Комітет Верховної Ради України з питань інформатизації та зв'язку

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

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

Інтернет речей: проблеми правового регулювання та впровадження

Друга науково-практична конференція
29 листопада 2018 року

Київ
КПІ ім. Ігоря Сікорського
2018

УДК 34:004](06)
І-73

І-73 **Інтернет речей: проблеми правового регулювання та впровадження :** Матеріали другої наук.-практ. конф., 29 лист. 2018 р., м. Київ / Упоряд. : В. М. Фурашев, С. О. Дорогих. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. – 168 с.

ISBN 978-966-622-921-5

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 в умовах застосування технологій Інтернету речей, зокрема із використанням штучного інтелекту, робототехніки, криптовалют, технологій блокчейн, «хмарних» технологій, «великих даних» тощо, а також питань інноваційного застосування ІКТ в юридичній діяльності та проблем вдосконалення законодавства з питань інформатизації, телекомунікацій, користування радіочастотним ресурсом, захисту персональних даних, інфраструктурної безпеки, кібербезпеки тощо.

Участь у конференції взяли провідні експерти і 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

Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП КПІ 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 № 10 від 26.12.2018 р.

Вченою радою факультету соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Протокол № 5 від 03.12.2018 р.

ISBN 978-966-622-921-5

З М І С Т

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

РОЗВИТОК ІНТЕРНЕТУ РЕЧЕЙ ЯК ФАКТОР ТРАНСФОРМАЦІЇ СИСТЕМИ ВИЩОЇ ОСВІТИ

В сучасному науковому та повсякденному обігу понятійний блок «Інтернет речей» (англ. Internet of Things, IoT) вже став доволі узвичаєним і використовуваним. Проте вплив цього феномену на всі сфери життєдіяльності людини і суспільства досліджено ще не достатньо.

Роль IoT в майбутньому доволі яскраво охарактеризована в Звіті Міжнародного союзу електрозв'язку (ITU) наступним чином: «Інтернет речей значно розширить цифровий слід. Крім людей, організацій та інформаційних ресурсів, вони об'єднуватимуть об'єкти, обладнані можливостями зйомки, обробки та зв'язку. Ця широкомасштабна інфраструктура створить численні дані, які можуть бути використані для підвищення ефективності виробництва та розподілу товарів і послуг, а також для покращення життя людей інноваційними способами» [1]. Здавалося б, переваги поширення Інтернету речей очевидні: суттєве полегшення життя людини, створення людині більш комфортніших умов її діяльності. Проте не варто скидати з рахунків і недоліки поширення IoT. Йдеться, наприклад, про формування такого феномену (хвороби), який має назву «цифрова деменція». Вона характеризується, зокрема, й тим, що людина вирішуючи будь-яку повсякденну або виробничу задачу апелює вже не до свого інтелекту і здібностей, а покладається суто на рішення пропоновані в мережі Інтернет. Неструктуроване і несистематичне спостереження за дітьми шкільного віку та студентами дає змогу говорити про реальність такої загрози. В цьому контексті, на перший план виходить проблема готовності сучасної людини діяти в нових умовах, вміти співвідносити себе з реальністю Інтернету речей. На наш погляд, сучасна система освіти ще занадто інертна щоб змогти підготувати індивіда до нових викликів і загроз.

Часто дослідження проблематики Інтернету речей пов'язують з питаннями формування і розвитку штучного інтелекту. При цьому нерідко дослідники вдаються до змальовування доволі загрозливих сценаріїв для людства, коли штучний інтелект стане протистояти людині і, навіть, зможе знищити її. Ймовірність (або неймовірність) того, що штучний (машинний) інтелект стане колись розумніший від людини обґрунтував відомий філософ 20-го століття Е.В. Ільєнков в роботі «Про ідолів та ідеали». Філософ певною мірою іронії вказував, що: «Якщо вам дуже вже хочеться створити машинний інтелект, хоча б рівний людському, то ви повинні почати з того, щоб навчити його «витримувати напругу суперечності» – стан А–не–А, у вигляді якого завжди виражається всередині кінцевого формалізму факт його «кінцівки», тобто його конфлікту з

конкретним різноманіттям явищ природи та історії» [2]. Тобто, враховуючи той факт, що машина «мислить» логікою математичною, а людина здатна (якщо будуть створені відповідні умови її поставання, зокрема і в системі освіти) осягати діалектичні суперечності, то в цьому сенсі «перевага» залишається на боці людини. Іншою умовою формування повноцінного штучного інтелекту філософ вважав таке: «Щоб створити штучний розум, хоча б рівноцінний людському, доведеться створювати зовсім не модель окремого «мислячого тіла», не модель індивіда, а модель всього того грандіозного «тіла» культури, всередині якого індивід з його двадцятьма мільярдами клітин мозку сам є всього-на-всього тільки «клітиною», яка сама по собі здатна «мислити» так само мало, як і окремий нейрон ...» [Там само]. В цьому сенсі, треба відповісти на питання: Чи може вважатися такою самостійною машинною цивілізацією вся Інтернет мережа, включно зі створеним контентом та всім масивом об'єднаних в ній технічних пристроїв? Ми не беремося дати однозначну відповідь на це питання.

Ще одним недоліком розвитку Інтернету речей є вразливість людини до загроз інформаційній безпеці та зростання ризиків, пов'язаних з конфіденційністю. Адже не кожен користувач сервісів IoT володіє компетентностями протистояти вказаним вище загрозам.

Трансформація системи освіти, на наш погляд, повинна здійснюватися таким чином, щоб забезпечити в майбутньому можливість формування діалектично мислячих людей, які, користуючись усіма перевагами IoT, зможуть протистояти загрозам, що пов'язані з його розвитком.

Використана література:

1. Measuring the Information Society Report. Volume 1. 2017. – С. 94. Електронний ресурс. Режим доступу https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf

2. Ильенков Э.В. Об идолах и идеалах. 2-е изд – К.: Час-Крок., 2006. Режим доступу: http://libelli.ru/works/idols/11.htm.

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

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

ІДЕНТИФІКАЦІЯ РОБОТА З ШТУЧНИМ ІНТЕЛЕКТОМ ЯК СУБ'ЄКТА ПРАВА

В літературі надано багато визначень терміну «штучного інтелекту», за підрахунками експертів загальна яких кількість перевищує півтори сотні. І цей факт має не складне пояснення. Штучний інтелект – явище в науці та практиці, яке з'явилося не так давно, але привернуло увагу багатьох вчених з різних галузей

знань завдяки складності завдань щодо його дослідження, а ще и безмежними перспективами його можливого застосування.

Узагальнюючи різні погляди на зміст зазначене явище, сформулюємо загальну мету створення штучного інтелекту – це копіювання (моделювання) роботи людського мозку (інтелекту, розумової діяльності тощо) за рахунок відтворення когнітивних функцій еквівалентних (тотожних) за критеріями, характеристиками і показниками когнітивним функціям людини.

За різними джерелами до переліку когнітивних функцій людини можна віднести:

- сприйняття, запам'ятовування, обмін інформацією;
- зіставлення, оцінювання, аналіз, узагальнення і використання інформації (даних);
- вибір стратегії і конкретних дій, експертна оцінка ситуації;
- визначення мети, планування, прийняття рішень;
- перетворення тексту в мову і навпаки;
- розпізнавання об'єктів і їх класифікація (гносиз);
- планування та здійснення цілеспрямованої рухової діяльності (праксис);
- самонавчання, самоорганізації, генерування нових знань тощо.

Вважається, що ШІ, який має можливості реалізовувати праксис як КФ, обов’язково повинен бути інтегрований з відповідною технічною системою (виконавчими пристроями та сенсорами) [1]. Таке об’єднання ШІ та технічних систем має назву роботів, яка широко використовується в літературі та практиці.

З метою подальшого проведення досліджень в сфері права надаємо наступне визначення: ***штучний інтелект (ШІ)*** *– 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) еквівалентні когнітивним функціям людини*.

Досить впевнено можна припусти, що штучний інтелект з повним набором КФ буде мати змогу самостійно (без участі людини):

- визначати як стратегічну мету діяльності, так і ціль конкретних дій;
- аналізувати, прогнозувати, планувати, приймати і виконувати рішення;
- адаптувати власну поведінку до змін зовнішніх та внутрішніх умов;
- навчатись, організовуватись, адаптуватись, перебудовуватись, розвиватись тощо;
- приймати участь в складних, багатовимірних процесах;
- добавляти, інтегрувати та вдосконалювати КФ в тій ступені, в якій це необхідно для виконання конкретних рішень.

В реальному житті людина здійснює певний вид діяльності, для якого необхідно мати конкретний набір КФ з характеристиками потрібної якості. Звичайно, ці якості набуваються людиною в процесі навчання та тренінгів. Для деяких КФ це відбувається протягом всього життя, для інших за певний період часу.

Людина від народження має потенційно повний набір всіх можливих КФ, які отримують розвиток протягом всього її існування відповідно до потреб, обумовлених конкретними обставинами та умовами її життя. На відміну від людини, на сучасному етапі розвитку науки, техніки та технологій ШІ програмується на наявність конкретного набору КФ з характеристиками потрібної якості. Але вже відомі дослідження щодо створення ШІ з набором певних КФ, якісні показники характеристик яких покращуються в процесі так званого його «самонавчання», тобто без участі людини. Властивості ШІ щодо «самонавчання» відкривають приголомшливі перспективи «саморозвитку» та «саморозмноження» без залучення людини.

Сформулюємо наступну гіпотезу: якщо КФ робота еквівалентні КФ фізичної особи, то робот є правовим еквівалентом фізичної особи.

В даному випадку ***робот*** *– це ШІ інтегрований з технічною системою, що дозволяє реалізовувати когнітивні функцій людини в процесі здійснення конкретного виду діяльності, пов'язаної, як правило, з однорідними об'єктами, що мають матеріальний або нематеріальний зміст.*

Широко відомі в теорії права наступні визначення:

правоздатність *– це визнана державою загальна для будь-якого суб'єкта права потенційна можливість мати юридичні права і обов'язки;*

дієздатність *– реальна персоніфікована для кожного суб'єкта права здатність своїми самостійними, усвідомленими діями отримувати для себе юридичні права і обов'язки, здійснювати їх та виконувати;*

деліктоздатність *– це здатність кожного суб'єкта права нести персональну юридичну відповідальність за скоєне ним правопорушення (делікт).*

Відповідно до Цивільного кодексу України дієздатність повнолітньої людини може бути обмежена лише за рішенням суду, як повинно базуватись на висновках судово-психіатричної експертизи.

В процесі судово-психіатричної експертизи проводяться дослідження КФ фізичної особи на основі комплексного застосування психопатологічних, патопсихологічних, нейропсихологічних і інструментальних методів. В процесі дослідження надається оцінка КФ людини шляхом визначення наявності когнітивних порушень, їх тяжкості, якісних характеристик, гостроти розвитку, динаміки їх частоти і впливу на здатність суб'єкта до довільної регуляції своєї поведінки.

Важливим є то, що негативні для визначення дієздатності людини висновки судово-психіатричної експертизи зводяться до наступного: фізична особа *не здатна свідомо і самостійно* приймати і реалізовувати рішення, які є адекватними ситуації, усвідомлювати свої дії та керувати ними, оскільки встановлено факт наявності у неї когнітивних порушень, тобто встановлено факт наявності критичного зниження характеристик і показників когнітивних функцій [2].

Водночас, задля вирішення проблеми підвищення ефективності да достовірності судово-психіатричної експертизи необхідно забезпечити для кожного методу та методики їх проведення наступне [3]:

– порушення для кожної конкретної КФ повинні мати ознаки, критерії, характеристики, показники;

– опис алгоритму визначення інтегральних оцінок за певними критеріями стану показників для досліджуваної сукупності когнітивних функцій, які були б релевантними правовому поняттю «обмежена дієздатність» з урахуванням відповідності юридичному і психологічному критеріям.

Можемо зробити узагальнюючий висновок – дієздатність фізичної особи залежить від характеристик і показників її когнітивних функцій.

Таким чином, якщо результати здійснення певної сукупності КФ або кожної окремо дають однаковий результат у випадку людини та у випадку робота з ШІ, то останній можна вважати правовим еквівалентом фізичної особи. Гіпотеза доведена.

Отже сформулюємо наступні твердження.

Твердження 1. Правосуб'єктність фізичної особи (правоздатність, дієздатність і деліктоздатність) ***презюмується***, не обмежена та не вимагає доказів за виключенням випадків визначених законом.

Твердження 2. Правосуб'єктність робота з ШІ (правоздатність, дієздатність і деліктоздатність) ***потребує доведення*** як правового еквівалента фізичної особи.

Запропонований в роботі підхід оцінки можливості визначення правосубєктності роботів з ШІ базується на наступних принципах:

1. Принцип правової еквівалентності фізичної особи (правові інститути: представництва, повіреного, управителя тощо);

2. Принцип презумпції правоздатності та дієздатності повнолітньої фізичної особи;

3. Принцип доведення необхідності обмеження дієздатності повнолітньої фізичної особи;

4. Принцип формування вичерпних вимог щодо спеціальної та галузевої правоздатності та дієздатності;

5. Принцип еквівалентності когнітивних функцій фізичної особи і штучного інтелекту;

6. Принцип визнання робота з ШІ як правового еквівалента фізичної особи;

7. Принцип доказового визнання дієздатності робота з ШІ.

Для забезпечення визначення дієздатності робота з ШІ як правового еквівалента фізичної особи необхідно проведення широких системних міждисциплінарних досліджень. Наприклад, дослідження з формування теоретико-методологічних положень проведення експертиз для:

1) окремих КФ людини, які реалізуються в роботах з ШІ;

2) окремих видів і типів КФ людини, які реалізуються в роботах з ШІ;

3) конкретної діяльності, яка може реалізуватись роботом з ШІ з відповідним набором КФ;

4) конкретних видів і типів діяльності, які може реалізуватись роботом з ШІ з відповідним набором КФ;

5) робота з супер ШІ, який здатний реалізувати будь-яку наперед невідому діяльність.

Висновок.

Визнання обґрунтованості справедливості викладеної гіпотези дозволить вирішити правові проблеми, пов'язані з роботами з 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.

Використана література:

1. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання // ІТ-право: проблеми та перспективи розвитку в Україні: збірник матеріалів ІІ-ї Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.). – Львів : НУ «Львівська політехніка», 2017. – С. 18-42.

2. Вандыш-Бубко В.В., Гиленко М.В. Когнитивные расстройства в судебно-психиатрической практике // Доктор.ру. 2013. № 5 (83). С. 86-92.

3. Илейко В. Р. Виды судебно-психиатрической экспертизы в гражданском процессе // Таврический журнал психиатрии. — 2003. — Т. 7, № 1. — С. 37–40.

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

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

ПЕРСПЕКТИВИ ВЗАЄМОДІЇ ІНТЕРНЕТУ РЕЧЕЙ ТА ІНТЕРНЕТУ ЛЮДЕЙ: ВИКЛИКИ ВІДЧУЖЕННЯ ТА ДЕГУМАНІЗАЦІЇ

«Інтернет речей» (англ. «Internet of Things»; надалі - IoT») – якісно новий етап у розвиткові кібернетичної реальності, коли вона перестає бути віртуальною і виходить у фізичний простір, у якого завжди існувала «природна людина», - Homo naturalis.

Кіберфізична реальність або IoT – це штучні пов'язання фізичних об'єктів, яких ніколи б не існувало би поза Інтернетом. Відтак фізичні об'єкти набувають «людських якостей» й зокрема - здатності обмінюватися в автоматичному режимі різноманітними даними, що є специфічним аналогом людського спілкування.

Особливим випадком IoT є *«робототехнічні агенти»* як людиноподібні (антропоморфні) автономні інтелектуальні системи, або ж системи «штучного

інтелекту», які доповнюють різноманітні механічні системи, що імітують різноманітні людські якості й зокрема:

- *рухливе тіло;*
- *органи відчуттів («сенсори»);*
- *здатність до самоуправління та самостійного прийняття рішень («штучний мозок»);*
- *здатність до комунікацій («штучні мови й канали зв'язку»).*

Так або інакше, з IoT, пов'язана проблема ймовірної дегуманізації Інтернету, а відтак дегуманізації самої людини, тобто втрати людиною своєї «першоприродної» сутності і набуття нею натомість дедалі виразніших ознак «штучності».

У філософії ця проблема традиційно формулювалася як проблема *«відчуження»* (англ. «alienation»; нім. «entfremdung»; «entäußerung»). Відповідна категорія є центральною в філософії Георга Гегеля й Карла Маркса. Відтак – вона є центральною й для філософських побудов неомарксистів, фрейдомарксистів тощо (Д'єрдь Лукач, Герберт Маркузе, Еріх Фромм та ін.).

Відчуження – це таке *опредмечування* людських якостей й результатів людської діяльності, відносин людини із нею ж створеними речами, внаслідок якого вони починають протистояти людині й навіть активно їй протидіяти, поневолювати її [1].

Особливою формою *опредмечування,* властивою товарному виробництву, є *оречевлення* («реіфікація»). Ця вперше впроваджена Карлом Марксом філософсько-соціологічна категорія означає форму соціальних відносин, за умов якої відносини між людьми набувають видимості відносин між речами.

Карл Маркс виокремлював чотири види відчуження:

- *від процесу праці;*
- *від продукту праці;*
- *від інших людей;*
- *від людського в собі* [1]

Кіберфізичні моделі перетворення соціуму й людини небезпечні тому, що на них істотний вплив справляє парадигма лінійності. В ідеалі йдеться про творення таких *«годинникоподібних» систем*, які можуть ефективно, з практично корисними наслідками, описуватись системами лінійних рівнянь. Оскільки в реальній соціальній дійсності подібних систем не так уже й багато, то доводиться, за висловлюванням Карла Поппера, із «хмар» робити «годинники». Доктрина, згідно з якою всі «хмари» є врешті-решт «годинниками», перетворилася на панівну віру серед адептів просвітницького раціоналізму, і всі, хто такої віри не поділяв, автоматично зараховувалися до реакціонерів-обскурантистів [2]. Цю віру автоматично успадкувала кібернетика.

Виходячи з оптимістичних припущень, можна стверджувати, що кіберфізичне маніпулювання оточенням людини ніколи не перетвориться на маніпулювання самою людиною, а відчуження праці, необхідним чином пов'язане з IoT, не перейде меж припустимого ризику і не загрожуватиме людській природі, тобто не призведе до втрати людиною сутнісної ідентичності.

Обґрунтуванням такого оптимізму може бути теза про те, що машини не здатні до самоорганізації й самостійного прийняття рішень. У такому разі виходить, що «бунт машин» - це лише безпідставна антиутопія. Відтак, «рожеві оптимісти» посилаються на «закони робототехніки» Айзека Азімова: «Робот не може заподіяти шкоду людині або у своїй бездіяльності допустити, щоб людина була заподіяна шкода» й т.п.

Однак, справа звичайно не в машинах і не в роботах зокрема, а в самих людях, певна частина яких не проти побудувати нову версію рабовласницького суспільства, яке цього разу називатиметься *«роботовласницьким».* І така загроза є цілковито реальною. Адже з появою «просунутого» Інтернету виросло покоління людей, переконаних в тому, що їхні проблеми і взагалі усі соціальні проблеми можуть вирішити «передові технології». Така точка зору активно підігрівається у маркетингових цілях техно-компаніями і її не проти «взяти на озброєння» політики технократичного ґатунку. Прикладом такого технократичного підходу є хоча б надмірний ентузіазм прибічників електронної системи охорони здоров'я (E-Health) в сучасній Україні. Канадський філософ українського походження Євген Морозов у цьому контексті небезпідставно стверджує: *«Чим розумнішими стають гаджети, тим тупішими стають люди»* (англ. «Smart Gadgets, Dumb Humans») [3].

Упокорення людини «Інтернетові речей», а відтак її *оречевлення* на кіберфізичних засадах може бути виправдане інтересами принесення людини в жертву «вищим цілям»: безпеки; ефективних комунікацій; життєдіяльності соціуму, сімейного будівництва нового типу й т.п.

У цьому плані особливо небезпечною уявляється перспектива гібридизації комп'ютерних і нанотехнологій. Йдеться наприклад про «розумний пил» (англ. «smart dust»): ультрамініатюрні мікросенсори, які, якщо їх розпилючити над певною територією, зможуть збирати й передавати інформацію. На засадах цієї технології в Університеті Берклі в 2016 році була опрацьована технологія *«невронального пилу»,* - «розумних» мікрочасточок, які можуть бути вживлені в нову кору людського мозку («неокортекс») й вступати у взаємодію з нейронами мозку. У 2018 році та ж сама команда дослідників просунулася далі й розробила *«штучний нерв»,* - стимулюючий пристрій (англ. «StimDust»), який може бути вживлений під шкіру людини й надавати ультразвукові сигнали [4].

Хоча усі ці технологічні інновації подаються в відкритому друкові як призначені виключно для благородних медичних цілей, але, враховуючи, що дослідження фінансує відома пентагонівська DARPA, - Агенція передових

оборонних технологій, неважко здогадатися про їх справжню ціль і всі виклики та загрози з цим пов’язані.

