоднішній день Інтернет є невід'ємною частиною нашого життя, без якої молодь не уявляє своє існування. Кожного ранку прокидаючись ми беремо в руки гаджети та заходимо в браузер, ми вже живемо ніби по алгоритмам, ніби запрограмовані вже на те щоб постійно сидіти в мережі Інтернет. Інтернет для нас сьогодні – це перегляд новин, спілкування, онлайн покупки і т. д. Це вже як частина нашого життя, без якої ми «не виживимо». Значну кількість часу ми витрачаємо на перебування в Інтернеті. Сучасна молодь настільки звикла користуватись Інтернетом, що можна сказати, що вона просто «живе» ним. З розвитком популярності інтернету а також віртуального життя, поступово починають забувати про реальне життя,

зокрема спілкування, виховання та елементарні правила етикету тим самим все більше та більше занурюються у віртуальний світ.

Підростаюче покоління розглядає Інтернет як основне джерело інформації й головний засіб комунікації. Молодь виходять в онлайн для пошуку певних корисних відомостей, новин і роботи, спілкування з друзями, знайомиться з піснями хітами та фільмами, здійснюють покупки в інтернет-магазинах, а також використовують його нескінченні можливості для самовираження та соціальної адаптації.

Процес негативного впливу Інтернет-середовища на свідомість людини, може призвести до трагічних наслідків. Розглянемо найголовніші недоліки впливу Інтернет-середовища:

Створення ілюзії

- Чим частіше дитина проводить час в інтернеті, тим рідше він знаходиться на вулиці, граючи в активні ігри, спілкуючись з однолітками, відчувачи при цьому тактильний контакт і живі емоції.

Безкарність

- Люди в Інтернеті почуваються в повній безпеці, вони знають, що їм не буде ніякого покарання за необдумані коментарі або за нецензурне спілкування з опонентами.

Соціальні мережі

- Чим більше людина перебуває в соціальних мережах тим скоріше уповільнюється процес її інтелектуального розвитку. Спілкування в соціальних мережах є жалюгідною імітацією повноцінного діалогу.
- Довготривале перебування у соцмережах може потягнути за собою те що людина сильніше починає залежати від громадської думки, не маючи своїх думок.

Здоров'я

- Перераховуючи негативні сторони впливу Інтернету на підростаюче покоління та на людину в цілому, не слід забувати і про здоров'я. Зір, слух, серцево судинна система у постійних користувачів глобальної Мережі завжди страждають.

Інтернет залежність

- Інтернет-залежність – це такий психологічний стан, який полягає у тому, що людина перетворюється на зомбі і в неї виникає бажання постійно перебувати в інтернеті.
- Наслідком є те, що люди, які багато часу проводять в мережі Інтернет, можуть почати брехати колегам, друзям або навіть членам своєї сім'ї.
- Інтернет-залежність ґрунтується на основі використання Інтернету як засобу задоволення людиною певних власних потреб, які не можна задовольнити іншими шляхами в реальному житті.

Інтернет-залежність має крайню ступінь негативних наслідків, а саме перетворення людей (в першу чергу, підлітків) в «Інтернет-мауглі».

Людина з синдромом мауглі – це така категорія людей (в основному, дітей\підлітків), які в силу тривалого перебування в кіберпросторі втрачають зв'язок з реальністю, інколи навіть не здатні розрізнити віртуальний та реальний світ.

Також вже існує таке поняття, як: «цифрова деменція» - це новий різновид слабоумства, люди вже не мають можливості запам'ятовувати інформацію, на будь-яке запитання яке їм поставлять вони будуть шукати відповідь в інтернеті не задумуючись над ним.

Безумовно, у сучасних умовах неможливо (та й неправильно) ізолювати молоду людину від використання Інтернет-ресурсів. Однак повинні бути продумані шляхи нейтралізації негативного інформаційного впливу комп'ютерних мереж.

- В першу чергу батьки мають більше часу приділяти своїм дітям та не привчати тих з малку до гаджетів з доступом до мережі Інтернет, або хоча б обмежувати такий доступ..
- Інтернет це не завжди погано, тому батьки мають навчити своїх дітей правильно користуватись ним та використовувати в правильному напрямку.

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

*Натяжний Я. М., Студент ХТФ КПІ ім.
Ігоря Сікорського*

*Науковий керівник: Радзієвська О. Г.,
старший науковий співробітник Науково-
дослідного інституту інформатики і
права НАПрН України, к. ю. н.,*

ШТУЧНИЙ ІНТЕЛЕКТ: ПРОБЛЕМИ РЕГУЛЮВАННЯ

З моменту створення релігій та міфів пройшло багато часу, проте дещо залишилося незмінним – наше бажання до самовдосконалення. Хтось хотів мати гостроту розуму Гефеста, красу Афродіти і т.д. Це один із багатьох факторів, котрі привели нас туди, де ми знаходимося зараз. Це наше минуле, оскільки: «Під час Аграрної революції людство відібрало мову в тварин і рослин та перетворило гранд-оперу анімів на діалог між людиною й богами. Під час Наукової революції люди змусили замовкнути і богів. Світ став шоу однієї людини»[1, ст. 122].

На даний момент людство створює все більше й більше нових технологій, які наближать нас до можливостей древніх богів. Однією з таких є штучний інтелект(АІ).

Некомпетентні журналісти друкують статті з сенсаційними заголовками, що завтра ми станемо рабами своїх же творінь. Фільми «Голівуду» також лякають своїх глядачів цією тематикою. Багато вчених намагалися стати передвісниками, наприклад Герберт Саймон. В 1965 році він промовив наступне: «Не пізніше, як за двадцять років машини зможуть виконувати будь-яку роботу, яку виконує людина»[2, ст.89]. Проте навіть у 2019 році машини не можуть досягнути повного функціоналу звичайної людини. Однак не все так жахливо як здається на перший погляд.

По-перше, неорганічний терор не відбудеться миттєво, на створення повноцінного AI можуть піти не роки, а десятки років. «Тридцять років тому творці штучного інтелекту заявляли, що супер розумні роботи от-от у нас з'являться. Потім дійсність це спростовує, і загальний інтерес до теми AI спадає»[2, ст.89]. Тобто поява розумних машин великою мірою залежить не тільки від технологічного становища, а й від інтересу суспільства.

По-друге, попри відсутність широкого застосування штучного інтелекту в сучасному реальному житті, уже розробляються нормативно-правові бази, що спрямовані на врегулювання суспільних відносин, які пов'язані з використанням AI. Штучний інтелект сьогодні існує лише умовно, тільки у рядках коду. Але чим більший код тим досконаліший механізм дії.

Одна із найімовірніших схем майбутнього – мирне співіснування людини розумної та штучного інтелекту. На початку можливу агресивну поведінку AI будуть регулювати спеціальні механізми, щось на зразок кнопки вимкнення, як на персональному комп'ютері. Із плином часу можливий сценарій злиття нашого органічного світу з неорганічним. Саме в цей момент, вище названий пристрій безпеки стане непотрібним. Таким чином, ми знову проведемо Дарвінські механізми еволюції і перейдемо на новий етап розвитку.

Початок свого шляху штучний інтелект отримав після подій Другої світової війни. У 1950-х роках з'явилися перші електронні комп'ютери. Саме тоді вчені з різних наукових галузей задумалися над створенням машини, котра ні в чому не поступається людині. На той час дослідження в області неврології показали, що мозок – це сукупність нейронів з відповідними зв'язками.

У той же час Алан Матісон Тюрінг припустив, що всі види розрахунків можливо відтворити в цифровому вигляді. У 1950-му році А. Тюрінг публікує статтю «Computing Machinery and Intelligence». Головним тезисом цієї статті стала думка: чи може AI мислити як людина. Саме тут науковець вперше опублікував свій легендарний тест, який на даний момент має багато інтерпретацій.

Поняття «Штучний Інтелект» і дисципліна «Дослідження штучного інтелекту» були впроваджені 1956 року на конференції в Дартмутському коледжі.

Сьогодні для створення програм AI використовують такі мови програмування: Python, C++, Haskell та інші.