Використана література:

1. Отчуждение (философия) // Википедия. URL: https://ru.wikipedia.org/wiki.
2. Morozov, Evgeny. To Save Everything, Click Here: The Folly of Technological Solutionism. PublicAffairs, 2013. Ch. 9. Smart Gadgets, Dumb Humans.
3. Поппер, Карл. Логика научного исследования : пер. с англ. / К. Поппер ; под общ. ред. В. Н. Садовского. – М. : Республика, 2004. – С. 47.
4. Bush, Steve. Berkeley engineers build smallest wireless nerve stimulator // Electronics Weekly.12th April 2018. URL: https://www.electronicsweekly.com/news/research-news/berkeley-engineers-build-smallest-wireless-nerve-stimulator-2018-04/

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

Мельник І. В.,
аспірант кафедри інформаційної політики та цифрових технологій Національної академії державного управління при Президентові України

ВПЛИВ ІНТЕРНЕТ РЕЧЕЙ НА ЦИФРОВУ КУЛЬТУРУ В УКРАЇНІ

Динамічні зміни науково-технічного, соціокультурного, інформаційного характеру, складні глобальні трансформації вимагають від України вироблення та запровадження інноваційних стратегій для інтеграції в актуальні світові процеси, коли можливостями доступу до світових інтелектуальних обмінів здатні користуватися різні соціальні групи населення.

Ціннісною основою для таких процесів має бути усвідомлення того, що наш світ глобалізується, наша сучасність перебуває у стадії посилення тиску інформаційної політики та цифровізації технологій, зміни підходів до понять що таке знання, які його різновиди, обсяг та способи здобування, можливості культури, соціальних процесів, навіть щоденні звички людини.

Сучасний світ – це світ інтерактивних обмінів, взаємодій, в тому числі і інтернет речей (Internet of Things, IoT - мережу фізичних об'єктів, оснащених технологіями для взаємодії один з одним і зовнішнім середовищем), трансформацій, котрі витворюють мобільні та гнучкі віртуальні зв’язки.

У цьому контексті явище цифрової культури є знаковим, оскільки вказує на домінуючу форму соціалізації сучасного суспільства – інформаційно-віртуальну. Кінематографічний і літературний кіберпанк, постфольклор, відеоскульптура й цифрові інсталяції, техно- та електронна музика, віртуальний музей та театр, софт-арт – все це було інноваціями ще десятиліття тому, натомість тепер – це, фактично, осердя різноманітних творчих практик масової культури людства, що є показником фундаментальних змін у пізнанні людини та її творчості.

Саме під впливом масовості цифрової культури докорінно змінюється й розуміння власне культури, яка є рушієм складних цивілізаційних процесів та їх стадій (1).

Ще одним глобальним знаковим феноменем є інтернет речей, який за свою майже тридцятилітню історію трансформувався від суто технологічного процесу до багатофункціонального явища.

Міжнародний союз електрозв'язку, який є найавторитетнішим світовим арбітром в цій галузі трактує поняття інтернет речей (IoT) як глобальну інфраструктуру для інформаційного суспільства, що дозволяє надавати розширені послуги шляхом взаємоз'єднання фізичних та віртуальних речей на основі існуючих і тих, що розвиваються сумісних інформаційних та комунікаційні технології. Завдяки використанню ідентифікації, збору даних, обробці та комунікації, інтернет речей повністю використовує дані для надання послуг для всіх видів додатків, з забезпеченням вимог до безпеки та конфіденційності статичної та динамічної інформації. З більш широкої точки зору інтернет речей сприймається як концепція з технологічними та соціальними наслідками. З технічної точки зору пристрій інтернет речей є частиною обладнання з обов'язковими можливостями зв'язку та необов'язковими можливостями зондування, активації, збору даних, зберігання даних та обробки даних. Пристрої інтернет речей збирають різні види інформації та передають її в інформаційно-комунікаційні мережі для подальшої обробки (10).

Враховуючи на підписання Україною Угоди про Асоціацію з Європейським Союзом, основні цілі розвитку інформаційного суспільства в Україні поступово узгоджуються з орієнтирами європейського розвитку. Серед них – ініціатива “Цифровий порядок денний для Європи” (“Digital agenda for Europe”), яка визначає пріоритетні позиції розбудови інформаційного суспільства в рамках європейської стратегії економічного розвитку “Європа 2020: стратегія розумного, сталого і всеосяжного зростання” (“Europe 2020: Astrategy for smart, sustainable and inclusive growth”). З метою інтеграції у світові процеси “цифровізації” у 2016 році Кабінет Міністрів України презентував проект “Цифровий порядок денний України 2020” (“Digital Agenda for Ukraine 2020”).

Саме поняття “цифрової культури” було введено до наукового обігу в 2000-х роках (2004 р., Т. О’Рейлі (T. O’Reilly) у зв’язку з виникненням технологій Web 2.0 – другого покоління мережевих сервісів Інтернету з якісно новим підходом до організації, реалізації та підтримки Web-ресурсів і є складовою широкого поняття культури (2).

Культура - сукупність матеріальних і духовних цінностей, створених людством протягом його історії; рівень розвитку суспільства у певну епоху; те, що створюється для задоволення духовних потреб людини (8).

Для дослідження деяких феноменов цифрової культури, таких як відеоігри, комп'ютерна анімація, персональні цифрові гаджети - уявлення про масову культуру є принципово необхідним. Крім того, ця типологія буде дуже

обмеженою без обліку багатоманітності субкультур і субкультурних ніш, які переживають розквіт саме в цифровій культурі. Таким чином, в поєднанні та взаємодоповненні тих методологічних принципів, які були викладені вище, складається перспективна дослідницька програма вивчення цифрової культури (3).

Цифрова культура з її культурологічними та соціокультурними аспектами є базовою основою сучасної світової культури, яка визначає нові цінності та смисли буття особистості, складовою суспільних процесів з його стрімким розвитком і видозміненням, що підтверджує еволюція дефініцій, використовуваних для аналізу й усвідомлення цифрових технологій (“цифрові” або “нові медіа”, “кіберпростір культури”, “кіберкультура”, “цифрова культура”, “пост-кіберкультура”). Іншою складовою цифрової культури є аналіз нових артефактів, нових практик, які виникли саме завдяки цифровим технологіям (комп’ютерна графіка, комп’ютерні ігри, Інтернет, системи віртуальної реальності, цифрові формати традиційних засобів комунікації, технологічне мистецтво тощо) і загальні еволюційні процеси “оцифровування” сучасної культури.

Таким чином в сучасному глобалізованому світі цифрова культура стає багатоаспектним явищем масової культури зі своєю продукцією, що знаходить відгук у мільйонів людей (6 С 135-136).

Науковець Д. Галкін вважає за доцільне розглядати цифрову культуру на декількох рівнях:

− матеріальному (технічні системи сучасних цифрових пристроїв: комп’ютери, смартфони, цифрові фотокамери з відповідним ПЗ);

− функціональному (соціальному): забезпечення діяльності інститутів, які визначають спосіб повсякденного життя, форми взаємодії, ритуали і традиції різних груп населення (від ведення електронної документації до творів технологічного мистецтва);

− символічному, оскільки символічна природа цифрової культури, яка формується в логіці цифрового кодування і розвитку мов програмування, не викликає сумнівів;

− ментальному, який стосується вкоріненості культури в психічне життя людей (цей рівень цифрової культури торкається дискусійних питань прийняття чи відкидання технологічного імперативу, нових звичок роботи з інформаційними даними тощо);

− духовно-ціннісному, що вміщує цінності цифрової культури в національному, міжнаціональному, релігійному, соціально-політичному, метафізичному контекстах (3).

Як сучасний культурологічний феномен поняття цифрової культури аналізують і зарубіжні науковці К. Бассет (C. Bassett), К. Гере (C. Gere), Г. Грибер (G. Creeber), М. Деузе (M. Deuze), Р. Мартін (R. Martin), М. Хенд (M. Hand), почасту ототожнюючи його з новими медіа. За влучним висловлюванням Ч. Гере (C. Gere), дигітальність є маркером культури останніх десятиліть, вона включає й артефакти, і комунікації, й ознаки, типові для сучасного способу життя (4).

У сучасній науці також існує тенденція тлумачити цифрову культуру як технологічний феномен, оскільки всі об’єкти цієї культури функціонують з допомогою цифрових пристроїв на основі принципу цифрового кодування інформації з допомогою бінарного коду, що стає системоутворювальним чинником цієї культури (з технологічного боку). У цьому випадку поняття “цифрової культури” збігається з дефініцією “електронної культури” (е-культури) як сукупності результатів творчості та комунікації людей в умовах впровадження ІТ-технологій, утворення єдиного інформаційного простору. Оскільки всі сучасні інформаційно-комунікаційні засоби (комп’ютер, інтернет речей, мобільний телефон, кіно- і телекамера, аналогові й цифрові відеокамери, плеєри, планшети, фотоапарати та ін.) є електронними пристроями, смислове поле електронної культури вміщує також феномени комп’ютерної, мультимедійної, кіберкультури як її різновиди (5).

Розвиток мініатюризації сенсорів датчиків інтернет речей повинно стати одним з основних стимулів до розширення сфери застосування інтернет речей в галузі масової цифрової культури.

Датчики вимірюють зовнішні фізичні дані, перетворюючи їх в сиру інформацію, яка в подальшому зберігається в цифровому вигляді, доступна для аналізу та обробки. Сьогодні датчики, які можуть визначити буквально все (від температури, діючої сили, тиску, положення та швидкості потоку до інтенсивності світла) використовуються в багатьох галузях.

Окремим перспективним напрямком, який представляє особливий інтерес, можна виділити використання датчиків в галузі масової цифрової культури, де виявлено широке застосування датчиків руху (інерції) та зображення, які використовуються в таких областях, як анімація, ігри, створення відеоизображения, стабілізація зображення, спорт та 3D-системи використання цифрових технологій для створення контенту, медіа застосувань тощо (7).

Концепція “Інтернету речей” дозволяє підвищити якість життя та діяльності людини, ефективність виробництв, державних служб, комунальних сервісів. Приблизна оцінка кількості “розумних” приладів, підключених до Інтернету до 2020 року, складе близько 30 мільярдів пристроїв, а світовий об’єм інвестицій у цю сферу – 24 трильйони доларів США. Це означає, що в даний час у світі виникає один з найбільших світових ринків абсолютно нових продуктів та послуг (9. С. 12-14).

Таким чином на основі аналізу вивчення вітчизняних і зарубіжних наукових джерел, державних нормативно-правових документів приходимо до розуміння, що поняття “цифрова культура”, “інтернет речей” та “масова культура” є багатоаспектними, й виходять за межі технологічної або цифрової галузі. Вони торкаються широкого кола соціогуманітарних, культурологічних, та інших аспектів. Основні смислові акценти цифрової культури пов’язані з виникненням нових специфічних інформаційно-віртуальних форм культури та культурної комунікації, в тому числі й інтернет-речей.

Використана література:

1. Астаф'єв А. О. "Питання розвитку цифрової культури українського соціуму". Аналітична записка / © Національний інститут стратегічних досліджень [Електронний ресурс] / А. О. Астаф'єв. – 2014. – URL: http://www.niss.gov.ua/articles/1631/.
2. Гаврілова Л. Г. Цифрова культура, цифрова грамотність, цифрова компетентність як сучасні освітні феномени [Електронний ресурс] / Л. Г. Гаврілова, Я. В. Топольник // ISSN: 2076-8184. Інформаційні технології і засоби навчання, 2017, Том 61, №5. – 2017. – URL:file:///C:/Documents%20and%20Settings/Admin/%D0%9C%D0%BE%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B/Downloads/1744-8024-1-PB%20(5).pdf.
3. Галкин Д. В. Digital Culture: методологические вопросы исследования культурной динамики от цифровых автоматов до техно-био-тварей [Електронний ресурс] / Д. В. Галкин // Международный журнал исследований культуры International Journal of Cultural Research. – 2012. – URL: https://culturalresearch.ru/files/open_issues/03_2012/IJCR_03(8)_2012_Galkin.pdf.
4. Гере Ч. Digital Culture [Електронний ресурс] / Чарлі Гере // reaktion books. – 2002. – URL: http://pl02.donau-uni.ac.at/jspui/bitstream/ 10002/597/1/digital-culture.pdf.
5. Гук А. А. Медийная культура как техногенный феномен [Електронний ресурс] / А. А. Гук. – 2016. – URL: http://mic.org.ru/new/542-medijnaya-kultura-kak-tekhnogennyj-fenomen.
6. Денисюк Ж. З. Масова культура і національна культурна ідентичність в добу глобалізації / Ж. З. Денисюк. – Київ: НАКККіМ, 2016. – 224 с.
7. Интернет вещей Безграничные возможности взаимодействия человека и машины Медиасектор и индустрия развлечений [Електронний ресурс]. – 2016. – URL: https://www.ey.com/Publication/vwLUAssets/EY-mne-internet-of-things-rus/$File/EY-mne-internet-of-things-rus.pdf.
8. Тюрменко І. І. Культурологія: теорія та історія культури: Навчальний посібник [Електронний ресурс] / І. І. Тюрменко, О. Д. Горбула // Київ: Центр навчальної літератури. – 2004. – URL: http://politics.ellib. org.ua/ pages-4215.html.
9. Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020) Концептуальні засади (версія 1.0) Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року [Електронний ресурс]. – 2016. – URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.
10. SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS Next Generation Networks – Frameworks and functional architecture models Overview of the Internet of things [Електронний ресурс]. – 2012. – URL: file:///C:/Documents%20and%20Settings/Admin/%D0%9C%D0%BE%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B/Downloads/T-REC-Y.2060-201206-I!!PDF-E.pdf.

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

Дранник В. А.,
викладач кафедри філософії ФСП КПІ ім. Ігоря Сікорського

ЩОДО ПИТАННЯ ПРО ІНТЕРНЕТ РЕЧЕЙ

Зараз, з розвитком технічних та наукових знань, все більше уваги повинно приділятися питанню правового регулювання в умовах застосування новітніх технологій Інтернету речей.

Сьогодні майже кожна людина має доступ до мережі інтернету і може користуватися або користується всіма його благами. Інтернет речей полегшує життя людини та допомагає їй у вирішенні багатьох питань, навіть без її участі. Це дуже спрощує життя людини і накопичує для неї багато вільного часу, яке людина зможе використовувати на самоосвіту, самовдосконалення, на творчі проекти. За допомогою Інтернету речей, сучасна людина буде завжди в русі подій та зможе контролювати одночасно багато речей у своєму житті та житті своїх близьких. Людина потребує допомоги з боку «розумних» систем, які зроблять її життя легшим, цікавішим, скерують ефективне використання нею навколишніх ресурсів. Інтернет речей займає важливу роль у розвитку людства та вирішує різноманітні людські завдання.

Але, з іншого боку, відбувається втручання до внутрішнього світу людини, зовнішній вплив. Людина стає заручником системи, яка може дати збій та нашкодити. Також, є ризик небезпеки розповсюдження персональної інформації, яка може потрапити до ненадійних суб'єктів. З огляду на це потрібне впровадження та використання основ правового регулювання в умовах застосування новітніх технологій Інтернету речей. Постає проблема в сфері безпеки і надійності самих пристроїв Інтернету речей та в сфері захисту персональних даних людини.

В подальшому треба удосконалювати систему Інтернету речей на всіх рівнях та розвивати правову культуру щодо цього. Мати чіткі, зрозумілі та дієві законодавчі акти щодо врегулювання цих технологій.

Також, звернути особливу увагу на підвищення серед людей рівня обізнаності у понятті Інтернету речей, його позитивних та негативних сторін, та правового врегулювання питань, що виникатимуть.

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

Гордієнко С. Г.,
д.ю.н., доцент, доцент кафедри ІППІВ
ФСП КПІ імені Ігоря Сікорського

МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ІНТЕРНЕТУ РЕЧЕЙ

Уточните значение слов, и вы избавите человечество от половины заблуждений[1].
За ослушание истине – верят лжи и заблуждениям[2].
Коли слова втрачають своє значення, народ втрачає свою свободу[3].

---

[1] Рене Декарт. http://si-sv.com/board/dekart/11-1-0-102
[2] Лесков Н.С. Собраниесочинений в 12 томах Том 12. – М.: Правда, 1989, - 448 с. – С. 94.
[3]Конфуций. Новейшийфилософскийсловарь: 2-е изд., переработ. и дополн.—Мн.: Интерпрессервис; КнижныйДом. 2001.— 1280 с.— (Мир энциклопедий).

Каждый выбирает для себя, женщину, религию, дорогу.
Дьяволу служить или пророку – каждый выбирает для себя[4].
Якщо я бачив далі інших, то тому, що стояв на плечах гігантів.
В філософії не може бути государя, тільки правда[5].

Приводом до роздумів на тематику так званого інтернету речей стали опубліковані матеріали науково-практичної конференції від 24 жовтня 2017 р. Вона відбулася в Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського»[6]. Матеріали були присвячені розкриттю сутності інтернету речей, трансформації суспільних відносин під їх впливом та проблемним питанням їх правового регулювання, а також розгляду нових викликів та загроз з точки зору технічного і правового забезпечення кібербезпеки під час впровадження та розвитку інтернету речей.

Окремі публікації викликали у автора ряд непорозумінь і стосуються в першу чергу заголовного виступу Баранова О. А.: Інтернет речей (IoT): огляд правових проблем.

Спробуємо це продемонструвати на цитатах, які можливо трактувати досить різнобоко і неоднозначно, але наука такого не терпить. Автор, як науковець свою точку зору мав би обґрунтовувати науковими аргументами, а не лише своїми власних відчуттями і думками. Хоча це є позиція автора.

Так автор пише: «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 призначені для надання послуг і проведення робіт в інтересах суб'єктів (юридичних або фізичних осіб)».

Очевидним є те, що ним не враховані правила визначення понять, які описані провідним фахівцем в галузі логіки Кондаковим М. І.[7] та нами у своїх роботах:визначення повинно бути ясним; поняття, як система знання – це сукупність відомих нам як основних, так і похідних ознак, що мисляться у понятті предметів, а також знання про те, у яких конкретних формах існують у дійсності ці предмети, що узагальнюються в понятті; одним з найважливіших правил утворення понять також є «закон тотожності» – не називай ту саму річ двома різними іменами і не називай дві різні речі тим самим ім'ям; у визначенні не

[4] Ю. Левитанский. Каждый выбирает для себя...
[5] Цитати Ісаака Ньютона про науку, релігію і людяність. https://www.depo.ua/ukr/svit/isaak-nyuton-o-04012015000500
[6] 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. – 238 с.
[7] Кондаков Н.И. Логика. М., 1954. - С. 300; Кондаков Н. И. Введение в логику. — М.: Наука, 1967.— 467 с.; Кондаков Н. И. Логический словарь-справочник. — М.: Наука, 1975.— 721 с.

повинно бути кола – термін, що зустрічається у визначальній частині, не повинен визначатися через обумовлений термін; зрозуміти явище – це значить з'ясувати його значення у конкретній системі явищ, що взаємодіють, у якій воно з необхідністю здійснюється, і з'ясувати саме ті особливості, завдяки яким це явище тільки може грати визначену роль у складі цілого; зрозуміти явище – значить з'ясувати спосіб його виникнення, «правило», за яким це виникнення відбувається з необхідністю, закладеною в конкретній сукупності умов, проаналізувати самі умови виникнення явища; визначення повинно бути співрозмірним – визначальна частина повинна виділяти саме той клас предметів, що представляє те, що визначається[8].

Зазначені закономірності двох авторів не відрізняються між собою за суттю, хоча і відпрацьовані незалежно, і в різні часові проміжки. Надалі, вважаємо за доцільне навести загально-філософські трактування стосовно понять.

Реальною підставою для ототожнення наукових характеристик «поняття» як «клітинки» мислення з характеристиками слова, терміна є те, що мислення завжди протікає у формі мови, а поняття виражається через слово, термін, найменування.

Кожне поняття реалізується через термін, кожне теоретичне судження – через вислів.

Існують пусті поняття, одиничні, загальні поняття, універсальні тазбірні поняття, емпіричні і теоретичні поняття, порівнянні і непорівнянні, сумісні і несумісні поняття, рівнозначні поняття; поняття, що знаходяться у відносинах логічного підпорядкування; перехресні поняття, явні і неявні, номінальні і реальні визначення.

До основних операцій з поняттями належать: узагальнення й обмеження понять і розподіл понять. Приватним видом розподілу є класифікація[9].

Тобто, під «Інтернетом речей» варто розуміти технологію, яксистему, що сприяє наданню послуг і проведенню робіт в інтересах суб'єктів (юридичних або фізичних осіб) через інформаційно-комунікаційні технології в реальному вимірі часу.

Адже інформаційно-комунікаційні технології (ІКТ) —уніфіковані технології та інтегровані телекомунікації (телефонні лінії та бездротові з'єднання), комп'ютерів, підпрограмного забезпечення, програмного забезпечення, накопичувальних та аудіовізуальних систем, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію. Іншими словами, ІКТ складається з інформаційних технологій (ІТ), а також телекомунікацій, медіа-трансляцій, усіх видів аудіо і відеообробки, передачі, мережевих функцій управління та моніторингу.