За даними Frost & Sullivan, лідером по сумі інвестицій в розвиток технології AI і кількістю укладених угод залишається США, за яким слідує Китай»[3](*інформація за останні два роки*).

Дуже важко говорити, а тим паче створювати закони для того, що не існує. Саме з такою проблемою сьогодні зіткнулися органи, завдання яких – розробити універсальну «конституцію» для AI.

Перша проблема – якого статусу набудуть наші неживі творіння. У цьому напрямку є декілька варіантів:

- особливий вид майна;
- юридична особа;
- нова правова категорія.

Особливий вид майна – відповідати за дії штучного інтелекту будуть господарі.

Юридична особа – застосування норм, які використовуються, на даний момент, для людей.

Нова правова категорія – AI матиме, виключно, свою правову базу.

Наступною проблемою є неможливість передбачати абсолютно всі фактори, котрі спрямовані на завдання шкоди людині. Даний пункт впливає із вислову П. Морхата, який зазначив: «Дуже важко говорити, а тим паче створювати закони для того, що не існує»[4].

«Також для впровадження штучного інтелекту в сфері життя людини існують наступні перешкоди:

- проблеми стандартизації систем AI;
- проблеми ліцензування;
- проблеми забезпечення персональних даних;
- проблеми забезпечення дотримання норм професійної етики»[4].

Підсумовуючи, хотілось би зазначити, що на даний момент регулювання штучного інтелекту є однією з найскладніших тем. Нормативно-правові та законодавчі акти, які стосуються цієї тематики існують тільки у вигляді чернетки. Проте дуже добре, що ми працюємо над цим саме зараз на випередження. Такий підхід дозволить зменшити кількість постраждалих від неврегульованості суспільних відносин у майбутньому і надасть змогу максимально ефективно співпрацювати з нашими творіннями. Створені сьогодні нормативно-правові акти, безумовно, матимуть велику кількість правок та додатків у подальшому у зв'язку з розвитком AI та виникненням

нових загроз співіснування людини та штучного інтелекту. Однак, на моє глибоке переконання в кінці шляху нас чекає повне визнання AI собі рівнею.

Список використаних джерел:

1. Ювал Ной Харарі. Homo Deus. / пер. з англ. О.Дем'янчука. м. Київ, Форс Україна, 2018. 512 с. Ст. 122.
2. Мічіо Кайку. Фізика майбутнього. / Переклала з англ. Анжела Кам'янець. м. Львів: Літопис, 2017. 432с. Ст.89.
3. Искусственный интеллект (мировой рынок). // TAdviser від 14.08.2019.UDL:#40.25_.D0.B5.D0.B2.D1.80.D0.BE.D0.BF.D0.B5.D0.B9.D1.81.D0.BA.D0.B8.D1.85_.D0.98.D0.98-.D1.81.D1.82.D0.B0.D1.80.D1.82.D0.B0.D0.BF.D0.BE.D0.B2_.D0.BD.D0.B5_.D0.B8.D0.BC.D0.B5.D1.8E.D1.82_.D0.BE.D1.82.D0.BD.D0.BE.D1.88.D0.B5.D0.BD.D0.B8.D1.8F_.D0.BA_.D0.B8.D1.81.D0.BA.D1.83.D1.81.D1.81.D1.82.D0.B2.D0.B5.D0.BD.D0.BD.D0.BE.D0.BC.D1.83_.D0.B8.D0.BD.D1.82.D0.B5.D0.BB.D0.BB.D0.B5.D0.BA.D1.82.D1.83
4. Морхат П. М. К вопросу о специфике правового регулирования искусственного интеллекта и о некоторых правовых проблемах его применения в отдельных сферах. URL: <https://cyberleninka.ru/article/v/k-voprosu-o-spetsifike-pravovogo-regulirovaniya-iskusstvennogo-intellekta-i-o-nekotoryh-pravovyh-problemah-ego-primeneniya-v-otdelnyh>

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

Олексенко М. П., студент ХТФ КПІ ім. Ігоря Сікорського

Науковий керівник: Радзівська О. Г., старший науковий співробітник Науково-дослідного інституту інформатики і права НАПрН України, к. ю. н.,

КІБЕРБЕЗПЕКА В КРАЇНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

Кіберпростір розвивається дуже нестримно і вже давно став частиною нашої повсякденності. Кібернетичне середовище дає нам безліч можливостей починаючи від спілкування і закінчуючи різними видами професійної діяльності. Підвищення кількості взаємозв'язків між учасниками суспільних інформаційних відносин, активне використання кіберпростору призвело до збільшення рівня кіберзлочинності. Це привело до активного розвитку та впровадження заходів кібербезпеки в усьому світі. Розглянемо методи протидії кіберзлочинності в країнах Європейського Союзу (ЄС).

Кібербезпека – це елемент інформаційної безпеки. У межах кібербезпеки вивчаються процеси формування, функціонування і еволюції кібероб'єктів, виявлення джерел кібернебезпек, що утворюються при цьому, визначення їх характеристик, а також їх класифікацію і формування правових норм, виконання який гарантуватиме захист кібероб'єктів від виявлених і вивчених

джерел кібербезпеки.

Європейські суспільства все більше залежать від електронних мереж і інформаційних систем. Розвиток інформаційно-комунікаційних технологій призвів не лише до розширення інформаційних можливостей суб'єктів суспільних відносин, але також до розвитку злочинної діяльності, яка становить загрозу як громадянам, підприємствам, урядам, так і критично важливій інфраструктурі кожної держави та міжнародному співтовариству загалом.

Кіберзлочинність складається із злочинних дій, які здійснюються в Інтернеті з використанням мереж електронних комунікацій і інформаційних систем. Це проблема без меж, яка може бути класифікована в трьох широких визначеннях:

1. атаки на інформаційні системи або фішинг (наприклад, підробні банківські сайти для отримання паролів, що забезпечують доступ до банківських рахунків жертв);
2. інтернет-шахрайство і підробка. (Великомасштабне шахрайство може бути здійснене в Інтернеті за допомогою таких інструментів, як крадіжка особистих даних, фішинг, спам і шкідливий код);
3. незаконний онлайн-контент, включаючи матеріали про сексуальне насильство над дітьми, розпалювання расової ненависті, підбурювання до терористичних актів і прославлення насильства, тероризму, расизму і ксенофобії.

З метою боротьби з кіберзлочинністю у ЄС було розроблено нові нормативно-правові акти та запроваджено оперативну співпрацю у рамках Стратегії кібербезпеки ЄС. Повідомлення Як вказано в повідомленні "Стійкість, стримування і захист: створення сильної кібербезпеки для ЄС", що ґрунтується і на основі Стратегію кібербезпеки ЄС, Європейська комісія продовжує роботу по ефективному кіберстримуванню у ЄС, у тому числі шляхом полегшення транскордонного доступу до електронних доказів для кримінальних розслідувань.

Серед основних нормативно-правових актів ЄС, які сприяють боротьбі з кіберзлочинністю, слід виділити наступні:

- *Директива про атаки на інформаційні системи* (2013 р.), метою якої є боротьба з великомасштабними кібератаками, вимагає від держав-членів посилення національних законів про кіберзлочинність і введення жорсткіших кримінальних санкцій. У 2017 році Комісія опублікувала звіт, в якому оцінюється, в якому ступені держави-члени вжили необхідні заходи для дотримання Директиви.
- *Директива про боротьбу з сексуальною експлуатацією дітей в*

Інтернеті і дитячій порнографії (2011 рік), у якій докладніше розглядаються нові події в онлайн-середовищі, такі як грумінг (злочинці зображуючи дітей заманювати неповнолітніх з метою сексуального насильства).

- *ePrivacy Directive Search* (2002 рік), відповідно якої постачальники послуг електронних комунікацій повинні забезпечувати безпеку своїх послуг і підтримувати конфіденційність інформації клієнта. У 2017 році Комісія запропонувала відмінити Директиву і замінити її Регламентом, що стосується поваги приватного життя і захисту особистих даних в електронних повідомленнях.