---

[8] Гордієнко С.Г.Молодому науковцю СБ України коротко про необхідне: Наук.-практ. посібник. – К.: Наук.-вид. відділ НА СБ України, 2008. – 89 с.

[9] Войшвилло Е.К. Понятиекак форма мышления: логико-гносеологическийанализ. — М.: Изд-воМГУ, 1989. —239 с.

Наразі ІКТ включають апаратні засоби (комп'ютери, сервери тощо) та програмне забезпечення (операційні системи, мережеві протоколи, пошукові системи тощо). У сучасному світі інформаційно-комунікаційні технології є важливою і невід'ємною частиною держави, бізнесу та приватного життя.

Термін ІКТ в наш час використовується для позначення об'єднання (конвергенції) аудіовізуальних та телефонних мереж з комп'ютерними мережами через один кабель або з'єднувальну систему. Є великі економічні стимули (величезна економія коштів за рахунок вилучення телефонної мережі) при об'єднанні аудіовізуальних, телефонних та електромереж з системою комп'ютерної мережі використовуючи одну єдину систему кабелів, сигнал розподілу та управління.

У подальшому за текстом є також недоречним використання автором різних скорочень«технології інтернету речей», тим більше посилаючись на багатьох вчених, які одночасно такої помилки допустити не можуть: …технологій Інтернету речей (IP),…технологій IoT, … регулювання в умовах застосування технологій ІВ, … вирішення проблем правового регулювання в умовах використання ІЗ. Очевидно, що неприпустимоназивати одну і ту ж річ різними іменами (див. правила), а за текстом мова йде саме про технології інтернету речей.

Також недоречним є використання у визначенні термінів «комплекси і системи», адже це також абсолютно дві різні речі.

Невиправданим і вкрай спірним є застосування автором тез словосполучень:

- «до системних бар’єрів можна віднести наступні…». Очевидно, що такі бар’єри можуть створювати систему, але вони не можуть бути системними, як і загрози – це тавтологія.
- «потребує відповідного правового супроводження». Супроводжувати можна даму до театру, а явище «інтернету речей» потребує правового регулювання і його забезпечення.

Також невиваженою, хоча і знову з посиланням на «багато вчених припускають» наявність трьох основних гіпотез, які власне і визначають основний зміст наукових підходів (також армійські статутні словосполучення: підхід, відхід і фіксація, а науковим був би метод, позиція та ін.) до реформування правових систем, обумовленого використанням роботів:

- роботи є об'єктом суспільних відносин, а значить і об'єктом правовідносин;
- роботи є суб'єктом суспільних відносин, а значить можуть бути суб'єктами правовідносин;
- роботи можуть бути як об'єктом, так і суб'єктом суспільних відносин, а значить і можуть бути як об'єктом, так і суб'єктом правовідносин.

Це дещо схоже на те, щоб визнати суб’єктами права друкарські машинки, а об’єктами - надруковані їх літерами тексти.І роботи, і комп’ютери, і друкарські машинки є лише засобами, які допомагають людині в її діяльності, адже саме для цього вона їх створює і програмує!!!

Очевидним також є те, що багато таких «вчених» малознайомі з теорією держави та права, яка це трактує дещо інакше.

Об'єкт права (правовідносин) — це те, із приводу чого виникає, існує саме правове відношення.

У юридичній літературі існують різні трактування об'єкта правовідносин. Проте у ході тривалої дискусії склалися в основному дві концепції — моністична і плюралістична. Об'єктом правовідносин можуть виступати тільки дії суб'єктів, оскільки саме дії, вчинки людей підлягають регулюванню юридичними нормами, і лише людська поведінка здатна реагувати на правовий вплив.

Об'єкти правовідносин настільки різноманітні, наскільки різноманітні правовідносини, що регулюються правом.

Залежно від характеру і видів правовідносин їх об'єктами виступають:

- Матеріальні блага, характерні головним чином для цивільних, майнових правовідносин.
- Нематеріальні особисті блага, більшість з яких типові для кримінальних і процесуальних правовідносин.
- Поведінка, дії суб'єктів, різного роду послуги і їх результати.
- Продукти духовної творчості.

Цінні папери, офіційні документи. Вони можуть стати об'єктом правовідносин, що виникають при їх втраті, поновленні, оформленні дублікатів. У наш час в країні склався ринок цінних паперів, акції купуються і продаються, тобто вони є об'єктами угод.

Суб’єкт права – це особа, організація чи специфічні соціальні утворення (наприклад держава) за якими право визнає здатність бути носіями суб'єктивних праві юридичних обов'язків.

Для суб'єкта права характерні наступні дві основні ознаки. По-перше, це особа, учасник суспільних відносин (індивіди, організації), яка за своїми особливостями фактично може бути носієм суб'єктивних прав та юридичних обов'язків. Для цього вона повинна володіти зовнішнєю відокремленістю, персоніфікацією та здатністю виробляти, виражати і здійснювати персоніфіковану волю.

По-друге, це особа, яка реально здатна брати участь у правовідносинах, набула властивості суб'єкта права в силу юридичних норм. Іншими словами, юридичні норми утворюють обов'язкову основу виступу індивідів, організацій, громадських утворень як суб'єктів права.

У сучасній юридичній літературі поняття «суб'єкт права» частіше за все використовується як синонім термінів «суб'єкт» чи «учасник правовідносин».

Усі суб'єкти права поділяються на три основні групи: індивідуальні суб'єкти(фізичні особи);колективні суб'єкти;громадські утворення.

Особливими суб'єктами права виступають такі специфічні соціальні утворення, як держава, територіальна група тощо.

Тепер дещо про «системну» тематику, яку досліджувало дійсно багато видатних вчених[10], однак проблеми «системології» як науки і досі повністю не вирішені.

На наше переконання, змістовне пізнання явищ можливе лише в разі розуміння і застосування системного методу дослідження понять, тому що термін «система» передбачає не «сукупність», а чітко визначений комплекс взаємопов'язаних та взаємозалежних елементів.

У нашому розумінні система – це комплекс взаємопов'язаних та взаємодіючих тим чи іншим чином обмеженого числа компонентів із спільною метою для досягнення визначеного результату.

Адже головним системоутворюючим чинником будь-якої системи є результат її функціонування, а просто головним - мета.

В. М. Садовський приводить, наприклад, близько 40 визначень поняття «система»[11].

Генезис категорії «система» досить повно дається у роботах Аверьянова О.М., який як найбільш загальне визначення системи пропонує розглядати «відмежовану безліч взаємодіючих елементів»[12]. Однак при застосуванні до суспільства це визначення недостатнє, оскільки соціальні системи суть системи цілісні, системи, зв'язок компонентів яких носить надто органічний характер.

Різними авторами поняття системи визначається по-різному, а тим більше і класифікується по-різному[13].

---

[10] Аббасова О.С., Абрамова Н.Т., Аверьянов А.Н., Автономов А., Акофф Р., Амосов Н.М., Аніщенко А.І., Анохін П.К., Аткінсон Р., Афанасьєв В.Г., Берталанфі Л., Біблєр В.С., Бір Ст., Блауберг П.В., Брунер Дж., Буєва Л.П., Вінер Н., Войшвилло Е., Воронцов Б.Н., Галантер Є., Гальперін П.Я., Ганзен В.А, Гіг Дж., Голованов Л.В., Головей Л.А., Глушков В.М., Добров Г.М., Дружинін В.В., Ємельянов С.В., Емері Ф., Енгельс Ф., Ешбі У., Іріков В.А., Каган М.С., Калошин П.Н., Карабанов Н.В., Карташев В.А., Кінг В., Кондаков Н.І., Конторов Д.С., Кліланд Д., Крейсберг М.М., Кремянський В.І., Кругліков Р.І., Кузьмін В.П., Кукушкіна Є.І., Лєкант П.А., Лекторський В.А., Ленін В.І., Лурія А.Р., Маліновська О.В., Маліновський А.А., Маркс К., Міллер Дж., Мирський Е.М., Момджян К.Х., Наппельбаум Е.Л., Нарський І.С., Ойзерман Т.І., Оруджев З.М., Оуене А., Паск Г., Петрушенко Л.А., Поздняков А., Пономарьов В.В., Поспєлов Г.С., Прибрам К., Рабіна М., Райбекас А.Я., Росс, Садовський В.Н., Саратовський В.Н., Саркісян С.А., Сасієні М., Свідерський В.І., Смірнов І.Н., Судаков К.В., Терещенко В.І., Тітаренко А.І., Тода М., Тюхтін В.С., Уйомов А.І., Уолш М., Урсул А.Д., Файзієв А.А., Федосєєв П.Н., Фогель Л., Фофанов В.П., Фролов І.Т., Фурман А., Ханіка Ф., Холл А.Д., Хорват І., Черняк Ю.Л., Черчмен Ч., Швирков В.Б., Шуміліна А.І., Шуффорд Е.Х., Юдін Е.Г., Ярошевський Т.М. та ін.

[11] Садовский В.Н. Основанияобщейтеории систем.М., "Наука",1974, 280 стр.

[12] Аверьянов А.Н. Система: философскаякатегория и реальность.Монография. - М., «Мысль», 1976. - 188 с.

[13] Афанасьев В.Г. Системность и общество.— М.: Политиздат, 1980. - 368 с.; Акофф Р., Эмери Ф.О целеустремленных системах: Пер. с англ. М.: Сов. радио, 1974; Дмитриев П.С., Удилов В.Н., Фролов А.П. Системный подход и егоприменение в выявлениивражескихагентов. - М.: ВКШКГБСССР, 1982; Свидерский А.И. О диалектикеэлементов и структуре в обьективномире и в познании. - М.: Соцэкгиз, 1962; Кремянский В.И. Методологическиепроблемы системного подхода к информации. - М.: Наука, 1977; Тода М., Шуффорд Э.Х. Логика систем: введение в формальнуюлогикуструктуры. Исследования по общейтеории систем. - М.: Прогресс, 1969 и др.

Надалі ми приведемо визначення академіка П. К. Анохіна, яке явно відрізняється від інших, що існують у відомій нам літературі: «системою можна назвати тільки такий комплекс вибірково залучених компонентів, у яких взаємодія і взаємовідношення здобувають характер взаємного сприяння компонентів на отримання сфокусованого корисного результату».

Це визначення на даний час, ми вважаємо базовим, але виразимо деякий жаль, так як це зробив Карташев В. А. з приводу того, що робота П. К. Анохіна, будучи, однією з видатних робіт стосовно систем, залишилася осторонь від уваги основної маси вчених, зайнятих системною проблематикою. Тому, що надрукована у вузькоспеціалізованому журналі[14], вона так і залишилася б на довгий час надбанням вузького кола фахівців, далеких від спеціальних питань «системного руху», як, утім, і більшість інших його робіт.

Досить цікаве і різностороннє бачення системності пропонує у одній із своїх фундаментальних праць Карташев В. А., який розглядає та аналізує кілька характерних «новинок» визначення П. К. Анохіна і зауважує, що досить цікавою характеристикою системи є її структура[15.]

Таким чином, основними ознаками систем є:наявність системної, інтегративної, колективної якості, відмінної від властивостей і якостей утворюючих їх компонентів; компоненти, частини, саме те, із чого утворюється ціле і без чого воно неможливе; наявність структури, внутрішньої організації системи (маємо справу із системно-структурною ознакою системності, цілісності); доцільність - прагнення до досягнення визначеної мети; наявність системно-функціональних ознак (існування в суспільній системі мети, позиції; набір засобів для досягнення цієї цілі, засобів або компонентів, що за своєю суттю є модулями; досягнення під цілей, як результат функціонування компонентів); системно-комунікативні ознаки (система - компонент іншої системи, взаємозалежна з іншими системами більш високого або низького рівня); історичні ознаки (час є неодмінною характеристикою системи); інтегративні ознаки, точніше управлінські; інформаційні ознаки.

Для більш повного розуміння систем варто додати, що всім соціальним системам властиві - цілеспрямованість, адаптивність, відкритість, можливість самовідтворення і розвитку, нелінійна причинність і залежність через їх досить високу складність.

Виходячи з викладеного ми маємо можливість визначити шляхи використання системного методу у пізнанні соціальних цілісностей через систему

---

[14] Анохин П.К. Теорияфункциональнойсистемы. — Успехифизиологических наук. 1970, т.1, № 1.
[15] Карташев В.А. Система систем. Очеркиобщейтеории и методологии. — М.: «Прогресс - Академия», 1995. — 325 с.

їх «діяльностей», який досить детально викладений у ряді видатних для сучасності робіт[16].

Однак, ми вважаємо, що найбільш раціональною системою, що відображає сутність і зміст соціальної діяльності, є система з наступних елементів: мета, завдання, об'єкт, предмет, суб'єкт, види, форми, методи, сили, засоби, процес фізичної діяльності та результат[17] (Д = М => З =>О-бт =>Суб-т => З => Ф => М => Фіз. Д = Результат).

Таким чином, ми можемо стверджувати, що системний метод у філософських методологіях пізнання соціально-політичних явищ займає провідне місце, тим паче, що всі вони, а їх відомо нам 72 побудовані на його принципах та закономірностях[18].

У своїх дослідженнях, як правило, нами використовується 7 найбільш пристосованих до умов сучасності методологічних платформи: діалектика; науковий реалізм; науковий матеріалізм; структурно-функціональний аналіз; системо-миследіяльнісна методологія (СМД-методологія); синергетика татеорія конвергенції.

А Барановим О. А., як видно з тез,використовується лише окремий елемент синергетики – біфуркаційність розвитку, одним з основоположників якої є І. Р. Пригожин - фізикохімік за родом занять, мислитель по суті, по культурній приналежності - людина з надзвичайно своєрідною інтелектуальною долею. Його називають«сучасним Ньютоном», а зроблене ним в науці визнають основою можливої в майбутньому нової моделі світобудови після моделей Ньютона і Ейнштейна.

Він ввів поняття «дисипативні структури»- стійкий, впорядкований неврівноважений стан системи, через яку проходять потоки енергії, маси і ентропії. Або популярне в останні десятиліття поняття -«самоорганізація».

---

[16] Фофанов В.П. Социальнаядеятельностькак система. Новосибирск, 1981; Юдин Э.Г. Системныйподход и принцип деятельности. Методологическиепроблемысовременной науки. - М.: Наука, 1978. - 212 с.; Карташев В.А. Система систем. Очеркиобщейтеории и методологии. — М.: «Прогресс - Академия», 1995. — 325 с. тощо.

[17] Картавцев В.С., Гордієнко С.Г. До питання про концептуальні засади діяльності Служби безпеки України // Науковий вісник Академії СБУ. - К., 1997. - № 5.

[18] Абсолютний ідеалізм; метафізика; гілеморфізм; онтологія; схоластика; емпіризм; критицизм; раціоналізм; ірраціоналізм; критичний раціоналізм; критичний реалізм; модернізм; постмодернізм; позитивізм; постпозитивізм; неопозитивізм; екзистенціалізм; психоаналіз; шизоаналіз; герменевтика; феноменологія; махізм; постметафізичне мислення; номадологія; діалектика; негативна діалектика; гілозоїзм; інструменталізм; структуралізм; постструктуралізм; ідіографізм; різома; конвенціоналізм; аксіологія; інтернаїзм; інтуїтивізм; історицизм; конституювання; кумулятивізм; філософська антропологія; науковий реалізм; марксизм; неомарксизм; неораціоналізм; надраціоналізм; неореалізм; неотомізм; персоналізм; монізм; дуалізм; плюралізм; прагматизм; редукціонізм; релятивізм; холізм; еволюційна епістемологія; евристика; екологічна етика; екстерналізм; емерджентний еволюціонізм; неогегельянство; неокантіанство; вульгарний матеріалізм; науковий матеріалізм; діалектичний матеріалізм; структурно-функціональний аналіз; нелінійних динамік теорія; СМД-методологія; синергетика; конвергенції теорія.

Синергетика – один із провідних напрямків сучасної науки, який репрезентує природничо-науковий вектор розвитку теорії нелінійних динамік у сучасній культурі.

На рівні самовизначення синергетика конституює себе як концепція неврівноваженої динаміки, або теорія самоорганізації нелінійних динамічних середовищ, яка утворює нову матрицю бачення об'єкта в якості складного. Фундаментальним критерієм «складності» у синергетиці виступає показник не статичного характеру (багаторівневість структурної ієрархії об'єкта й т.п.), а показник суто динамічний - наявність іманентного потенціалу самоорганізації. Синергетика досліджує клас систем, що перебувають за межами стану термодинамічної рівноваги (тобто досить неврівноважених), предметний ареал синергетичної парадигми конституюється і локалізується «удалині від рівноваги».

Таким чином, синергетикою «досліджуються явища, в умовах нестійкості, і визначається та нова структура, що виникає за межею нестійкості», на основі чого синергетиці вдається встановити універсальні й «глибокі аналогії», які «проявляються між зовсім різними системами при проходженні ними точок виникнення нестійкості». Іншими словами, складність, відтепер розглядається не як виключення, а як загальне правило. На цій основі синергетика формулює свою основну тезу: на всіх рівнях структурної організації буття саме неврівноваженість виступає умовою й джерелом виникнення «порядку», саме «неврівноваженість є те, що породжує «порядок з хаосу». Фундаментальною властивістю досліджуваних синергетикою об'єктів виступає їх складність і«нелінійність», яка досліджується в синергетиці за допомогою біфуркаційного механізму.

Додамо також, що, поділяючи точку зору В. В. Копєйчикова на визначення«права» як найбільш адаптованого до вимог, що пред’являються до визначень, пропонуємо свою трактову права як системи норм, які встановлені державою, мають офіційний формально-визначений характер, виражають права й обов’язки учасників правовідносин, направлені на регулювання найбільш важливих суспільних відносин, є загальнообов’язковими для всього населення та охороняються державою. Таким чином, під «Інтернетом речей» варто розуміти технологію, як систему, що сприяє наданню послуг і проведенню робіт в інтересах суб'єктів через інформаційно-комунікаційні технології в реальному вимірі часу.

А під правом інтернету речей слід розуміти систему норм, які встановлені державою, мають офіційний формально-визначений характер, виражають права й обов’язки учасників правовідносин у галузі інформаційно-комунікаційних технологій зі сприяння проведення робіт в реальному вимірі часу і є загальнообов’язковими для всього населення та охороняються державою.

Як нами вбачається, за певних, сприятливих дослідженням умов (необхідність дослідження, наявність замовника, чітка мета та завдання дослідження, кваліфікований авторський колектив, наявність часу та необхідних матеріальних засобів), зазначене вище, може слугувати плідним підґрунтям для

розгляду такого неоднозначного і складного явища, як так званий «інтернет речей».

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

Фурашев В. М.,
к.т.н., доцент, с.н.с.

ПРАВО У СВІТЛІ ТЕХНОЛОГІЙ ІНТЕРНЕТ-РЕЧЕЙ

Інтернет речей як сукупність взаємопов`язаних, через дротові або бездротові мережі на основі використання стандартних протоколів зв`язку, фізичних пристроїв та маючи визначені засоби здійснення передачі і обміну даними між фізичним світом і комп'ютерними системами, спроможністю зчитування та приведення в дію, функцію програмування та ідентифікації, що, у підсумку, дозволяє виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів, є сукупним результатом досягнень у сферах інформатизації, механізації, роботизації та розробки та поетапного впровадження штучного інтелекту.

Цілком природно, що «феномен» Інтернет речей не може не відобразитися на інших процесам, які відбуваються у суспільстві, зокрема на суспільних відносинах.

Тому виникає питання відповідності темпів отримання результатів науково-технічного прогресу та етапностей їх впровадження у реальне життя з готовністю суспільства цих змін у своєму, в першу чергу, особистому житті.

Чисельні наукові та публіцистичні публікації свідчать далеку від усвідомлення пересічними громадянами результатів сучасного науково-технічного прогресу та їх впливу та спрямованість трансформаційних процесів суспільних відносин. Для прикладу, можна навести висновки дослідження експертів ф. “Pod Group” [19]: “... експерти вказують на катастрофічну неготовність суспільства прийняти прийдешні зміни.

Pod Group опитувала 2000 службовців про умови їх праці протягом останніх 12 місяців, а потім дізнавалася думку про небезпеку автоматизації протягом наступних 15 років. 12% заявили, що за останній рік їх роботодавець відмовився від послуг якихось працівників, замінивши їх механізмом або програмним рішенням.

Найактивніше автоматизують робочі процеси в Уельсі - там наслідки автоматизації спостерігали 14% опитаних. Найбезпечніше для робочих людей місце в Сполученому Королівстві - Північна Ірландія, там на витіснення роботами поскаржилися лише 7% службовців. При цьому лише 20% побоюються втратити

[19] Джерело інформації: http://internetua.com/za-god-mashiny-zamenili-csast-rabotnikov-v-12-britanskih-kompanii

роботу через автоматизацію в доступному для огляду майбутньому - в наступні 15 років. Саме в Уельсі стурбованих найменше - лише 16%. Голова Pod Group і організатор дослідження Чарльз Тауерс-Кларк вказує, що до наслідків Четвертої промислової революції не готові ні працівники, ні роботодавці. «Звичайно, «штучного інтелекту (ШІ)» не варто побоюватися до такої міри, щоб припинити розвиток технології зовсім. Але трохи страху [за своє робоче місце] не завадить, адже це спонукало б нас розвивати якості, недоступні ШІ, створюючи тим самим можливості для гармонійної співпраці людей і машин. Зараз же люди своїми очима бачать, як їх замінюють програми, і ховають голови в пісок. ШІ тим часом росте як на дріжджах».