- *Рамкове рішення про боротьбу з шахрайством і підробкою негрошових платіжних засобів* (2001 рік), що визначає шахрайську поведінку, яку держави ЄС повинні розглядати як кримінально карні злочини. 13 вересня 2017 року Комісія запропонувала нову Директиву, спрямовану на оновлення існуючої правової бази, усунення перешкод на шляхи оперативної співпраці і посилення заходів по відвертанню і наданню допомоги жертвам, з тим, щоб правозастосовні дії проти шахрайства і підробки безготівкових платіжних засобів були ефективніші.

Також було створено **Європейський центр кіберзлочинності (European Cybercrime Center (EC3))**. Європейська комісія зіграла ключову роль в формуванні EC3, який почав свою роботу в січні 2013 року. EC3 виступає координаційним центром у боротьбі з кіберзлочинністю у Європейському Союзі, об'єднуючи європейський досвід у сфері кіберзлочинності для підтримки розслідувань кіберзлочинів в державах-членах і забезпечуючи колективний голос європейських слідчих по кіберзлочинності в правоохоронних і судових органах.

Сьогодні кожна держава намагається створити власну систему боротьби із кіберзлочинністю. Створюється законодавча та нормативно-правова база, зокрема:

- *Закон про кіберзлочинність* - Південна Африка (Південна Африка підписала Будапештську конвенцію в 2001 році)
- *Закон про обмін інформацією про кібербезпеку (CISA)* - Сполучені Штати Америки.
- *Директива ЄС про мережу і інформаційну безпеку.*
- *Закон про кіберзлочинність*, 2001, Австралія.
- *Глава 08: 06 (Кіберзлочинність і комп'ютерні злочини)* Ботсвана
- *Закон про неправомірне використання комп'ютерів*, 2007 рік, Бруней-Даруссалам.
- *Закон про кібербезпеку*, Китай.
- *Закон про комп'ютерні злочини*, Малайзія.
- *Закон про попередження кіберзлочинності*, 2012 рік, Філіппіни

- *Закон про комп'ютерний злочин*, Таїланд.
- *Закон про кіберзлочинність*, 2015 рік, Танзанія.
- *Закон про неправомірне використання комп'ютеру*, 2013 United States Code США.

Українській владі варто більш активно розвивати власну систему кібербезпеки, створювати спеціальні структури та запроваджувати заходи, які будуть попереджувати злочини у кіберпросторі як проти звичайних громадян, так і проти держави. Для створення ефективної системи протидії кіберзлочинам недостатньо декларативних нормативно-правових актів, які існують на сьогодні. Слід розробити систему та дієві механізми заходів протидії кіберзлочинам з відповідним відображенням у нормативно-правовому полі. Ґрунтовний аналіз наведений правових актів Європейського Союзу та законодавчих актів інших країн допоможе Україні у формуванні нормативно-правової основи та налагодження механізмів взаємодії у питання подолання кіберзлочинності.

Список використаних джерел:

1. Офіційний сайт Європейського Союзу. URL: ec.europa.eu

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

Крюкова Є. О., студентка ХТФ КПІ ім. Ігоря Сікорського

Науковий керівник: Радзієвська О. Г., старший науковий співробітник Науково-дослідного інституту інформатики і права НАПрН України, кандидат юридичних наук

ЕЛЕКТРОМОБІЛЬ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Електромобілі - це частина майбутнього. Вони «вміють» те, на що не здатні авто з двигуном внутрішнього згорання. Створюються усі умови для зручного та безпечного, у тому числі для природи, користування електромобілями.

За даними інформагентства "Інтерфакс-Україна", попит на електромобілі в Україні в першій половині 2019 року, в порівнянні з попереднім роком, зріс на 58 %. У минулому році українці придбали 5,3 тисячі електрокарів, що майже вдвічі більше, ніж до 2017 році. Однак на тлі загальної цифри зареєстрованих в Україні авто ця цифра виглядає незначною. Загалом 2018 року в країні було вперше за реєстровано близько 200 тисяч автомобілів [1].

Вважається, що головною перевагою електромобіля є його екологічність та безпечність для навколишнього природного середовища. Але є і недоліки: електромобілі можуть становити ще більшу небезпеку для довкілля, ніж

звичайні авто. Норвезький університет наук і технологій довів це. Вчені у дослідженні вивчили вплив на навколишнє середовище процесу виготовлення та експлуатації звичайних авто та електромобілів. Заводи, на яких виробляють електромобілі, викидають більше токсичних відходів, ніж виробники звичайних авто. Використання вугілля для вироблення енергії для електромобіля створює парниковий ефект.