Подібних прикладів можна навести дуже багато. Але як бути? Науково-технічний прогрес, його результати – процес об’єктивний, процес якій можна загальмувати у часі, але не можливо відмінити взагалі.

Відповідь на це, зовнішньо складне, питання, у сучасних умовах, слід шукати у найбільше впливових, з точки зору формування суспільних відносин, чинниках та факторах.

Під час визначення зазначених чинників та факторі слід звернути увагу на функції права, які полягають у здійсненні впливу права на свідомість і поведінку суб'єктів суспільних відносин з метою розв'язання конкретних завдань. На сьогодні, основна функція права полягає в тому, що воно є нормативним і загальнообов'язковим засобом врегулювання суспільних відносин. Але ця функція може та, з часом, обов`язково, під впливом зовнішніх об’єктивних обставин, зміниться та буде наступною - основна функція права полягає в тому, що воно є нормативним і загальнообов'язковим засобом формування та врегулювання суспільних відносин.

Виходячи з цього, одним з таких факторів є процес встановлення правовідносин, тобто суспільних відносин, які регульовані нормами права. Саме таки суспільні відносини мають загальнообов`язковий характер та охороняються державною владою від порушень через систему правозастосування. Саме таки суспільні відносини мають найбільший шанс на скоріше усвідомлення кожним пересічним громадянином сутності джерела їх виникнення.

Таким чином, науково-технічний прогрес та його наслідки, зокрема, Інтернет речей, вимагають нагальних змін ролі та місця права та його функцій подальшому розвитку як національного суспільства, так і загальносвітового.

Враховуючи реалії сучасності (глобалізаційні процеси у різних сферах, залежність країн один від одного та ін.), сутність цих змін полягає, на думку автора, у тому що:

а) на національному рівні:

- право повинно бути виключним механізмом «примусовості» в системі забезпечення існування визначеної системи державного управління, її «обслуговуючої» компонентою;
- право повинно стати реальної складової економіки;

- право повинно стати одним з основних «стимуляторів та двигунів» подальшого розвитку, за всіма напрямами, національного суспільства, в першу чергу, у економічної, соціальної та науково-технічної сферах;

- необхідне переглянути підходи та пріоритети у визначенні та встановленні правовідносин з точки зору суб`єктності суспільних відносин.

Це можливо здійснити за умов докорінного перегляду ролі та місця права, в цілому та кожної її складової, в системі державного управління, забезпечення життєдіяльності держави і суспільства.

б) на загальносвітовому рівні:

- встановити правові механізми одними з головних показників визначення ступеня та інтенсивності розвитку світового суспільства, спрямованості, ступеня та розвитку науково-технічного прогресу;

- забезпечити координованість та спрямованість національних правових механізмів та механізмів міжнародного права з метою впровадження/блокування випереджаючого формування суспільних відносин внаслідок результатів науково-технічного прогресу;

- вкрай необхідно вже наразі замислитися над питаннями суб'єктності суспільних відносин.

Головним принципом права повинно бути «формуючий» принцип – принцип формування суспільних відносин через механізм випереджаючого, моделюючого, прогнозного визначення суб'єктів суспільних відносин та встановлення відповідних правовідносин.

У цьому контексті, про ситуацію в Україні, то, на погляд автора, українська правова наука, українські вчені у всіх сферах правової науки, готові втілення у життя «формуючого» принципу права. Впевненість у такому висновку знаходиться у численних наукових розробках у всіх сферах правової науки.

Але, на жаль, навіть приблизного висновку, неможливо зробити у сферах законотворчої та законодавчої діяльності, а також сфері правозастосування та правоохоронної сфері.

Отже, що стосується Інтернет речей у сукупності з спрямованістю та темпами створення штучного інтелекту є дуже потужним сигналом по розгляду, прийнятті відповідних рішень та швидше втілення в їх в життя.

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

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

СУЧАСНІ ВИКЛИКИ ПРАВУ І ЮРИДИЧНІЙ НАУЦІ (НА ПРИКЛАДІ DLT І КРИПТОПРАВА)

Сучасний світ, що тісно пов'язаний з технологіями, зумовлює постійний пошук нових ідей, підходів, поглядів на різні соціальні інститути. Щодо деяких з них такий вплив є очевидним. Зазначена проблематика перебуває в поле зору дослідників гуманітарних наук, в першу чергу соціології та соціальної філософії. Метою даного виступу є виокремлення та визначення низки пов’язаних проблем у сфері права, правового регулювання, які викликані виникненням та розповсюдженням деяких видів інформаційних технологій.

У даному виступі будуть розглядатись окремі аспекти феномену технологій розподілених реєстрів (що відомі під англомовною абревіатурою DLT) і технологій шифрування інформації (узагальнено пропонується розуміти як різноманітні терміни з приставкою крипто-), також буде побіжно розглянуто висловлені точки зору щодо концептуалізації криптоправа, при цьому мова буде іти лише про процес концептуалізації, оскільки вести мову про концепт, доктрину або предмет ще зарано, до того ж ідеологія формування криптоправа можливо означатиме і зміни усієї парадигми сучасного права.

По-перше необхідно визначитись щодо термінів, понять та їх розуміння з погляду виокремлення соціальних відносин, які потребують або не потребують правового регулювання.

DLT є видом технології розподіленої обробки і зберігання інформації (тобто її обробки декількома пристроями). Особливостями DLT є відсутність центрального адміністрування, одночасний розподіл копій інформації між пристроями, використання і синхронізація даних згідно з алгоритмом консенсусу, застосування шифрування на всіх етапах. Проводити технічний та історичний екскурси в особливості такої технології потреби немає, оскільки для розуміння як саме вона впливатиме на соціальні відносини та право, доцільно виділити лише її особливості (так звані особливості «для цілей правового регулювання»). Першою особливістю є відсутність якогось одного фізичного носія інформації, що зберігає усю інформацію, або її частину. Інформація, яка зберігається, перебуває одночасно у всіх учасників системи, при цьому жоден з них не контролює ані усю інформацію, ані якусь критично важливу частину. Другою особливістю є захист інформації засобами шифрування від перехоплення та модифікації на всіх етапах обробки та зберігання. Зазначені властивості пов’язані між собою.

На сьогодні найбільш відомими серед фахівців є різні види DLT, хоча в масовій свідомості мова йде практично лише про блокчейн (та, звісно, про криптовалюти). Слід зазначити, що інші види DLT (наприклад побудова

розподіленого реєстру в існуючій комп'ютерній мережі - «приватний блокчейн») перебувають у полі зору технічних спеціалістів і ніяк не межують з проблематикою правового регулювання, більш того повною мірою вписуються в існуючу нормативно-правову базу технічного захисту інформації. Водночас, здатність такої технології значно впливати на суспільство є очевидним (про що свідчить випадок блокчейну і криптовалют), а перспективи наприклад DAG (система «направленного ациклічного графу») та її окремих застосувань фахівцями розцінюються як значні. Таким чином, можливо виникнення якихось видів «пост-блокчейну», тому для цілей правового регулювання більш правильним все ж розглядати DLT.

Отже, поле для регулювання визначено. Що ж саме відбуваються у правових аспектах використання технологій. Насамперед, лавиноподібне зростання кількості публікацій. Так, на початку 2018 року О.А.Баранов, аналізуючи кількість робіт щодо «блокчейну» та аспектів його правового регулювання за допомогою бази «Google Scholar" визначив факт стрімкого збільшення числа публікацій (третина з усіх – за останній, 2017 рік) [1, с. 69]. Слід зазначити, переважна більшість робіт є англомовними, а праці юристів стосуються правових аспектів, ґрунтуючись на законодавстві різних країн. Зазначене підкреслює глобалізацію інформаційних технологій у сучасному суспільстві. Водночас характерною рисою є і спільність підходів до правового розуміння використання технологій різними дослідниками.

Що ж саме є викликом праву взагалі у зазначених технологіях, якщо вони є лише технологіями і принципово не повинні вирізнятись для цілей правового регулювання?

Для відповіді на це питання наведемо різні кути зору юристів, що можливі у даному випадку.

По-перше, це погляд практика. Якщо звернутись до соціальної мережі "Facebook" або до спеціалізованих ресурсів, то можливо спостерігати, що в Києві щотижня проводиться мінімум по одній події присвяченій блокчейну або криптовалютам і кожна друга передбачає правові аспекти. Кількість мастер-класів, лекцій і т.п. на цю тему сягнула десятків. Юридичні компанії і практикуючі юристи намагаються бути в тренді і пропонують різні послуги, адаптовані під використання крипто-технологій. Деякі моменти (на кшталт продажу київської квартири за криптовалюту) стають новиною для загальнонаціональних ЗМІ та телебачення. Але як правило мова йде про пошук відповідних алгоритмів дій по досягненню цілей клієнта в умовах існуючого чинного законодавства, його переваг, вад та пробілів (що іноді відомо під скомпрометованим терміном «схеми»). Тобто юристи-практики застосовують норми існуючого законодавства під конкретний випадок, що дозволяє вирішити проблему конкретної особи. Розберемо, приклад продажу пиріжків за криптовалюту. Улітку 2017 року і ЗМІ з'явилась новина, що одне київське кафе стало приймати криптовалюту як засіб платежу. Нібито клієнт кафе запропонував

офіціанту розплатитись криптовалютою і вони зробили це відразу (відкривши новий крипто-гаманець і закривши угоду), що мав підтвердити чек закладу, хоча на світлині було поміщено не фіскальний чек, а лише рахунок. Через деякий час з'явились коментарі юристів, що супроводжують подібні практики. У даному разі кафе (з метою PR) провело оплату як акцію (знижка і операція як продаж за 1 копійку), а клієнт сплатив суму фактично не на рахунок кафе, а іншій особі. Питання сплати НДС у такому разі не підіймалося. Зрозуміло, що через незначний обсяг операції вона не привернула увагу фіскальних органів, але у значних масштабах така «схема» буде витлумачена як ухилення від сплати податків. У подальшому з'явились інші алгоритми дій, які зумовлюють відсутність ризиків для клієнтів, що активно використовуються і обговорюються практиками та розповсюджуються на мастер-класах [2-4].

По-друге, погляд політика. Як правило, народні депутати України, політики та політичні партій намагаються реагувати на нагальні проблеми суспільства. Перші з них роблять це через законодавчу творчість, що проявляється у відповідних законопроектах. З огляду на формат заходу можливо лише проілюструвати, що в одному з законопроектів стосовно регулювання використання криптовалют, його ідеологія полягає у встановленні певних державних преференцій для бізнесу в сфері криптовалют. Таким чином, позицією політиків стосовно регулювання є встановлення якихось преференцій для певних соціальних (економічних) груп, що є стейкхолдерами у цьому питанні, а у деяких випадках – узагалі вирішення особистих проблем. Так, наприклад, активність законотворців різко зросла після виявлення факту наявності в них криптовалюти, а отже їх особистої зацікавленості у визначенні її правового статусу. На нашу думку, більшість з законопроектів з питань регулювання криптовалют, які подано до Верховної Ради, є суто політичними проектами.

По-третє, погляд державних органів (або регуляторів). У даному випадку з проблемного поля технологій доцільно виокремити позицію державних органів відповідальних за формування і реалізацію державної політики, оскільки правові проблеми DLT визначаються у розрізі правового забезпечення державних програм розвитку. Але зазначений шлях вимагає директивного підходу і у праві, що не повною мірою враховує існуючу ситуацію – популярні застосування DLT виникли поза правом і поза державами, тому не потребують традиційного «правового забезпечення» розвитку з боку держави. Інші державні органи зосереджені на проблематиці «регулювання–нерегулювання» цієї сфери. Переважна більшість публікацій присвячена як раз регуляторним аспектам сфери DLT. В Україні на сьогодні в основному існує зосередженість регуляторів передусім на криптовалютах, тому різні підходи зосереджуються лише у питанні пошуку конкретного регулятора і форм такого регулювання [5, 6].

Погляд вітчизняної правової науки у цьому питанні на жаль найбільш апатичний. У першу чергу це зумовлено вкрай вузьким підходом до питань застосування технологій в рамках відповідних галузей правової науки як до

чогось суть прикладного і нецікавого для теоретиків. Диференціація на окремі галузі і встановлення між ними бар'єрів (наприклад, у вигляді чіткої відповідності дисертаційних досліджень визначеним паспортам спеціальностей) не сприяє належному розгляду питань. Якщо проаналізувати існуючий масив публікацій з цього приводу, то мова йде насамперед про ще одне адміністрування (адміністративно-правові аспекти регулювання певної сфери - у даному випадку застосування технологій). У такому разі увага дослідника буде зосереджена лише на правовому втіленні ще одного об'єкта для державного регулювання. В іншому випадку є намагання вирішити окремий казус - чи є криптовалюта річчю у розумінні цивільного права, яка форма угоди у смарт-контракту, тощо. Тобто в даному разі мова йде про розгляд проблеми лише у вузьких рамках окремої галузі права.

Чи можливо розглядати проблему комплексно?

Можливо, але не в рамках усталених галузей української юридичної науки. За межами нашої держави висловлено різна кількість цікавих правових концепцій, починаючи від «права-коду» Л.Лессіга [7] і закінчуючи концептуалізацією криптоправа К.Рейес [8]. З огляду на обсяг виступу не маємо змоги викласти відповідні концепції, але можливо зосередити увагу на наступних питаннях, що зумовлюють, на думку К.Рейес, концептуалізацію особливого права. В основі є розміркування над феноменом «смарт-контрактів», що з юридичного боку не є контрактами взагалі. На думку К.Рейес концептуалізація криптоправа проявляється в тому, що застосування технології по суті і є правом, що регламентує суспільні відносини, при цьому у ході таких відносин право формується та змінюється [8, p. 399]. Дану точку зору не слід плутати з «м'яким правом», що зосереджено на питаннях юридичної сили та примусу. У даному разі юридична сила та примус зумовлені самою технологією, отже криптоправо не може бут м'яким. Звичайно, К.Рейес розуміє право не так, як традиційно розуміють його позитивісти, точка зору яких традиційно є панівною на пострадянському просторі. Ключовим моментом у міркуваннях вченої є те, що правова структура (CLS), формується технологією і заміняє собою державу, при цьому примус і юридична сила приписів забезпечується самою крипто-технологією. Саме структури, а не технології, не їх прояви і не відносини осіб з використанням технологій повинні піддаватись регуляторному впливу держави.

Зазначене вище лише вкрай схематично викладає загальні підходи, але на нашу думку беззаперечним є те, що DLT здатні здійснити серйозний вплив на сутність права та юридичну науку схожий з тим впливом, що здійснила усередині 1990-х років поява Інтернету як глобальної мережі.

Використана література:

1. Баранов О.А. Інтернет речей (IoT) і блокчейн/ Інформація і право. 2018. № 1 (24). С. 59-71.

2. Миняйло Н. Квартира за «эфиры». Как обменять криптовалюту на жилье в Киеве/Delo.ua. 03/10/2017. URL: https://delo.ua/business/kvartira-za-efiry-vozmozhno-li-kupit-zhile-v-kieve-za-kriptov-335064/

3. Мамченко Н. Криптовалюта в Украине: судебная практика и новые законопроекты/ Судебно-юридическая газета. 23.10.2017. Выпуск 35-38. URL: https://sud.ua/ru/issue/339

4. Середа А. Налогообложение операций с криптовалютами в Украине/Бухгалтер 911. 26.03.2018. URL: https://buhgalter911.com/news/news-1036240.html

5 Самоходський І., Шелест О. Зелена книга регулювання ринку криптовалют. Травень 2018. К.: Офіс ефективного регулювання, 2018. 80 с.

6. Проект розпорядження Кабінету Міністрів України «Про схвалення Концепції державної політики у сфері віртуальних активів», підготовлений Міністерством економічного розвитку і торгівлі України, 25.10.2018. URL: http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=dbfc2a7e-47f9-4fce-911066ed61c0ae17&title=ProektRozporiadzhenniaKabinetuMinistrivUkrainiproSkhvalenniaKontseptsiiDerzhavnoiPolitikiUSferiVirtualnikhAktiviv

7. Lessig Lawrence. The Code in Law, and the Law in Code. Draft: 15.03.2000. URL: https://cyber.harvard.edu/works/lessig/pcforum.pdf

8. Reyes Carla. Conceptualazing Cryptolaw/Nebraska Law Review. 2017. Vol. 96. Issue 2. P. 385-445.

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

Карчевський М. В.,
д.ю.н., професор, перший проректор
Луганського державного університету
внутрішніх справ імені Е. О. Дідоренка

ПРАВО ПРОТИ ТЕХНОЛОГІЧНОГО «КІНЦЯ СВІТУ»

Найбільш радикальним поглядом на перспективи людства в контексті розвитку технологій є концепція технологічної сингулярності. Її автор, В. Віндж, уважає, що після появи інтелекту, який перевершить людський, швидкість прогресу стане надвеликою. Людство опиниться в «режимі, який відрізняється від нашого минулого не менш радикально, ніж ми, люди, самі відрізняємося від нижчих звірів. Така подія анулює через непотрібність всі людські закони, можливо, в одну мить. Некерована ланцюгова реакція почне розвиватися за експонентою без будь-якої надії на відновлення контролю за ситуацією» [3]. На думку В. Віндж, до цього приведуть або технології штучного інтелекту (artificial intelligence, AI), або технології підсилення інтелекту людини (intelligence amplification, IA).

Гіпотеза появи AI достатньо широко представлена у літературі. Питання частково розглядалося нами раніше [5]. В свою чергу, IA потребує певних коментарів. У науці все помітнішою стає скептична думка щодо реальності повноцінного автономного штучного інтелекту. Існує навіть таке неперевірене припущення, що прогнози його появи роблять, як правило, ті, хто дуже поверхово стикається з технічним боком питання. Наприклад, Девід Мінделл на підставі емпіричного дослідження з питань застосування сучасних роботів формулює так звані «міфи робототехніки», тобто типові хибні уявлення щодо її перспектив [9]. Зокрема, повна автономність штучного інтелекту розглядається як «утопічна ідея

про те, що сьогодні або в майбутньому роботи зможуть діяти повністю самостійно» [9, с. 11-12].

Технічний прогрес може піти шляхом фізичної інтеграції людини та технологій. Комплекс означених питань розглядають дослідники проблематики трансгуманізму. За визначенням Ніка Бострома «трансгуманізм – це спосіб мислення про майбутнє, який базується на тій підставі, що людина в її нинішній формі не є кінцем нашого розвитку». Трансгуманізм розглядається як «інтелектуальний та культурний рух, який відстоює можливість і бажаність принципового поліпшення стану людини через застосування, розвиток та надання широкого доступу до технологій ліквідації старіння, посилення людських інтелектуальних, фізичних і психологічних можливостей». Крім цього, трансгуманізм може розглядатися як «вивчення наслідків, потенційних переваг та небезпек технологій, які дають змогу подолати основні людські обмеження, а також пов'язане вивчення етичних питань, обумовлених розробкою та використанням таких технології» [0].

До соціальних трансформації, що можуть бути викликані використанням технологій трансгуманізму, як правило, відносять наступні. Створення абсолютно контрольованої еволюції людини в інтересах глобальних корпорацій [7]. Поява нових видів реалізації морфологічної свободи (можливість змінювати своє тіло на власний розсуд) та права на репродукцію (допоміжні репродуктивні технології, сурогатне материнство, донорство генетичного матеріалу, посмертна репродукція, дизайн дітей) [12,2]. Принципово нові види посягань – біогенетичні та когнітивні [8]. Нові способи вчинення злочинів проти життя та здоров'я.

Отже технологічна сингулярність розглядається як загальний негативний фінал однієї з двох гіпотез: або розвиток автономного штучного інтелекту, або розвиток технологій, які підсилюватимуть здатності людини (технології трансгуманізму). Однак попри аргументи про невідворотність такого сценарію, проведений нами аналіз перспективних завдань права свідчить про те, що людство має можливість зберегти контроль над ситуацією. Розв'язання у ефективному правовому регулюванні. З урахуванням зроблених раніше висновків [5], основні положення щодо його забезпечення наступні.

1. Розвиток технологій неможливо заборонити. Попри ризик небезпек абсолютна заборона розробки систем штучного інтелекту чи трансгуманістичних технологій є неможливою. Правове регулювання у цій сфері має забезпечувати стимулювання соціально ефективного використання технологій та мінімізацію ризиків зловживання технологією. Окремим завданням правового регулювання в даному контексті має стати обмеження деструктивних впливів глобальних корпорацій.

2. Правове регулювання має забезпечити максимальну диверсифікацію технологічних рішень. Технологія має не обмежуватися, а навпаки стати якомога різноманітнішою. Якщо право буде формувати умови/вимоги для створення якомога більшої кількості різноманітних рішень у сфері технологій, це

забезпечить ефективне попередження розвитку негативних наслідків. Наприклад, відомі негативні сценарії «епідемії» імплантатів (заподіяння шкоди людству через порушення роботи всіх імплантованих пристроїв) або «чорного слизу» (знищення біомаси планети наноботами, що виконують програму самовідтворення) будуть просто неможливими, через гарантовану наявність альтернативних технічних рішень.

3. Актуальною та затребуваною для сучасного рівня технологій є класична схема «розробник-власник-користувач». Так, Резолюцією Європарламенту від 16 лютого 2017 року щодо норм цивільного права про робототехніку пропонуються такі механізми як створення системи реєстрації роботів, спеціального фонду страхування цивільної відповідальності, пропорційна відповідальність розробників та власників роботів, залежна від часу, протягом якого власник здійснював навчання робота тощо [10]. Ускладнення технологій вимагатиме переходу до нової, більш складної, схеми правового регулювання. Певно, що правове регулювання соціалізації штучного інтелекту пройде шлях від розгляду робота як об'єкта відносин до наділення його правами, обов'язками та відповідальністю. Визнання роботів суб'єктами права можна розглядати як закономірний результат розвитку технологій. Наприклад, згадана резолюція Європарламенту вводить у юридичний обіг поняття «електронна особистість». О.Е. Радутний досліджує можливості кримінально-правового регулювання в сфері робототехніки за допомогою інституту,побудованого на основі кримінально-правових заходів, що застосовуються до юридичних осіб [11]. В контексті суб'єктності потребуватиме розв'язання і проблема правового статусу фізичної особи, здатності якої підсилені за допомогою технологій трансгуманізму. Гіпотетично дана проблема не видається складною і може бути розв'язана шляхом додавання певних обтяжуючих або пом'якшуючих обставин, обмежень щодо обіймання певних посад, виконання робіт тощо.

4. Крім традиційної юстиції, ітиметься про появу двох нових видів, умовно назвемо їх «змішана юстиція» та «юстиція штучного інтелекту», функціонування якої буде забезпечувати протидію роботам, що є загрозою для соціального розвитку та стабільності. Юстиція штучного інтелекту буде створена на основі роботів. Така система передбачатиме узагальнення в чіткі алгоритми досвіду, отриманого за час існування традиційної юстиції.

5. Забезпечення правових гарантій реалізації морфологічної та репродуктивної свободи шляхом балансу між реалізацією права певною особою та потребою забезпечити загальну безпеку, стабільність та розвиток.

6. Розв'язання питання про межі кримінально-правового регулювання в сфері біогенетичних та когнітивних утручань, суспільно-небезпечних порушень морфологічної або репродуктивної свободи, а також порушень вимог диверсифікації технологічних рішень.

7. Оскільки контроль за розвитком та використанням певних технологій вимагатиме ефективної системи моніторингу, аналіз юридично значимої

інформації стане набагато складнішим та вимагатиме принципово нових професійних компетенцій. Традиційний розподіл завдань між юристами та спеціалістами стане вкрай неефективним. Буде спостерігатися конвергенція юридичних та технічних наук. Потребуватиме розв'язання питання визначення та розвитку нових видів юридичних професій.

8. Правове регулювання в сфері використання сучасних технологій має бути технологічно нейтральним. Наприклад, ч. 3 ст. 190 КК України передбачає відповідальність за «шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки». На момент набрання чинності новим КК України (17 років тому) застосування комп'ютерної техніки для здійснення шахрайства дійсно могло свідчити про підвищену суспільну небезпечність посягання. Поширеність засобів електронної комерції, систем дистанційного банківського обслуговування була незначною. Користувалися ними великі господарюючі суб'єкти. Тому положення ч.3 ст. 190 КК досить чітко окреслювали коло діянь, які обґрунтовано було розглядати як *особливо кваліфікований вид шахрайства*, близький по ступеню суспільної небезпечності до шахрайства у великих розмірах. Проте стрімкі темпи проникнення інформаційних технологій у фінансову сферу зумовили якісну зміну даного виду шахрайства. Правоохоронні органи фіксують відчутну кількість таких злочинів, зв'язаних із спричиненням шкоди, що відповідає ознакам простого або кваліфікованого шахрайства (ч. 1, ч. 2 ст. 190 КК). Чи можна вважати обґрунтованою, а саме цього вимагає тлумачення норми, кримінально-правову оцінку таких дій за ч. 3 ст. 190 КК? Питання швидше риторичне. У сучасних умовах немає підстав стверджувати, що використання електронно-обчислювальної техніки в процесі здійснення шахрайства настільки підвищує рівень суспільної небезпечності вчиненого діяння. Маємо ситуацію, коли технологічно орієнтована правова норма (ч. 3 ст. 190) втрачає актуальність саме через наявність у ній положень, що відносяться до певної технології. Схожий приклад можна навести з кримінально-правовим регулюванням в сфері використання криптовалюти. З великою вірогідністю можна прогнозувати появу пропозицій щодо доповнення КК відповідними спеціальними нормами. Разом з цим, більш глибокий аналіз чинного законодавства наочно демонструє можливості юридичного відображення новітніх технологічних тенденцій за допомогою наявних загальних норм[6]. Швидкість розвитку технологій вимагає відмовлятися від законодавчих формулювань, що вказують на певні види технологій. Будь який закон, пов'язаний із конкретною технологією матиме дуже обмежений час корисного існування.

Наприкінці хотілося б звернути увагу на сучасний стан речей та актуальність проблематики для національного правового поля. Зараз Україна не в лідерах розвитку сучасних технологій (хоча перша в світі енциклопедія кібернетики була видана саме українською). Деякі бачать у цьому позитив – небезпека новітніх загроз для нас нібито є значно нижчою. Але це не так. Існує

відома проблема яка називається «цифровий розкол» (digital divide). Успішність соціальної групи, країни перебуває у прямій залежності із можливістю доступу до сучасних інформаційних технологій. Соціальні групи, країни, які не мають доступу (мають обмежений) до новітніх на даний момент часу інформаційних технологій з дуже незначною вірогідністю зможуть його отримати в майбутньому. З часом різниця рівня використовуваних технологій буде збільшуватися.

Крім очевидних проблем з вітчизняним виробництвом маємо ситуацію, коли чинне законодавство певною мірою блокує розвиток сучасних інформаційних технологій. Йдеться, зокрема, про доступ до персональних даних та державних інформаційних ресурсів. Схема правового регулювання така, що не забезпечує динамічної та прогнозовано результативної реалізації проектів в сучасних сферах використання інформаційних технологій.

В таких умовах перше, що необхідно зробити, для того щоб не опинитися на сумному та безперспективному боці «цифрового розколу» - максимально лібералізувати та дерегулювати діяльність, пов'язану із обробкою персональних даних. Це створить в Україні підґрунтя для стрімкого розвитку сучасних інформаційних технологій: інтернету речей, Big Data тощо. Стануть можливими амбітні інноваційні проекти. Питання безпеки персональних даних, що набуде надзвичайної гостроти також отримає нові, набагато ефективніші способи розв'язання. Активне використання персональних даних у правовому полі створить ринок необхідний для розвитку технологій їх обробки та захисту.

О.А. Баранов визначає наступні правові проблеми, пов'язані з розширенням використання технологій Інтернету речей: «визначення механізмів реалізації принципу попередньої згоди на використання та "на стирання" персональних даних (ст. 17 Регламенту ЄС 2016/679 від 27.04.16 р.); правовий вплив на регулювання транскордонних потоків персональних даних, що передбачає не тільки цілеспрямовану діяльність по впорядковуванню інформаційних відносин, але і непряму дію правових засобів і методів на різних суб'єктів, що не підпадають безпосередньо під правове регулювання; використання персональних даних інтелектуальними комплексами, що функціонують без участі суб'єктів (юридичних або фізичних осіб)»[4]. Крім цього формулює висновок про те, що необхідність створення багаторівневої і багатооб'єктної системи захисту персональних даних «потребує формування нової системи правового регулювання» [4].

Слід погодитися с дослідником. Висловлені О.А. Барановим положення знаходять певне підтвердження на рівні судових рішень ЄСПЛ. Так, у справі Big Brother Watchand Othersv. The United Kingdom (2018)розглядалися питання аналізу інтернет трафіку та його співвідношення з «класичними» видами порушення приватності. Зрозуміло, що аналіз значної кількості даних щодо інтернет-з'єднань здатен порушити приватність особи значно істотніше ніж навіть візуальне спостереження. Нова технологічна реальність вимагає нових правових рішень.

Разом з цим, очевидно, що правовий режим персональних даних представляє собою лише частку глобальної правової проблеми. Називати її будемо

формування правових гарантій ефективного розвитку навколишнього інформаційного середовища. Це комплекс питань, що стосуються правового регулювання використання інформаційних технологій, забезпечення доступу до інформації, а також формування інформаційного ресурсу. При цьому регулювання формування інформаційного ресурсу має включати не тільки зрозумілі сьогодні питання створення баз даних, діяльності ЗМІ, попередження маніпуляцій суспільною свідомістю тощо. Самостійним аспектом проблеми має стати побудова оптимального правового режиму збереження накопичуваних людством даних та забезпечення доступу до цього ресурсу. Живі істоти, які сотні мільйонів років тому спостерігали формування вугільних пластів (або самі ставали їх часткою) навряд чи могли передбачити появу вугільної промисловості, металургії, теплоелектростанцій тощо. Сьогодні відбувається схожий процес. Людство накопичує величезні об'єми даних. Як вони будуть використовуватися через значний проміжок часу невідомо, однак очевидно що їх використання відбуватися буде. Якщо так, необхідно досліджувати можливості (доцільність) правового регулювання зберігання та використання даних, що накопичує людство. Потребуватиме розв'язання питання власності таких активів, переходу їх у статус виключної власності народу держави (планети) або даних, що можуть вільно використовуватися будь ким. Можливо є сенс режим великих масивів відпрацьованих даних організовувати на основі правових механізмів, що використовуються сьогодні для регуляції археологічної діяльності.

В решті решт, регулювання інформаційного навколишнього середовища можна розглядати як встановлення координатної системи для майбутньої правової оцінки як штучного інтелекту так і технологічно вдосконалених людей,оскільки саме в цій сфері відбуватиметься переважна частина їх соціально значимої активності.

Використана літераратура:

1. Bostrom N. The transhumanist frequently asked questions: a general introduction. Nick Bostrom`s personal site. URL :http://nickbostrom.com/views/ transhumanist.pdf (дата звернення: 16.08.2018).
2. Sandberg A. Morphological Freedom - Why We not just Want it, but Need it. Trans Vision Conference. Berlin, June, 22 - 24, 2001. Anders Sandberg's pages. URL: http://www.aleph.se/Nada/Texts/MorphologicalFreedom.htm (дата звернення: 16.08.2018).
3. VingeV. The Coming Technological Singularity .Acceleration Studies Foundation. URL: http://www.accelerating.org/articles/comingtechsingula-rity.html (дата звернення: 16.08.2018).
4. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей. Інформація і право. 2016. № 2(17). С. 83-89.
5. Карчевський М. В. Правове регулювання соціалізації штучного інтелекту. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2017. № 2. С. 99-108.
6. Карчевський М.В.Безготівкові гроші, електронні гроші, криптовалюта. Сайт дистанційного навчання Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.URL : http://lduvs.lg.ua/mod/page/view.php?id=7375 (дата звернення: 21.11.2018)

7. Комлева Н. А. Трансгуманизм и «гуманитария» как угроза правам человека. Научная электронная библиотека КиберЛенинка. URL : https://cyberleninka.ru/article/n/transgumanizm-i-gumanitariya-kak-ugroza-pravam-cheloveka (дата звернення: 16.08.2018).
8. Майоров А. В., Потапов А. Д., Волкова А. М. Синтез человека и технологий в XXI веке: основные вызовы и угрозы. Научная электронная библиотека КиберЛенинка.URL : https://cyberleninka.ru/article/n/sintez-cheloveka-i-tehnologiy-v-xxi-veke-osnovnye-vyzovy-i-ugrozy (дата звернення: 16.08.2018).
9. Минделл Д. Восстание машин отменяется! Мифы о роботизации. М.: Альпина диджитал, 2015.164 с.
10. Нормы гражданского права о робототехнике. Резолюция Европарламента от 16 февраля 2017 года. P8_TA-PROV(2017)0051. Переклад Незнамов А.В. для Robopravo.ru. URL : http://robopravo.ru/riezoliutsiia_ies (дата звернення: 19.09.2018).
11. Радутний О. Е. Суб'єктність штучного інтелекту у кримінальному праві. Право України. 2018. № 1. С. 123 – 136.
12. Рыбаков О. Ю., Тихонова С. В. Конвергенция технологий, репродукция человека и естественное право: философия трансгуманизма. Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2017. № 2. С. 100 - 105.

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

Харитонов Є. О.,
д.ю.н., професор, зав. кафедрою Національного університету «Одеська юридична академія», член-кор. НАПрН України
Харитонова О. І.,
д.ю.н., професор, зав. кафедрою Національного університету «Одеська юридична академія», член-кор. НАПрН України

ДО ПРОБЛЕМИ ЦИВІЛЬНОЇ ПРАВОСУБ'ЄКТНОСТІ РОБОТІВ

В матеріалах торішньої конференції, присвяченої проблемам Інтернету речей, ми, спираючись на розуміння Інтернету речей як сукупності взаємодіючих технічних систем і комплексів, призначених для реалізації суспільних відносин, у тому числі, пов'язаних з наданням послуг або проведенням робіт, на основі використання різноманітних даних і мережі Інтернет за безпосередньої участі або без участі суб'єктів цих відносин (юридичних або фізичних осіб) [1, с. 101], ми обстоювали позицію, що існують усі підстави вважати ІР об'єктом цивільних правовідносин.

Такий висновок, зокрема,обґрунтовувався й тим, що у згаданому визначенні ІР йшлося про те, що «надання послуг або проведення робіт» відбувається «за безпосередньої участі або без участі суб'єктів цих відносин (юридичних або фізичних осіб)». Тобто, таке формулювання припускає, що суб'єктами відносин (правовідносин) Інтернету речей є юридичні або фізичні

особи. Але Інтернет речей (штучний інтелект, який у ньому використовується) не є ні тим, ні іншим.

Недостатньо переконливою (точніше, занадто абстрактною) видавалася й теза, що роботи, використовувані в Інтернеті речей можуть бути як об'єктом, так і суб'єктом суспільних відносин, а значить можуть бути і об'єктом, і суб'єктом правовідносин [2]. Погоджуючись з думкою, що інформаційне поле не є унікальною особливістю лише біологічних організмів, а виступає загальною властивістю Всесвіту [3], ми, водночас, виходили з того, що при сучасному рівні знань вплив на інформаційне поле з метою його впорядкування реально можливий лише у частині його біологічного (людського) субстрату. Чим, власне і обґрунтовувався кінцевий висновок, що Інтернет речей є, поки що, об'єктом, але не суб'єктом правовідносин.

Однак розвиток інформаційних технологій відбувається, навіть, швидшими темпами, ніж очікувалося. Практично щоденно з'являються новини про використання різних форм штучного інтелекту, на які покладаються функції, котрі раніше (і поки що) виконували люди (медичні, юридичні, журналістські, мистецькі, комунальні послуги, керування транспортними засобами тощо).Причому, вже йдеться не просто про використання ІТ як інструментарію в руках людини, а про, значною мірою, автономне функціонування штучного інтелекту в межах і умовах визначених завдань з метою виконання останніх. Наступним кроком може стати створення «загального штучного інтелекту», здатного запам'ятовувати отримані навички і використовувати їх для вирішення наступних проблем, що до останнього часу вважалося відмінною рисою людини, тобто, такого, що відповідає інтелекту(способу мислення) людини [4]. Непоодинокими є випадки оригінальної інтерпретації машинами (програмами) завдань, поставлених для них людиною, що нагадує сюжети антиутопій, оскільки штучний інтелект поки що виглядає для науковців як «чорний ящик» [5].

Це зумовлює необхідність перегляду парадигми правосуб'єктності роботів (Штучного інтелекту) у контексті пошуку відповіді на низку питань функціонування Інтернету речей як сектору цивільного обігу. Зокрема, хто виступає стороною відносин послуг, «самостійно» наданих комп'ютером? Хто має відповідати за помилки програми? Адже власник комп'ютера – лише власник, програміст – лише складає програму, провайдер – лише посередник у наданні послуги тощо).

У зв'язку з цим варто зауважити своєчасність появи публікацій на цю тему, зокрема, «проривної», як ми б її назвали, статті О.А. Баранова «Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах», [6, с. 75-95] у якій обґрунтовується необхідність визнання роботів зі штучним інтелектом, які є найважливішим елементом технологій Інтернету речей, суб'єктами суспільних відносин – «еквівалентами фізичної особи».

Погоджуючись з багатьма положеннями запропонованої концепції, маємо зазначити, що низка її аспектів потребує всебічного обговорення і наступного доопрацювання.

Зокрема, здається недоцільним вести мову про загальну правосуб'єктність ШІ, розглядаючи роботів як гіпотетичних учасників будь-яких правовідносин. Досить складно уявити роботів суб'єктами конституційних, адміністративних, карних тощо відносин. Натомість, «природною» є їхня участь у цивільних правовідносинах, оскільки, власне, для оптимізації цивільного обігу і створювався Інтернет речей. Отже першою видозміною має бути постановка питання про визнання ШІ суб'єктом цивільних правовідносин. (Власне, використовуваний у дискусії термін «фізична особа» також запозичений з цивілістики). Відправним положенням тут є те, що на практиці учасники відносин у ІТ-сфері переважно виступають як учасники цивільних відносин, а відтак характеризуються певним цивільно-правовим статусом.

Разом із тим, як на наш погляд, конструкт «еквівалент фізичної особи» виглядає не надто вдалим. Слід зазначити, що критичний підхід до його використання не стосується можливості визнання «штучного інтелекту» учасником відносин у сфері використання ІТ (Інтернету речей), квазі-суб'єктом цивільних правовідносин, однак є рушійною силою до пошуку інших юридичних прийомів залучення роботів з ШІ до участі у цивільних відносинах.

Зокрема, таким прийомом може бути використання категорії «юридична особа», підставою для чого можуть слугувати й положення чинного цивільного законодавства. Так, згідно зі ст.2 ЦК України учасниками цивільних відносин можуть бути фізичні та юридичні особи, держава Україна, територіальні громади, іноземні держави та інші суб'єкти публічного права. Спираючись на цю норму, можемо запропонувати розуміння сутності роботів зі штучним інтелектом, як «квазі-юридичної особи», чи, якщо завгодно, «еквіваленту юридичної особи». Чому саме юридичної, а не фізичної особи? З тих міркувань, що фізична особа – це людина, і це змусить запровадити низку обмежень і спеціальних застережень при визначенні правосуб'єктності роботів. Натомість, «юридична особа» сама по собі є фікцією, що дозволяє позірно визначати її ознаки, вимоги до правового статусу, застосовувати у необхідних фактах «подвійну» фікцію тощо. Прикладів такого гнучкого підходу в сучасному правопорядку маємо досить багато. Скажімо, чим, як не «подвійною» фікцією, є визнання юридичною особою повного товариства, так само, як і «onemen company»? (на тлі того, що вже сама юридична особа є фікцією, названі види юридичних осіб, навіть, не мають ознак навіть цієї«фіктивної особи»).

Зауважимо, що, загалом, нічого аж надто незвичайного у такому підході нема, якщо згадати, що своїм визнанням суб'єктом цивільних прав і обов'язків юридична особа завдячує, зокрема, саме такому прийому як фікція.

Тому не бачимо достатньо вагомих заперечень проти того, аби визнати ще одну фікцію – квазі-юридичну особу – роботів зі «штучним інтелектом».

Необхідною умовою участі особи у цивільних правовідносинах є наявність у неї цивільної правосуб'єктності, тобто соціально-правової можливості (здатності) бути учасником цивільних відносин, яка охоплює правоздатність та дієздатність.

Цивільна правоздатність – це здатність суб'єкта мати цивільні права і обов'язки. (У ЦК України загальне визначення правоздатності відсутнє, однак, містяться окремі визначення правоздатності фізичних (ст. 25) і юридичних (ст. 68) осіб, які фактично тотожні). Цивільна дієздатність – це здатність суб'єкта своїми діями набувати для себе цивільні права і створювати цивільні обов'язки. Дієздатність у ЦК визначена тільки стосовно фізичних осіб. Такий підхід тут є виправданим, оскільки щодо юридичних осіб ці два поняття завжди існують нерозривно. Тому наявність правоздатності у організації означає, що вона володіє і дієздатністю. У зв'язку з цим іноді вживається термін «праводієздатність юридичної особи». Такий підхід виправдано, як на нашу думку, може застосовуватися і для характеристики правосуб'єктності «віртуальних осіб (організацій)».