Співавтор дослідження професор Андерс Хаммер Сторман пояснив, що під час збірки електромобілей підприємство викидає вдвічі більше парникових газів, ніж складаючи звичайне авто.

Крім цього, окрему небезпеку становить виробництво акумуляторів та електромоторів, оскільки потребує більшої кількості токсичних речовин нікелю, міді та алюмінію, які збільшують ризик окислення ґрунту.

За словами Стормана, у багатьох факторах впливу на виникнення кислотних дощів, смогу, токсичності екосистеми та скорочення природних ресурсів електромобілі потенційно більш небезпечні, ніж звичайні автомобілі.

Тим не менше, у деяких випадках електромобілі все ж корисні, зазначили вчені.

Вчені зазначили, що якщо електромобіль живиться електроенергією, яку виробляють з низьковуглецевого вугілля або за допомогою альтернативних джерел енергії, то електромобіль може допомогти зменшити викиди парникових газів [2]. Зокрема у Європі, де електроенергія виробляється за допомогою різних типів палива, використання електромобілів є виправданим і шкодить навколишньому середовищу менше ніж авто з двигуном внутрішнього згорання.

На сьогодні у Франції та Великій Британії вже існують урядові програми з боротьби із забрудненим повітрям, які вказують на те, що продаж бензинових та дизельних автомобілів після 2040 року буде заборонений. А Ізраїль планує заборонити всі бензинові та дизельні автомобілі з 2030 року та повністю прибрати податки на електромобілі.

В Україні нещодавно був зареєстрований новий законопроект у Верховній Раді під номером № 10405, який вводить зелені номерні знаки для електромобілів, отримав підпис Президента України Володимира Зеленського та став законом. Закон набуде чинності з 1 січня 2020 року. Він включає в себе такі питання як впорядкування питань руху, паркування і зарядки електромобілів. Для цього в правила дорожнього руху і державних будівельних норм повинні бути внесені відповідні зміни.

Крім того, Закон вводить штрафи за зупинку або стоянку інших авто на місці для електромобілів, а також за створення перешкод водіям електрокарів в зупинці або парковці. Розмір штрафу коливатиметься між 20 і 30

неоподатковуваними мінімумами ходів громадян, що становить в грошовому еквіваленті на сьогодні від 340 до 510 гривень. Інспекторам з парковки надається право в такому випадку затримати автомобіль порушника, в тому числі за допомогою евакуатора [3].

Для водіїв електромобілів будуть розширені можливості для більш зручного та функціонального управління, тому більшість захоче перейти на цей вид транспорту. Деякі опції щодо управління електромобілем, зокрема, контроль технічного стану чи зарядки акумулятора, стану безпеки автомобіля і т.п. можна буде здійснювати через мережу Інтернет. З часом кількість функцій віддаленого управління буде лише зростати. Тому актуальним постає питання інформаційної безпеки під час експлуатації електромобіля.

Для того щоб сказати про управління електромобілем за допомогою мережі Інтернет, потрібно зазначити, що таке Інтернет речі.

Інтернет речі – це назва, яка відповідно концепції підключення будь-якого пристрою, лампи, холодильника, всього, що ви тільки можете придумати до Інтернету. Ми бачили, як ця концепція переросла в цифровізацію і підключення багатьох побутових приладів протягом останнього десятиліття. Ще в 2012 році налічувалося від восьми до десяти мільярдів речей, які, як вважається, були підключені до Інтернету, і це число продовжує зростати з року в рік. Деякі навіть пророкують, що до 2020 року буде встановлено 24 мільярди підключених пристроїв – іншими словами, 4 пристрої на людину.