Зміст дієздатності роботів з ШІ, як учасників цивільних відносин, з позицій оцінки можливості їхньої участі у оборудках в ІТ-сфері можна визначити наступним чином.

Оскільки правосуб'єктність юридичної особи охоплює і правоздатність, і дієздатність, стосовно неї можна вести мову про різні види правосуб'єктності (диференціацію правосуб'єктності). Щоб не вдаватися до складних словесних конструкцій, правосуб'єктність у таких випадках доцільно позначати скорочено – «здатність», маючи на увазі, що йдеться про здатність юридичної особи бути суб'єктом певних цивільних відносин.

Розрізняємо такі види правосуб'єктності юридичної особи: 1) правочиноздатність; 2) деліктоздатність; 3) трансздатність; 4) бізнесздатність. Разом із тим, пропонуємо включити до переліку видів правосуб'єктності юридичної особи також «кіберздатність», під якою маємо на увазі здатність бути активним учасником відносин у ІТ-сфері (укладати договори як користувач, бути учасником соціальних мереж, приймати участь в інтерактивних акціях тощо). Відмінність від правочиноздатності тут полягає в тому, що «кіберздатність» може реалізовуватися за допомогою не лише правочинів, а й юридичних вчинків). Слід також наголосити, що «кіберздатність» варто розглядати як елемент спеціальної правосуб'єктності роботів зі штучним інтелектом.

Використана література:

1. Баранов О. «Інтернет речей» як правовий термін // Юридична Україна. – 2016. – № 5-6. – С. 96-103.

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

3. Бог повсюду. Физик из США выдвинул теорию о том, что Вселенная обладает сознанием: – URL: http://nv.ua/techno/science/bog-povsjudu-amerikanskij-fizik-vydvinul-teoriju-o-tom-chto-vselennaja-obladaet-soznaniem-1546675.html

4. Исследователи Google создали искусственный интеллект, способный учиться как человек. – URL: https://zn.ua/TECHNOLOGIES/issledovateli-google-sozdali-iskusstvennyy-intellekt-sposobnyy-uchitsya-kak-chelovek-242259_.html

5. Черная коробочка. У ученых появилась серьезнейшая проблема с ИИ. – URL: https://glavnoe.ua/news/n327461-chernaja-korobochka.-u-uchenyh-pojavilas-sereznejshaja-problema-s-ii

6. Баранов О. А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах // Юридична Україна. – 2018. – № 5-6. – С. 75-95.

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

Радутний О. Е.,
доктор філософії (Ph.D.) в галузі юридичних наук, доцент, доцент кафедри кримінального права № 1 Національного юридичного університету імені Ярослава Мудрого (м. Харків)

ДОДАТКОВІ АРГУМЕНТИ ЩОДО ПРАВОСУБ'ЄКТНОСТІ ШТУЧНОГО ІНТЕЛЕКТУ

Дискусія про доцільність визнання штучного інтелекту суб'єктом правовідносин набирає обертів через обґрунтоване очікування появи у найближчий короткий час штучного інтелекту вищого ступеню розвитку (суперінтелекту – Artificial Superintelligence, ASI) [1], когнітивні властивості якого (зокрема, сприйняття інформації, розпізнавання об'єктів та їх класифікація, творчість та генерування нових знань, оцінка ситуації, вибір оптимальної стратегії і тактики дій, побудова ціннісних суджень, самостійність прийняття рішень і самостійне їх виконання, пам'ять як повне збереження всього набутого обсягу інформації тощо) будуть перевищувати відповідні здібності людини. Завдяки повній обізнаностіASI у принципах своєї побудови і роботи, самонавчанню, саморозвитку та самовдосконаленню врешті решт утвориться ситуація, за яку будуть відсутні фактичні та правові підстави для притягнення до відповідальності як його розробника (виробника), так і користувача або власника.

У зв'язку з цим підтримки та подальшого розвитку заслуговує пропозиція щодо визнання штучного інтелекту суб'єктом правовідносин, яку аргументують О.А. Баранов (роботи-андроїди можуть виступати стороною у суспільних відносинах тому, що вони можуть самостійно оцінювати дії інших суб'єктів і самостійно формувати або змінювати мету та зміст своїх дій, їх дії не можуть бути заздалегідь передбачені)[2, с. 31 – 45], М.В. Карчевський [3, с. 109 – 113; 4], Крістофер Хернас (Christoffer Hernæs) [5], проф. University of Washington School of Law Райан Кало (Ryan Calo), проф. Umeå Universitet (Швеція) Питер Асаро (Peter M. Asaro), а так само автор цих тез [6, с. 98 – 102; 7, с.123 – 136; 8, с. 200 – 206].Нормативне закріплення такої пропозиції знайшло свій вираз у відповідній Резолюції Європейського парламенту від 16.02.2017 р. (European Parliament resolution of 16 February 2017 with recommendations to the Commissionon Civil Law

Rules on Robotics (2015/2103(INL) [9], в якій пропонується серед вже відомих категорій (фізичні особи та юридичні особи) утворити нову під назвою «електрона особа (особистість)», яка матиме власні специфічні права та обов'язки. Тому в сфері кримінального права та інших правових дисциплін, що опікуються загальною та інформаційною безпекою, необхідно зосередити зусилля у зазначеному напрямку, популяризувати, аргументувати та розвивати вказану ідею.

Поряд з цим залишається актуальною позиція В.А. Мисливого [10, с. 122 – 126] щодо обґрунтованості притягнення водія (яким є фізична особа) до відповідальності у випадку помилкових дій автопілота AV (AutonomousVehicles – транспортного засобу під керуванням штучного інтелекту), але лише до того часу, поки всі місця в останньому не будуть перетворені у пасажирські.

Обачливість пропозиції О.А. Баранова про можливість визнання робота з штучним інтелектом не рівноправним а́ктором (діючим суб'єктом, який вчиняє дії, що спрямовані на інших), а лише правовим *еквівалентом* фізичній особі (одного разу у тексті – юридичній) в якості суб'єкта правовідносин [11], тобто фактично лише правовим сурогатом, скоріш за все, має витоки в феноменальності та революційності самого запропонованого підходу. Але, якщо відкинути сторонні заклики (на кшталт «цього не може бути», «це не притаманно всьому, що ми до цього часу знали» та інші подібні), то у сухому залишку отримаємо той беззаперечний факт, що суб'єктність фізичної особи має підґрунтя лише у тому, що людина сама визначає правила, за яким включає будь-кого у коло суб'єктів правовідносин (себе, тобто фізичну особу, а також юридичну особу, державу, інші утворення) або не приймає сюди інших (тварин, рослин, роботів тощо). Доктринальне закріплення такого стану речей відбувається на рівні загальної теорії права та галузевих напрямків, нормативне – в положеннях міжнародних актів, Конституції та іншого суверенного законодавства.

Однак, припустимо в якості моделі для роздуму, що людство зустрічає іншу високо розвинуту або таку ж саму цивілізацію. У цьому випадку питання про можливість правової взаємодії та наділення її представників правосуб'єктністю навіть не стоятиме. Цілком абсурдною виглядала би заява про те, що ми не можемо з вами вступати у правові відносини, оскільки за вами у наших документах не було закріплено певного статусу. У порядку денному будуть лише питання про своєчасність та механізм внесення змін у чинне законодавство. І поряд з звичними суб'єктами правовідносин з'являться нові. Рішення про розширення кола суб'єктів правовідносин буде залежати не від Бога, оракула або сил природи, а від самої людини. Відразу в міжнародні акти, відповідні Конституції та інше національне законодавство будуть внесені певні зміни, завдяки чому умови так званог осуспільного колективного договору зазнають певної трансформації.

Але так само можливо роздивитися й навколо, чи не є поряд з людиною та її звичними штучними утвореннями (юридична особа, держава, громада, належним чином оформлений колектив тощо) інші претенденти, які заслуговують на

надання їм статусу суб'єкта правовідносин. Зокрема, відповідно до Кембриджської декларації про свідомість (The Cambridge Declaration on Consciousness) від 7 липня 2012 р. [12], люди не є унікальними у наділенні неврологічними механізмами, які генерують свідомість, а разом з нею і свідому поведінку. Свідомість властива всім ссавцям, всім птахам і багатьом іншим тваринам, зокрема деяким членистоногим і головоногим молюскам (наприклад, восьминогам та кальмарам).Штучне збудження одних і тих же ділянок мозку у людини і у тварин викликає відповідну поведінку і чуттєвий стан. Причому, де б в мозку у тварин не відбувалось таке штучне збудження, більшість форм їх подальшої поведінки узгоджуються з дослідженими чуттєвими станами. Це і є прояв того, що має назву усвідомленої поведінки. Зазначена декларація покладає тягар спростування її висновків на тих, хто переконаний у протилежному,але надає аргумент для визнання свідомості у штучного інтелекта та визнання правосуб'єктності останнього. У будь-якому випадку, оскільки мова йде не про примітивного робота або алгоритм, а про ASI, то останній фактично стане представником іншої високо розвинутої цивілізації, яку ми несподівано виявимо поряд з людством на планеті Земля.

Якщо, виходячи з доволі молодої по історичним міркам гуманістичної антропоцентричної концепції, правосуб'єктність фізичної особи презюмується і не вимагає доказів, то слід згадати, що таке саме право для юридичної особи як доволі новаторського суб'єктного утворення теж колись було дивним і провокаційним, але через незначний час стало звичним і сьогодні сприймається як аксіома без будь-яких доказів. Вважається само собою зрозумілим, що таке штучне утворення, як юридична особа, яке позбавлене фізичної форми і про діяльність якого ми дізнаємося лише з паперів або через прояви поведінки його повноважних представників (як фізики дізнаються про існування електрону лише по слідам, що він залишає за собою), має права й обов'язки і є повноцінним суб'єктом правовідносин. Раніше невідома сутність (юридична особа) була створена лише однією силою людської думки, тож ніщо не заважає останній визначитися певним чином й щодо штучного інтелекту. Фокусування уваги на тому, яким саме чином у площині права вдалося домовитися про те, що носієм прав та обов'язків стане нове штучне утворення (юридична особа, замістьїї засновників або учасників – фізичних осіб), дає дороговказ наукового та законодавчого пошуку.

Таким чином, твердження О.А. Баранова про кардинальну протилежність ситуації щодо можливості визнання суб'єктом правовідносин фізичної особи та штучного інтелекту підлягає, з дозволу дослідника, певному вдосконаленню: це лише поверхово здається, що ситуація кардинально протилежна, насправді, вона така сама, як й щодо юридичних осіб. Якщо постулатом загальної теорії права є твердження про те, що особа визнається суб'єктом правовідносин лише тому, що вона здатна бути суб'єктом права (С. Алексєєв, А. Венгеров, М. Козюбра, О.

Петришин, С. Погребняк, М. Цвік, О. Скакун, В. Смородинський та інші), то воно не утворює жодних перешкод для штучного інтелекта.

Тому й друге твердження О.А. Баранова (про необхідність окремого доведення можливості визнання правосуб'єктності за штучним інтелектом)так само, з повагою до першопроходця, може бути розвинуте: факт можливості визнання правосуб'єктності за ASIпотребує не стільки доведення, скільки законодавчого закріплення. Насправді, доказами є все те, що нас оточує та з'явиться у найближчому майбутньому, якщо не є достатнім самої правової презумпції.

ASI не повинен розглядатися в якості еквівалента фізичної особи так само, як ніколи не розглядалася подібним чиномй юридична особа (навіть випадку обрання форми приватного підприємства або господарського товариства з одним засновником або учасником), або держава як суверенна персона у якості еквівалента юридичної особи. ASI повинен стати самостійним правовим а́ктором.

Використана література:

1. Nick Bostrom. How long before superintelligence? Oxfrord Future of Humanity Institute. University of Oxford. Originally published in Int. Jour. of Future Studies, 1998, vol. 2 // URL: https://nickbostrom.com/superintelligence.html – Заголовок з екрану.
2. Баранов О.А. Інтернет речей (IoT): мета застосування та правові проблеми/ О.А. Баранов // Інформація і право: науковий журнал / редкол.: В.Г. Пилипчук та ін. – К.: Науково-дослідний інститут інформатики і права Національної академії правових наук України, 2018. – № 2 (25). – 164 с. – с. 31 – 45
3. Карчевский Н.В. Перспективные задачи уголовного права в контексте развития робототехники / Н.В. Карчевский // Соціальна функція кримінального права: проблеми наукового забезпечення, законотворення та правозастосування : матеріали міжнар. наук.-практ. конф., 12-13 жовт. 2016 р. / редкол.: В. Я. Тацій (голов. ред.), В. І. Борисов, (заст. голов. ред.) та ін. – Х. : Право, 2016. – 564 с. – с. 109 – 113
4. Карчевський М.В. Право роботів, або робот з правами / М.В. Карчевський // Наукова думка, 2017 // URL: http://ukrainepravo.com/scientific-thought/naukova-dumka/ pravo-robotiv-abo-robot-z-pravami/ – Заголовок з екрану.
5. Christoffer Hernæs. Artificial Intelligence, Legal Responsibility And Civil Rights / Christoffer Hernæs // Techcrunch, Aug 22, 2015 // URL: https://techcrunch.com/2015/ 08/22/artificial-intelligence-legal-responsibility-and-civil-rights/ – Заголовок з екрану.
6. Радутний О.Е. Місце штучного інтелекту в структурі суспільних відносин, які охороняються кримінальним правом/О.Е. Радутний // Фундаментальні проблеми кримінальної відповідальності: матеріали наук. полілогу,м. Харків,7вересня2018р./ [упоряд.: Ю.В. Баулін, Ю.А. Пономаренко].–Харків:Право, 2018. – 208 с.: іл. – с. 98 – 102
7. Радутний О. Суб'єктність штучного інтелекту у кримінальному праві / Юридичний журнал «Право України», 1/2018 – с.123 – 136
8. Радутний О.Е. Artificial Intelligence (штучний інтелект) як суб'єкт правовідносин в галузі кримінального права / О.Е. Радутний // Матеріали Міжнародної науково-практичної конференції «Політика в сфері боротьби зі злочинністю» з нагоди відзначення 25-річчя навчально-наукового юридичного інституту. – Івано-Франківськ, 2017. – 255 с. – с. 200 – 206
9. 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 – Заголовокзекрану.

10. Мисливий В.А. Кримінально-правова охорона кібернетичної безпеки в умовах глобалізації / В.А. Мисливий // Кримінально-правове забезпечення сталого розвитку України в умовах глобалізації : матеріали міжнар. наук.-практ. конф., 12-13 жовт. 2017 р. / редкол.: В.Я. Тацій (голов. ред.), В. І. Борисов, (заст. голов. ред.) та ін. – Х. : Право, 2017. – 560 с. – с. 122 – 126

11. Баранов О.А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах / О. Баранов // Юридична Україна. – 2018. – № 5-6. – С. 75–95

12. Кембриджська декларація про свідомість / Філософська думка, 2016, № 2, с. 78 – 80 // URL : http://journal.philosophy.ua/sites/default/files/library/files/-The%20Cambridge%20 Declaration %20on %20 Consciousness.pdf/ – Заголовок з екрану

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

Новицький А. М.,
д.ю.н., професор. Університет
Державної фіскальної служби України

ПЕРСПЕКТИВИ ФОРМУВАННЯ ПРАВОВОГО ЕЛЕМЕНТУ ІНТЕРНЕТ ВІДНОСИН

Впровадження Інтернет-відносин в усі сфери життєдіяльності людини неминуче призводить до переорієнтації не тільки поглядів на важливість та неминучість змін а і призводить до щоденної констатації фактів таких змін в житті кожної людини, як індивіда, як члена суспільства, як громадянина. Розвиток інформаційних відносин в Інтернет та за допомогою Інтернет стали потенційними двигунами сучасного динамічного прогресу людства. Інформація, як товар, та інформатизація відносин стала одними із основних джерел прибутку багатьох підприємців. Необхідно відмітити в цьому процесі провідну роль мережі Інтернет. Розвиток електронного бізнесу сприяє утвердженню нових суспільних відносин, що виникають у віртуальному світі мережі, встановлюють свої правила поведінки, свої кодекси честі. Разом з тим, частина суб'єктів підприємницької діяльності сприймають Інтернет переважно як один із засобів збільшення прибутків та реальний шлях до заволодіння часткою світового ринку збуту товарів і послуг, при цьому маючи реальну можливість обходу встановлених віками правил укладання міжнародних угод у торгівлі, наданні послуг, соціальних зобов'язаннях, сплаті податків тощо [1].

Комерціалізація відносин в Інтернет зумовила необхідність та фактичну можливість не тільки здійснювати певні домовленості, укладати угоди, давати гарантії чи здійснювати правочини, сьогоднішній розвиток техніки надає можливість формування особливих суспільних відносин, пов'язаних із практикою віддаленого керування окремими об'єктами, процесами чи процедурами.

З однієї сторони це значно спрощує життя, та забезпечує підвищений комфорт існування людини, як члена соціуму, з іншої – встановлює цілий ряд додаткових загроз.

Проаналізуємо окремі особливості інституційного забезпечення відносин в Інтернет, пов'язаних із підприємницькою діяльністю. Разом із розвитком

комерційних відносин розвиваються нові інститути інформаційного суспільства - електронний банкінг, електронні гроші, електронний бізнес, електронні аукціони. Розвиток зазначених специфічних інститутів притаманних інформаційному суспільству зумовлений і сформованими правилами поведінки, які виражені в нормативно-правових актах та фактично регулюють зазначені суспільні відносини. В той же час необхідно відзначити, що неможливо адекватно та завчасно визначати правила поведінки чи встановлювати особливості правового регулювання тих чи інших нових елементів комерціалізації суспільних відносин в Інтернет. Яскравим прикладом є економічно підтверджений ажіотаж навколо криптовалюти Bitcoin.

Проблема встановлення правового статусу криптовалюти, нарівні із традиційними платіжними елементами, не дали можливість у багатьох юрисдикціях світу адекватно, в правовому полі, відреагувати на нові економічні виклики Інтернету, як основного генератора криптовалюти, як окремого фінансового інституту. Досі існують як позитивні відгуки від вчених, юристів, фінансистів щодо майбутнього таких фінансових інструментів, але, в той же час, ми розуміємо і наявність ряду ризиків, які є непередбачувані в подальшому і можуть викликати значні економічні потрясіння в світі. Зокрема, ризики, що випливають із запровадження Bitcoin у фінансову систему держави. По-перше, криптовалюта Bitcoin не регулюються законодавством жодної із держав світу. Тобто, жодна із держав світу не бере на себе будь-які гарантії щодо забезпечення даної криптовалюти. По-друге, всі відносини пов’язані із обігом будуються виключно на довірі, відсутні системи страхування та гарантування збереження таких криптовалют. Відсутні механізми правового оскарження здійснення операцій, відміни операцій тощо. По-третє, відсутні механізми збереження та гарантій недоторканності електронних крипто гаманців суб’єктів зазначених фінансових операцій. По-четверте, залежність від технологічних та програмних аспектів. Наприклад втрата електронного гаджета, втрата паролю та доступу до електронного гаманця призведе до втрати всіх активів. По-п’яте, нерівність учасників у майнінгу криптовалют. Засновники, та перші особи, які почали дані емісійні процеси мають набагато конкурентніші позиції у порівнянні із іншими. Із часом майнінг одиниці криптовалюти стає все затратнішим, і це є економічно невигідним. По-шосте, повна анонімність щодо фінансових операцій із крипто валютою суперечить загальному принципу банківських відносин – знай свого клієнта, що дає можливість ідентифікувати кожного учасника фінансових відносин. По-сьоме, держава має можливості жодним чином впливати на фінансову стабільність даної валюти (підтримати курс, провести додаткову емісію, контролювати відсоток назавжди втрачених активів), що може стати причиною втрати державного фінансового суверенітету [2].

Особливістю сучасного розвитку правового регулювання інтернет-відносин стає і розуміння того, що все більше потенційно складних та затратних процесів комерціалізації відносин в Інтернет стають автоматично врегульованими

відповідними програмами та спрощують процедури прийняття рішень, здійснення правочинів, ведення комерційних відносин. В той же час виникають труднощі щодо встановлення суб'єктів зазначених правовідносин, адже однією із сторін, забезпечення здійснення відповідного правочину виступає не фізична особа, як суб'єкт, чи як уповноважена особа для здійснення правочину від імені юридичної особи, а саме програмний продукт, який вже може самостійно розвиватися, удосконалюватися та приймати відповідні рішення, які мають юридичну силу та відповідні юридичні наслідки.

Тому нам необхідно говорити про формування нових суб'єктів права – які не є живими істотами, не є членами соціуму в сучасному розумінні людства, проте вже в недалекому майбутньому досить сильно зможуть впливати не тільки на прийняття рішень, а й самостійно приймати рішення, бути нормативно визначеними суб'єктами правовідносин та здійснювати відповідні правочини.

Використана література:

1. Новицький А.М. Теоретичні аспекти правового регулювання електронного оподаткування. *Науковий вісник Національного університету ДПС України (економіка, право).* 2008. № 4 (20). С. 156-160.

2. Новицький А.М. Встановлення правового режиму криптовалюти як елемент фінансової безпеки держави. *Трансформація фінансових ринків в умовах глобальної нестабільності: реалії сьогодення та погляд у майбутнє: Збірник матеріалів Виїзного науково-практичного семінару (6-15 жовтня 2017 р.) та Міжнародної науково-практичної інтернет-конференції (30 жовтня 2017 р.) Університет ДФС України, ННІ фінансів, банківської справи, Кафедра фінансових ринків, ННІ права, Кафедра господарського права та процесу, Міжнародна академія інформатики, John cabot university in Roma, Universita degli studi di Padova, Universita degli studi di Perugia. – Ірпінь: Університет ДФС України,* 2017. 471 с.[335-339].

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

Брайчевський С. М.,
к.ф.-м.н., старший науковий співробітник

ПАРАМЕТРИЧНИЙ РЕЗОНАНС В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ ЯК ПРЕДМЕТ ПРАВОВОГО РЕГУЛЮВАННЯ

Швидкий розвиток сучасних інформаційних технологій породжує нові виклики і нові ризики, що потребують ретельного вивчення. До їх числа відносяться і специфічні проблеми правового регулювання, пов'язані з використанням Інтернету речей (далі - IoT) [1].

Правове регулювання в галузі використання технологічних (в тому числі інформаційних) систем саме по собі не є чимось новим. Але досі правові аспекти функціонування інформаційних систем не виходили за межі проблеми їх захисту від несанкціонованих дій людини. Тобто правове регулювання поширювалось на відносини між людьми, а машина виступала лише як знаряддя в руках людини. В ситуаціях, коли функціонування системи призводило до негативних наслідків,

вважалося, що відповідальність за її дії несуть розробники та експлуатаційники, тобто людина.

Але сьогодні (принаймні, теоретично) розглядаються ситуації, в яких відповідальність лягає саме на машину, незалежно від участі людини [2, 3]. Такий погляд на технологічні системи є принципово новим, оскільки передбачає можливість того, що їх функціонування може мати соціальні наслідки, а отже, вони самі можуть розглядатися як суб'єкти суспільних відносин. Фактично, сказане означає, що за певних умов технологічна система набуває елементи суб'єктності. На перший погляд, це суперечить загальноприйнятим уявленням про сутність технологічних систем. Адже вважається, що машина лише виконує програму, закладену в неї людиною. І разом з тим, розвиток сучасних інформаційних технологій, зокрема Інтернету речей, свідчить, що такі ситуації можливі. Якщо не вдаватися до наукової фантастики, то мова, очевидно, йде не про повноцінну суб'єктність машини, а про наявність в її функціонуванні окремих рис, характерних для справжнього суб'єкта – людини.

Вважаємо, що в рамках обраної нами теми ключовим чинником є здатність машини самостійно приймати рішення. Підкреслимо, що йдеться не про імітацію прийняття рішення, що, взагалі кажучи, на наш час не є чимось особливим (прикладом може служити комп'ютер, що грає в шахи). Ми маємо на увазі здатність машини приймати рішення, яке однозначно не визначається алгоритмом, обраними значеннями його параметрів та структурою вхідних даних. Саме така поведінка машини дає підстави говорити про її відповідальність за власні дії, що є предметом правового регулювання.

Нижче ми проаналізуємо одну з таких можливостей, зумовлену нелінійними ефектами в IoT-системах. А саме, можливість виникнення в них параметричного резонансу (в широкому розумінні).

Нагадаємо, що термін «Інтернет речей» на початку означав концепцію впровадження радіочастотних міток в систему керування логістичними ланцюжками [4, 5]. З часом під IoT почали розуміти концепцію обчислювальної мережі фізичних предметів ("речей"), оснащених вбудованими технологіями для їх взаємодії одне з одним або з оточуючим середовищем [6]. Головна ідея полягала в тому, що використання таких мереж дозволить (принаймні, частково) виключити участь людини. На наш час переважає розуміння IoT як сукупності технічних систем і комплексів, що взаємодіють між собою через мережу Інтернет [1, 3]. Вважається, що концепція IoT в практичній реалізації має як технологічні, так і соціальні наслідки [2].

Нижче ми проаналізуємо один із аспектів можливих реалізацій цієї концепції. А саме, внесок в роботу системи IoT нелінійних ефектів.

Коли ми говоримо про нелінійні ефекти, маємо на увазі те, що система IoT, взагалі кажучи, є нелінійною. Нагадаємо, що нелінійними називають динамічні системи (тобто системи, стан яких змінюється в часі), що математично описуються нелінійними рівняннями. Навпаки, лінійні системи – такі, що

описуються лінійними рівняннями [7]. Ми не будемо заглиблюватись в теорію нелінійних систем, обмежившись лише деякими загальними зауваженнями..

Строго кажучи, лінійних систем в природі не існує, тому що реальні процеси завжди описуються нелінійними рівняннями. Лінійна система – це свого роду абстракція, в якій лінійні рівняння дають результат, достатньо точний для практичних цілей. В більшості випадків ми маємо справу саме з такими системами. Суттєво нелінійні системи зустрічаються достатньо рідко. Але часто нелінійність системи за певних умов стає помітною в практичному плані. Тоді кажуть про нелінійні ефекти в такій системі.

Ми обмежимось одним з багатьох можливих явищ, пов'язаних з специфічною поведінкою навколишнього середовища системи IoT. А саме, з ним ми можемо зустрітись,якщо система містить в собі датчики, що відстежують зміни в часі деякого набору параметрів. Якщо значення параметрів періодично змінюються, в системі може виникнути т. з. параметричний резонанс [8]. В спрощеному викладі він полягає в збільшенні амплітуди коливань в системі, пов'язаних з коливаннями параметрів середовища. Під коливаннями системи ми розуміємо періодичну зміну її внутрішнього стану. Така зміна можебути пов'язана, наприклад, з періодичним завантаженням додаткових даних від групи датчиків, які уточнюють дані про стан зовнішнього середовища.

Для ілюстрації сказаного наведемо умовний приклад. Нехай програмний комплекс обов'язково виконує цикли, обходячи чергові набори вхідних даних. Отже, маємо періодичний процес з заданою частотою. В звичайній автоматичній системі ця частота відома і має дуже малу величину. Тому ця обставина не впливає на її роботу. Але в системах IoT обмін даними здійснюється через мережу Інтернет, а отже може мати помітну величину, яка, до того ж, не є сталою.

Припустімо, що в ході цього процесу визначається швидкість зміни деякого параметра оточуючого середовища, який також періодично змінюється.Кожний раз, коли система фіксує достатню швидкість зміни, лічильник збільшується або зменшується залежно від напрямку зміни параметра. Тоді у випадку співпадіння частот лічильник буде необмежено зростати. В результаті стає можливим хибне спрацьовування системи з непередбачуваними наслідками.

Таким чином, суто технологічні властивості системи IoT можуть зумовити такі її дії, що значною мірою моделюють власну поведінку. Ця поведінка не випливає з алгоритму разом з наявними значеннями показів датчиків, Тому, враховуючи можливі негативні для суспільства наслідки, вона може сприйматися як суб'єкт соціальних відносин і підлягати правовому регулюванню. Наприклад, у випадку явної загрози для суспільства, така система може бути демонтована за рішенням суду.

Використана література:

1. Баранов А.А. Интернет вещей и искусственный интеллект: истоки проблемы правового регулирования - ІТ-право: проблеми та перспективи розвитку в Україні:

збірник матеріалів ІІ-ї Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.). – Львів : НУ «Львівська політехніка», 2017. – 318 с. (С. 18-42).

2. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений - Структура и функциональные модели архитектуры. Обзор Интернета вещей. URL: http://handle.itu.int/11.1002/1000/11559

3. Баранов О.А. «Інтернет речей» як правовий термін. Юридична Україна. – 2016. – № 5-6. – С. 96-103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe ?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf

4. Леонид Черняк. Платформа Интернета вещей (рус.). Открытые системы. СУБД, №7, 2012. Открытые системы. URL: https://www.osp.ru/os/2012/07/13017643/

5. Kevin Ashton. That ‘Internet of Things’ Thing. In the real world, things matter more than ideas. (англ.). RFID Journal (22 June 2009) http://www.rfidjournal.com/ articles/view?4986

6. Internet Of Things (англ.). Gartner IT glossary. Gartner (5 May 2012). — «The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment». URL: https://www.gartner.com/it-glossary/internet-of-things/

7. Боулдинг К. Общая теория систем — скелет науки. — М.: Наука, 1969.

8. К. Магнус. Колебания: Введение в исследование колебательных систем. 1982. Москва. Мир. 304 с.

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

Барікова А. А.,
аспірант юридичного факультету
Київського національного університету
імені Тараса Шевченка

СИНЕРГЕТИЧНА ПАРАДИГМА ПРОЦЕДУРИ СИСТЕМАТИЗАЦІЇ ПРАВА ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Інтенсифікація процесу цифровізації всіх сфер життєдіяльності обумовлює потребу в запровадженні відповідних регулятивних рамок для діяльності на ринку електронних комунікацій як функціональному інфраструктурному комплексі національної інноваційної економіки. У результаті імплементації норм систематизованого в такий спосіб права електронних комунікацій стає можливою реалізація принципу «good governance» у діяльності національного регулятивного органу в частині реалізації дозвільних процедур і ліцензування при здійсненні діяльності на ринку електронних комунікацій, притягненні до адміністративної відповідальності за правопорушення, вчинені у сфері електронних комунікацій.

По суті, у цьому плані можна вести мову про динамічну природу процедури систематизації права електронних комунікацій з урахуванням взятих на себе Україною зобов’язань перед Європейським Союзом щодо гармонізації вказаної

галузі національного права відповідно до норм наднаціонального права електронних комунікацій. Відповідно, як вказує С. Стеценко, йдеться про нормотворчу адміністративну процедуру неюрисдикційного характеру [1, с. 266–267]. У цьому сенсі процедура систематизації права електронних комунікацій пов'язана зі встановленням порядку реалізації виконавчо-розпорядчої діяльності суб'єктів публічної адміністрації в частині інституціоналізації (розробки і прийняття) та імплементації норм позитивного матеріального права (права електронних комунікацій).

При цьому функціональний вимір процедури систематизації права електронних комунікацій може бути повною мірою реалізований у межах синергетичної парадигми. Синергетична методологія має значний потенціал у такому юридичному дослідженні при встановленні механізмів і закономірностей самоорганізації в умовах саморуху правової матерії [2, с. 40; 3, с. 166]. На цей процес вливають такі фактори, як випадкові значні події для розвитку ринку електронних комунікацій, параметр порядку в національній правовій системі, узгодження мікрокосму та макрокосму в праві електронних комунікацій. Відповідно, у синергетичному ракурсі процедура систематизації права електронних комунікацій визначає самоорганізований та дисипативний характер його системи, для якої притаманні активний метаболізм, інтенсивні взаємодії її складових, поєднання позитивних і негативних зворотних відношень, зв'язок мінливості, спадковості та відбору, чергування атракторів і гомеостазів [4, с. 56].

Звідси причинами застосування синергетичної методології при консолідації норм права електронних комунікацій є нестабільний характер, еволюція та коеволюція відносин на ринку електронних комунікацій. Відтак, форми процедури систематизації права електронних комунікацій охоплюють самочинний перехід системи відносин на ринку електронних комунікацій в новий стан і самоорганізацію, накопичення (зокрема, лавиноподібне) постійних змін (флуктуацій), фазові переходи на шляху до досягнення стану рівноваги (точки біфуркації) з урахуванням як детермінованості процедури систематизації українського права в частині його гармонізації з наднаціональним правом електронних комунікацій, так і свідомого вибору для імплементації положень вторинного права Європейського Союзу, кореспондуючих національним правовим традиціям.

Потрібно зауважити, що чинна сфера консолідації норм права електронних комунікацій має недостатньо впорядкований вимір. У контексті зазначеного переліку законотворчих ініціатив у сфері систематизації права електронних комунікацій потрібно вказати, що такий стан справ відзначається динамічними рисами. Тому при реалізації процедури систематизації права електронних комунікацій нелінійна реакція на вплив такого динамічного фактора, на переконання І. Пригожого, дозволяє встановити самозародження суворо упорядкованих структур [5, с. 49–50]. Принагідно для синергії зусиль суб'єктів публічної влади як учасників національної, регіональних і відомчих процедур

систематизації права електронних комунікацій окрему увагу при консолідації юридичних норм потрібно приділяти таким інститутам права електронних комунікацій:

– забезпеченню технологічної нейтральності [6], доступу на ринок електронних комунікацій, зокрема наданню генеральних (загальних) дозволів, а також запровадженню повідомного принципу для здійснення діяльності на ринку електронних комунікацій [7, с. 33, 310–311] згідно з приписами ст. 7 Закону України «Про ліцензування видів господарської діяльності» [8];

– лібералізації державного контролю та нагляду в частині спостереження за підконтрольними об'єктами, інформування про факти відхилень від правомірного функціонування та запобігання вчиненню правопорушень [9, с. 538] на підставі ч.ч. 3, 4, 6 ст. 3 Директиви 2002/21/ЄС [10], п. 19 преамбули Директиви 2009/140/ЄС [6], ст. 2 Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» [11];

– порядку притягнення до адміністративної відповідальності за правопорушення, вчинені у сфері електронних комунікацій, із урахуванням вимог п. 12 преамбули Директиви 2002/20/ЄС щодо застосування критеріїв об'єктивної обґрунтованості, пропорційності та співмірності національного обмеження прав задля досягнення загального інтересу [12], п. 69 Директиви № 2009/136/ЄК стосовно компетенційних і ресурсних стимулів [13] насамперед щодо бланкетних норм про адміністративну відповідальність [14, с. 171–172] задля забезпечення законності та дисципліни, досягнення превентивного, карного та стимулюючого значення санкцій [15, с. 15]; їх відповідності, ефективності, пропорційності, переконливості (ст. 21а Директиви № 2009/140/ЄС [6]), можливості застосування в період будь-якого делікту, у тому числі для виправлених порушень (ст. 15а Директиви № 2009/136/ЄК [13]).

Отже, процедура систематизації постає як послідовно здійснюваний порядок консолідації норм права електронних комунікацій на підставі прийнятого рішення щодо інтеграції національного та транскордонного ринків електронних комунікацій. Така процедура має нелінійний неюрисдикційний характер, зорієнтована на регламентацію позитивних відносин.

Використана література:

1. Стеценко С.Г. Адміністративне право України : навч. посіб. / С.Г. Стеценко. – Київ: Атіка, 2007. – 624 с.

2. Туманов Г.А. Организация как функция государственного управления / Г.А. Туманов // Советское государство и право. – 1986. – № 1. – С. 40–41.

3. Честнов И.Л. Правопонимание в эпоху постмодерна / И.Л. Честнов. – СПб. : Изд-во С.-Петербург. ун-та, 2002. – 272 с.

4. Тарасевич В.М. Экономическая синергетика: концептуальные аспекты / В.М. Тарасевич // Економіка і прогнозування. – 2002. – № 4. – С. 56–71.

5. Пригожий И. Философия нестабильности / И. Пригожий // Вопросы философии. – 1991. – № 6. – С. 46–57.

6. Directive 2009/140/EC of the European Parliament and of the Council of 11/25/2009 Amending Directives 2002/21/EC on a Common Regulatory Framework for Electronic

Communications Networks and Services, 2002/19/EC on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities, and 2002/20/EC on the Authorisation of Electronic Communications Networks and Services // Official Journal of the European Communities. – 2009. – L 337. – Vol. 52. – Pp.37–69.

7. Баранов О.А. Правове регулювання доступу на ринок телекомунікацій / О.А. Баранов // Інформація і право. – 2011. – № 2(2). – С. 32–38.

8. Про ліцензування видів господарської діяльності : Закон України від 02.03.2015 р. № 222-VIII : із зм. і доп. станом на 28.09.2017 р. // Відомості Верховної Ради України. – 2015. – № 23. – Ст. 158.

9. Заярний О.А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія / О.А. Заярний. – Київ: ВД «Гельветика», 2017. – 700 с.

10. Directive 2002/21/EC of the European Parliament and of the Council of 03/07/2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive) // Official Journal of the European Communities. – 2002. – L 108. – Vol. 45. – Pp. 33–50.

11. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 05.04.2007 р. № 877-V : із зм. і доп. станом на 04.04.2018 р. // Відомості Верховної Ради України. – 2007. – № 29. – Ст. 389.

12. Directive 2002/20/EC of the European Parliament and of the Council of 03/07/2002 on the Authorisation of Electronic Communications Networks and Services (Authorisation Directive) // Official Journal of the European Communities. – 2002. – L 108. – Vol. 45. – Pp. 21–32.

13. Directive 2009/136/EC of the European Parliament and of the Council of 11/25/2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and The Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws // Official Journal of the European Communities. – 2009. – L 337. – Vol. 52. – Pp. 11–36.

14. Заярний О.А. Правові та організаційні основи удосконалення матеріального адміністративно-деліктного законодавства в інформаційній сфері на шляху євроінтеграції / О.А. Заярний // Адміністративне право і процес. – 2014. – № 3(9). – С. 169–185.

15. Коломоєць Т.О. Адміністративний примус у публічному праві України: теорія, досвід та практика реалізації : автореф. дис. … д-ра юрид. наук : 12.00.07 / Т.О. Коломоєць ; Національний університет внутрішніх справ. – Харків, 2005. – 43 с.

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

Фещенко К. С.,
студент ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Фурашев В. М.,
к.т.н., доцент, с.н.с.

ТРЕНДИ XXI СТОЛІТТЯ: ІНТЕРНЕТ РЕЧЕЙ

«Інтернет речей» - майбутнє інформаційного суспільства. Сучасне життя супроводжується невпинним розвитком інформаційно-комунікаційних технологій, кожного дня науковці-винахідники презентують для світу нові унікальні речі, які

удосконалюють та полегшують наше повсякденне життя. Це не дивно, адже XXI сторіччя стало сторіччям якісних технологічних зсувів та значних наукових проривів. Він перетворює буденні для нас речі в нові, розумні технології, під'єднуючи їх до мережі та наділяючи новими функціями. Дана технологія надає пристроям самостійне функціонування. Важко уявити, що мобільні телефони сучасного зразка з'явилися всього лише декілька десятків років назад.

Сьогодні нормальною вважається ситуація, за якої традиційне телебачення, преса та радіо поступаються популярністю глобальній мережі Інтернет. Адже саме Інтернет виступає рушійною силою розвитку багатьох передових технологій. Однією з таких є «Інтернет речей». Що ж являє собою словосполучення "інтернет речей"? Проводячи відповідні опитування, виявилося що 80% викладачів та 60% студентів не мали уявлення, що це за дивна річ, про яку, на їх думку, вони ніколи не чули.

Інтернет речей (Internet of Things) - це певна сукупність пристроїв, в яких вбудовані датчики, які зчитують певну інформацію через дротові та бездротові мережі [1]. Вперше даний термін був введений в науковий обіг у кінці 90-х рр. відомим британським вченим Кевіном Ештоном, крім того, саме «Інтернет речей» вчені пов'язують з четвертою промисловою революцією. Технології, які дозволяють реалізувати Інтернет речей, вирішують чотири основні задачі: ідентифікацію, збирання даних, зберігання даних та обмін інформацією [2]. На сьогодні загальновідомими стали такі девайси як smart house, fitness tracker, petcube, smart watch, саме ці речі є тими пристроями, які будують мережу Інтернету речей, і покликані вдосконалювати та покращувати якість нашого повсякденного життя. Кількість таких винаходів у світі невпинно зростає, науковці-дослідники намагаються впроваджувати новинки у всі сфери суспільного життя, починаючи з повсякденного харчування і завершуючи управлінням снами, мотивацією та екологічним станом навколишнього середовища. Можемо уявити, як працює мережа «інтернету речей»: пристрої, що пов'язані між собою обробляють, аналізують, чи обмінюються інформацією, яка на основі зробленої роботи дає змогу прийняти самостійні рішення.

Отже, переваги «Інтернету речей» полягають в наступному:

– по-перше, це простота використання, не потрібно бути комп'ютерним генієм, щоб вміти користуватися такого роду девайсами, крім того ці речі полегшують життя для людей з обмеженими можливостями, для людей літнього віку, і взагалі для всіх тих, хто бажає спростити та покращити своє життя, економлячи при цьому власний час;

– по-друге, Інтернет речей надає можливісті керувати пристроями на відстані (якщо це бездротова мережа);

– по-третє, Інтернет речей дає можливість для появи ефективніших методів виробництва та ведення бізнесу.

Проте важливо зазначити і негативні сторони швидкого розвитку Інтернету речей. Кожна з таких «розумних» речей, які і формують Інтернет речей, має

датчики зчитування інформації, які підключено до Інтернету, а отже кожна людина, яка використовує дані девайси може позбаватися недоторканості свого приватного життя. Крім того, не варто залишати поза увагою і вартість даних девайсів, за сучасної економічної ситуації в світі і в Україні, зокрема, такі пристрої не по кишені більшості населення. Комп'ютеризовані речі роблять наше життя простішим, в будь-якій сфері використання. Овертон довів, що людей можна привчити до всього, посилаючись на його дослід треба пройти лише декілька етапів: від заперечення до легалізації/впровадження.[3]

На сьогоднішній день в Україні активно впроваджується проект, що має назву «Єднання поколінь на користь громад». Ідея проекту полягає у допомозі літнім людям та людям з обмеженими можливостями брати участь у суспільному житті міста, чи користуватися перевагами smart city.