Однак, рух промислових інтернет речей (ІІР) не обмежується особистими речами або предметами домашнього вжитку. У міру того як технологія з часом розвивалася, стаючи все менше і простіше в реалізації, кількість об'єктів, якими можна керувати віддалено через інтелектуальний пристрій, збільшилася. Тепер навіть машини можуть управлятися через Інтернет за допомогою підключеного пристрою. Найважливішим аспектом є включення / вимикання даного елемента. Якщо він має цей перемикач, він майже напевно стане частиною Інтернету речей. За визначенням це означає, що майже кожне електричний пристрій може приєднатися до величезної і постійно зростаючої мережі пов'язаних об'єктів. Інтернет речі можна умовно розділити на дві категорії:

1. Інтернет мене (речі, які спілкуються з вами і через Інтернет, і через ваш смартфон. Якщо вас з вашим смартфоном немає поруч, значить, ця штука відключена від решти світу. Типовими пристроями сьогодні є розумні годинник і фітнес-трекери).

2. Все інше (в прямому сенсі це речі, які безпосередньо пов'язані з Інтернетом).

Наші пристрої та особисті речі пов'язані один з одним, а також з нами через мережу Інтернет, тому рівень нашої власної інформаційної безпеки

постійно перебуває під загрозою. Потенційні можливості для компаній скористатися нашими даними і хакерами для проникнення в наші мережі можуть рости з тією ж швидкістю, що і кількість елементів, які можна буде підключити. Якщо національне законодавство і системи забезпечення інформаційної безпеки не будуть відповідати вимогам часу, наслідки для безпеки, особистих даних і конфіденційності здаються безмежними. Це ж стосується і безпеки транспортного засобу, водія, який є учасником дорожнього руху, та інших, задіяних у цьому процесі.

Небезпека, ймовірно, є однією з перших потенційних пасток, які приходять на думку, коли ми думаємо про Інтернет речей. Збільшення числа підключених пристроїв автоматично збільшує кількість точок входу і можливостей для злочинців.

Якщо хакери потенційно можуть отримати доступ до наших пристроїв, а також до наших телефонів або комп'ютерів, тоді на що ми можемо сподіватися щодо наших банківських реквізитів, медичних записів або іншої особистої інформації? Навіть якщо ми не піддаємося нападу особисто, наші пристрої можуть використовуватися злочинцями без нашого відома або згоди. У масштабах дорожньо-транспортного руху, є підстави стверджувати, що дистанційний злам програмного забезпечення електромобіля становитиме реальну загрозу життю та здоров'ю як його водія та пасажирів, так й інших учасників руху.

Крім того збір даних через наші цифрові пристрої та незаконне їх використання теоретично може бути зроблено повністю без нашого відома. Ці дані потім можуть бути використані, наприклад, страховими компаніями при визначенні того, які поліси нам дозволено приймати, або університетами при виборі між заявниками. Що стосується електромобіля, то незаконне використання даних про його технічний стан, місцезнаходження, маршрутизації може стати предметом протиправних посягань, шахрайства та інших злочинних діянь, що здатні завдати матеріальної чи моральної шкоди власнику транспортного засобу.

У той час як деякі закликають до державного законодавства, вже є ряд компаній, що працюють над рішеннями для підвищення безпеки підключених пристроїв [4]. Це переважно техніко-технологічні заходи, які потребують ліцензування та нормативно-правового врегулювання.

Електромобілі – це наше майбутнє. У подальшому вони будуть лише удосконалюватися і стануть невід'ємною частиною нашого буття. Для успішного та безпечного їх запровадження необхідно уже сьогодні звернути особливу увагу на питання безпеки, зокрема питання інформаційної безпеки.

Список використаних джерел:

1. Електромобіли в Україні будуть с зеленими номерами. Президент підписав закон. // *Українська служба Deutsche Welle* від 07.08.2019. URL: <https://www.google.com/amp/s/tsn.ua/ru/amp/ukrayina/elektromobili-v-ukraine-budut-s-zelenymi-nomerami-prezident-podpisal-zakon-1390662.html>
2. https://ipress.ua/news/elektromobili_shkodyat_ekologii_bilshe_nizh_zvychayni_avto_9135.html
3. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66116
4. <https://medium.com/high-mobility/a-beginners-guide-to-the-internet-of-things-connected-cars-and-the-future-of-mobility-11a10449ee4f>

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