На вище сказаному прикладі, ця теорія дійсно працює. Якби не намагалися бабусі сперечалися зі своїми онуками що до розумної техніки, говорячи, що їхнє дитинство повинне промайнути на дитячому майданчику чи в бібліотеці, а не за цим залізним монстром. Та все ж переглягають сторінки погодою чи новинами в мережі інтернету, бо це є частиною нашого життя.

Використана література:

1. http://nv.ua/ukr/science/lectures/lektorij-shcho-take-internet-rechej-i -navishcho-vin-potriben-1326653.html.

2. Геселева Н. В. Інтернет речей як складова четвертої промислової революції [Електронний ресурс] / Н. В. Геселева – URL: http://www.m.nayka.com.ua/?op=1&j=efektyvna-ekonomika&s=ua&z=5315.

3. Д. П. Овертон. Вікно Овертона: технологія знищення, або Як легалізувати що завгодно URL: https://www.ar25.org/article/vikno-overtona-tehnologiya-znyshchenn ya-abo-yak-legalizuvaty-shcho-zavgodno.html.

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

Круц А. О.,
студент ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Фурашев В. М.,
к.т.н., доцент, с.н.с.

«ІНТЕРНЕТ РЕЧЕЙ». ДОПОМОГА ЧИ ЗАГРОЗА?!

«Інтернет речей» являється однією з прогресуючих технологій. Це мережа, в якій можуть взаємодіяти між собою усі прилади, якими ми користуємося. Впровадження «Інтернету речей» слід розглядати як реальне формування фундаментальних основ кіберцивілізації.[2, 39] За допомогою обміну даними речі «спілкуються» один з одним.

«Інтернет речей» надає звичайним користувачам абсолютно новий рівень комфорту, тим самим викликаючи величезні зміни у повсякденному житті. І тут ми повертаємо увагу на проблему безпеки. Елементи такої системи мають бути

захищеними, тому що замість користі вони можуть принести величезну шкоду. Тобто злочинці можуть отримати доступ до інформації про хазяїна, яка і зберігається в речах із вбудованими комп'ютерами. Відсутність на даний час стандартів для захисту таких мереж трохи сповільнює впровадження інтернету речей у повсякденне життя.[1] Це одне із найважливіших питань, що повинно турбувати нас стосовно прагнення використання цієї концепції.

Концепція інтернету речей дуже широка. Немає чіткого списку приладів, для яких можна застосувати цей підхід. Це можуть бути як побутові прилади, так і гаджети, котрі можна носити. Також до інтернету речей відносять автомобілі та інший транспорт з системою автопілоту – такі, що можуть їздити без водія.

Тепер уявіть собі, що це все може бути налаштовано проти вас самих. В один день все може вийти з ладу і цим нанести велику шкоду вам і оточуючим. Комп'ютер, якого ми вважаємо за товариша, може обернутися нам ворогом.

Сучасний науково-технічний прогрес є невід ємною складовою еволюційного розвитку світу.[2, 40] Тому прогресування програм як зброї – неминуче. З часом програм, які захищають нас від цього, стає все більше, але небезпечні програми теж могутнішають. У розвитку програми як зброя стоять на ступінь вище. У зв'язку з цим, виникає необхідність на об'єктивних засадах передбачати приблизний сценарій майбутніх подій для формування раціональної та меньш помилкової стратегії.[3, 99]

В наш час розв'язати програмну війну дуже легко. Рівень захищеності нашого інформаційного світу дуже низький. І загроза може бути не тільки комфортним умовам, але і нашому життю.

Ми постійно опираємось на розвиток стратегій подолання загроз, але не замислюємося про їх утилізацію. А це може стати наступною сходинкою на шляху до успіху.

Використана література:

1. Владимир Парамонов. Інтернет речей. [Електронний ресурс] /Парамонов В.// «Розумна» електроніка. – URL: https://www.turkaramamotoru.com/uk/Інтернет-речей-20010.html

2. Матеріали науково-практичної конференції. Інтернет речей: проблеми правового регулювання та впровадження / МНПК // Інтернет речей: проблеми правового регулювання та впровадження. – 2017. – 237 с.

3. Згуровський М.З. Тернистий шлях до відродження / М.З. Згуровський. – Київ: Генеза, 2010. – 368 с.

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

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

ЕТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ: МІЖНАРОДНО-ПРАВОВІ ЗАСАДИ

Спектр питань щодо визначення етичних аспектів впровадження і використання інформаційно-комунікаційних технологій формується вже протягом кількох десятиліть.

Світовий Саміт з інформаційного суспільства, який серед багатьох інших питань, заклав засади етичних аспектів використання інформаційно-комунікаційних технологій (ІКТ) у Женевському плані дій 2003 р. [1], визначив також, у 2014 р. [2], і подальші їх перспективи на період після 2015 р.

Посприяла цьому і цілеспрямована діяльність Організації Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО), де у рамках її Програми «Інформація для усіх» було запропоновано Кодекс етики для інформаційного суспільства.

Сьогодні можемо говорити, про основні напрями розвитку етичних аспектів використання ІКТ, у тому числі і технологій Інтернету речей, які світове співтовариство вважає принциповими і першочерговими. Задля цього, пропонується виходити з наступних позицій:

a) ІКТ у цілому варто визнати у якості однієї із суспільних послуг, що відіграє ключову роль для розвитку інформаційного суспільства і має важливе значення для сприяння здійсненню прав і основних свобод;

b) забезпечення прав людини і основних свобод;

c) забезпечення усіх заходів задля зміцнення миру і відстоювання таких цінностей, як свобода, рівність, солідарність, терпимість, колективна відповідальність і турботливе відношення до природи;

d) визнання того факту, що усі зацікавлені сторони повинні:

враховувати *етичний аспект* при використанні ІКТ;

постійно підвищувати рівень обізнаності і сприяти обговоренню на національному, регіональному і міжнародному рівнях *етичних можливостей* і проблем, пов'язаних з використанням ІКТ;

сприяти повазі основних *етичних цінностей* при використанні ІКТ і попередженні зловживань при їх використанні;

e) залучати зацікавлені сторони до продовження досліджень етичних аспектів ІКТ, аналізувати їх поточні і перспективні проблеми і можливості;

f) постійно підвищувати рівень захисту конфіденційності і персональних даних.

При цьому вважається, що інформаційне суспільство повинно спиратись на:

(a) загальновизнані цінності;

(b) турбуватись про спільне благо та

(c) попереджувати зловживання при використанні ІКТ.

Варто звернути увагу на головні позиції в контексті нашої теми – етичних аспектів впровадження і використання технологій Інтернету речей, а саме:

заходи для розвитку Інтернету і інших ІКТ –

передбачається, що вони забезпечуватимуть безпеку, надійність і стабільність критично важливих і повсюдно поширюваних прикладних технологій і послуг, задля цього держави і зацікавлені сторони вживатимуть заходів задля розвитку надійного Інтернету та інших ІКТ, що забезпечують безпеку, надійність і стабільність критично важливих та повсюдно поширюваних прикладних технологій і послуг;

технологічні і методологічні стандарти і рішення –

передбачається, що технологічні і методологічні стандарти і рішення щодо доступу, операційної сумісності повинні забезпечити якомога більш широкий доступ до контенту і його виробництву та сприяти еволюції і вдосконалені Інтернету і інших ІКТ в цілях більшої інклюзивності і подолання усіх форм дискримінації; при цьому, основні технічні стандарти, що використовуються в Інтернеті і інших ІКТ, повинні мати відкритий характер для забезпечення операційної сумісності і можливості впровадженн інновацій;

Інтернет і інші ІКТ повинні використовуватись для скорочення цифрового розриву, а також для впровадження технологій і прикладних розробок;

активна соціальна участь у суспільному житті шляхом використання Інтернету і інших ІКТ повинна забезпечуватись на недискримінаційній основі – цьому сприятиме прийнятний за ціною доступ до Інтернету; при цьому такий доступ повинен бути забезпечений для усіх мовних, культурних, соціальних груп, чоловіків і жінок, включаючи людей з фізичними, сенсорними та когнітивними недоліками, а також людей, що говорять мовами меншин.

Зрозуміло, що у цих умовах виправданими будуть кроки щодо спільної роботи, спрямованої на попередження зловмисного використання ІКТ шляхом поєднання законодавчих заходів, освітніх заходів з подолання медійної і інформаційної некомпетентності, технічних заходів і превентивних заходів щодо самостійного і спільного регулювання безпеки в Інтернеті.

Окремо світове співтовариство визначає питання щодо підтримки використання ІКТ для підвищення ефективності демократії і демократичних інститутів і покладає на держави відповідальність за забезпечення інклюзивного, сучасного і правового середовища для розвитку інформаційного суспільства.

Використана література:

1. Світовий саміт з інформаційного суспільства. План дій 2003 р. [Електронний ресурс]. – Режим доступу: http://ict.az/en/content/216.

2. WSIS + 10 Statement on implementation of WSIS Outcomes and the WSIS + 10 Vision for WSIS Beyond 2015. [Електронний ресурс]. – Режим доступу: http://www.itu.int /net/wsis/documents/HLE.html.

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

Головко О. М.,
к.ю.н., старший. викладачка кафедри публічного права КПІ імені Ігоря Сікорського

СЕКС-ФУТУРОЛОГІЯ: ІНТЕРНЕТ РЕЧЕЙ У ДІЇ

Інтернет речей (далі – IoT) ввірвався у наше життя досить стрімко. Він зачепив багато сфер життя людини, навіть самих інтимних. Не оминув цей процес й сферу надання секс-послуг. Ким, запитаєте ви? Звичайно ж, роботами. Наразі вже існує ряд пристроїв, які можуть задовольняти сексуальні потреби людини, синхронізуючись не тільки з ПК, але й з будь-яким гаджетом. Більше того, вже не є футурологічною вигадкою реальний секс на відстані. Це стає деталі реалістичніше за рахунок синхронізації парних пристроїв для задоволення сексуальних потреб або через можливість передачі управління цими пристроями на відстані (наразі використовується через передачу іншій особі автоматично згенерованого електронного посилання). В якомусь сенсі це крок до появи «транскордонного сексу».

Враховуючи специфічність теми та її інтимний характер в зарубіжній пресі це питання висвітлюється досить обережно. Втім, це відбувається в таких виданнях як «The New York Times», «The Guardian», «The Chicago Tribune». Більше того, вже проводяться конференції саме з цієї тематики. Найбільш відома з них - Def Con hackers' conference в Лас-Вегасі, яка включала секцію під назвою "Hacking the Vibrating Internet of Things". Більше того, в світі періодично відбуваються хакатони з подібної тематики [1].

Однак, показовим є той факт, що ці науково-практичні заходи мають суто технічну складову, в той час як правові аспекти залишаються поза увагою. Особливо, враховуючи той факт, що на вищезазначених заходах обговорюються випадки поширення хакерства секс-девайсів, що зачіпає питання порушення прав людини, посягання на честь та гідність особи, її статеву свободу тощо. Тож важливо усвідомити, що дане питання охоплює проблему правого регулювання, навіть відносин кримінально-правового характеру, адже визначивши в чинному Кримінальному кодексі України такі родові об'єкти як статева свобода та статева недоторканість особи держава взяла на себе обов'язок захищати їх від усілякого роду посягань.

Можливо, наше суспільство ще не готове до обговорення цих аспектів існування IoT, однак у світі вже відомі практики подання позовів на виробників секс-девайсів, які синхронізуються з технічними пристроями та можуть бути під'єднані до мережі Інтернет. Так, у 2016 році Standard Innovation (відома як виробник секс-девайсів із можливістю приєднання до мережі Інтернет) довелося заплатити позивачам 3,75 мільйонів доларів США після того, як стало зрозуміло, що їх вібратор We-Vibe збирає дані про кількість та режим використання, а також відправляти дані про параметри температури та вібрації [2]. Враховуючи

можливість замовлення майже будь-яких подібних приладів як для чоловіків, так і для жінок через мережу Інтернет – висока ймовірність появи нової загрози сучасності не тільки «десь за океаном», але й в Україні. Як мінімум, є три напрямки, які потребують дослідження в цій сфері: забезпечення приватності, гарантія захисту від зламу та персоналізація.

Приймаємо ми цю тему в науковій спільноті чи ні – питання часу. А поки очікуємо поширення світової практики в питаннях регулювання правовідносин, що виникають з причин несанкціонованого втручання в роботу девайсів, котрі представляють IoT концепцію.

Використана література:

1. How Internet-connected sex toys make it clear that we need to worry about the Internet of Things URL: https://hackernoon.com/how-internet-connected-sex-toys-makes-it-clear-that-we-need-to-worry-about-the-internet-of-things-525c2156e4e2.

2. Maker of 'Smart' Vibrators Settles Data Collection Lawsuit for $3.75 Million URL: https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html

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

Яременко О. І.,
к.н. держ. упр., доцент, завідувач кафедри правових наук та філософії Вінницького державного педагогічного університету

ФІЛОСОФСЬКО – ПРАВОВІ ЗАСАДИ ФЕНОМЕНУ ВІРТУАЛЬНО – ЦИФРОВОЇ РЕАЛЬНОСТІ

Високі темпи розвитку інформаційних комп'ютерних технологій інституювали електронні форми соціальної взаємодії, створили умови для міграції суспільних відносин в цифровий простір, надали широкі можливості відображення матеріальних явищ світу у віртуальному форматі, що актуалізує наукові дослідження в цій царині.

Результати аналізу наукових публікацій свідчать про наявність високого інтересу до проблематики віртуальної реальності. Філософськіїї аспекти, дослідження впливу на діяльність людини та функціонування соціуму здійснено в наукових доробках Ф. Бікоки, Д. Бласковича, Е. Кастельса, Д. Лоуміса, П. Луненфельда, Г. Рейнголда, Д. Шеєра та інших.

Правові проблеми віртуалізації суспільних відносин проаналізовано в працях І. Арістової, О. Баранова, К. Бєлякова, В. Брижка, О. Довганя, Д. Дубова, О. Золотар, Б. Кормича, О. Кохановської, О. Марущака, В. Пилипчука, В. Фурашева та інших.

Характерною рисою наукових досліджень в цій царині є поліваріантність трактувань віртуальної реальності та її взаємозв'язку з правовою дійсністю. Відповідно ця тематика потребує подальшого наукового аналізу.

Метою даної статті є аналіз філософських основ феномену віртуально – цифрової реальності та проблеми їх інституалізації правовими засобами.

Започаткування теоретичних розробок в сфері віртуальної реальності було здійснено в середини 60 – х років 20-го ст., коли І.Сазерленд, досліджуючи роль нових інформаційних технологій, відзначив, що дисплей, підключений до цифрового комп'ютера, дає можливість сприймати поняття, які неможливо відтворити в фізичному світі. Об'єкти, що відображаються комп'ютером, не відповідають традиційним ознакам, характерним для фізичної реальності і, в майбутньому, за його допомогою можна буде контролювати існування матерії [1,с. 507].

Однією із характерних рис віртуальної реальності є прояв у формі симуляції матеріальної картини світу, що обумовило філософсько - теоретичні дискусії щодо руйнування традиційних уявлень про матеріальність та ідеальність. Як зазначає П. Луненфельд, взаємозв’язок реального та ідеального є однією із найдавніших проблем в історії філософії. Реальність завжди розглядалася як така, що існує незалежно від перипетій чуттєвого досвіду, а ідеальність – як те, що існує в свідомості людини в якості ідеальної моделі. Нове середовище, під назвою «віртуальна реальність», що створене в науково-технічних лабораторіях, викликало інтенсивні дебати в гуманітарних науках на предмет того, що ж насправді є реальним [2, с. 6].

А. Кутирьов з цього приводу зазначає, що рішучий перелом у трактуванні буття і зміні відносин ідеалізму та науки настав тоді, коли люди зіткнулися з середовищем, яке є неадекватним матеріальності, в результаті чого пізнання стало невидимим, невідчутним, поза просторово - часовими параметрами, швидкостями і ритмами живого. Застосування електрики і магнітних полів, теорія відносності, розщеплення атома, винахід комп'ютерів зробили оточенням людини те, що в класичну епоху вважалося нематеріальним. Головним рубежем в "зраді" науки матеріальності і переорієнтації на ідеальне, він вважає інформаційну революцію, що призвела до появи безпредметного, знакового, екраномічного штучного середовища [3, с. 21].

В той же час, Д. Люміс не бачить жодних проблем для розвитку людства у зв’язку із процесами віртуалізації. Він приходить до цілком логічного висновку про те, що перцептивний світ, створений нашими почуттями та нервовою системою, є настільки функціональним, що повністю відображає фізичний світ і більшість людей сприймає його в реальному житті, навіть не задумуючись, що такий контакт з ним є опосередкованим [4, с. 115**].**

М. Клінв 2005 році зазначав, що віртуальна реальність буде інтегрована у повсякденне життя людини та її діяльність, а технології віртуальності активно впливатимуть на поведінку людини, між особистісне спілкування та процеси пізнання. Поступова міграція діяльності у віртуальний простір призведе до важливих змін в економіці, світогляді та культурі, засобах масової інформації, маркетингу, охороні здоров'я, сфері нерухомість тощо. Віртуальне середовище

сприятиме розширенню основних прав людини,розвитку свободи і добробуту, соціальній стабільності[5, с. 115]

В сучасних умовах процеси віртуалізації знаходить свій прояв в двох взаємопов'язаних практичних площинах – в технологічному та інформаційно-комунікативному. Спектр використання віртуальних технологій надзвичайно широкий – від створення віртуальних офісів компаній до складних методів проектування виробничих процесів чи візуалізації тривимірних зображень об'єктів для споживачів продукції та послуг.

Віртуальну реальність в аспекті соціального інформаційно-комунікаційного середовища доречно кваліфікувати як віртуально-цифровий простір. Це транскордонне інфраструктурно-цифрове середовище, утворене надскладною динамічною системою з'єднаних стаціонарних та мобільних електронних пристроїв, в якому здійснюються інформаційні процеси та комунікації, відбувається виконання робіт та надання послуг в межах технічних можливостей, регулятивних норм та воле виявлення суб'єктів. Виходячи з високого рівня абстрактності цього поняття, необхідною методологічною основою є аналіз її складових, серед яких можна виділити забезпечувальні, організаційно - функціональні, інформаційні, комунікаційні та регулятивні.

В юридичній науці має місце дискусія щодо взаємозалежності права та віртуальної реальності. Так, О. Дзьобань зазначає, що у праві, як соціальній сфері, діє логіка віртуальності. Віртуальний простір права утворюється через інформаційно-комунікативну активність суб'єктів правовідносин, кожен з яких являє свою симулятивну реальність правової ситуації. Кінцева кількість можливих світів (тобто уявних варіантів скоєння злочину, ступеня провини злочинця, фактів справи і їх доведеності, винесення справедливого вердикту) взаємодіють і систематизуються у динамічному неоднозначному синергетичному полі права [6, с. 11**]**.

О. Баранов натомість вважає що у філософському сенсі немає підстав вважати реальність та віртуальність еквівалентними поняттями, а значить немає підстав вважати, що якісь суспільні відносини можуть самостійно та автономно реалізовуватися у віртуальній реальності [7, с. 213**]**.

В той же час, К. Беляков підкреслює, що віртуальність є тотальною ознакою соціальної реальності і стосується практично всіх елементів суспільства: економіки, політики, науки, мистецтва, сім'ї, сексуальних стосунків. На його думку, створене інформаційно-комунікаційними технологіями «віртуальне» середовище, є не якоюсь альтернативою, а невід'ємною частиною реального світу, що знайшло свій вираз у концепції «реальної віртуальності», комунікація та взаємодія в рамках якої впливає на життя суспільства та держави. З позицій інформаційного права науковцем запропоновано поняття віртуально - інформаційних правових відносин як взаємних відносин двох чи більше осіб із приводу майнових благ, що породжуються обставинами виникнення та існування в інформаційно-технологічному просторі, як результат комунікації та обміну

даними в електронно-цифровій формі, що визначається наднаціональними ознаками на засадах юридичної рівності та автономії волі їх суб 'єктів [8, с.52, 61**]**.

На думку А. Мюррея, дискусія про необхідність регулювання кіберпростору вже не актуальна, а на сьогодні питання полягає в тому, як максимально ефективно формувати відповідне законодавство, виходячи з принципу верховенства права [9, с. 11].

Цілком обґрунтованою є думка, про те, що ІТ-законодавство або кіберзаконодавство має бути спрямоване на регулювання мережевих відносин, свободи слова, права на приватність, інтелектуальну власність, безпеку в Інтернеті, безпеку баз даних та авторські права на комп'ютерні програми, протидії злочинності в Інтернеті, онлайн-обміном товарами та послугами [10, с. 115].

Таким чином, можна говорити про активні процеси формування теорії правового регулювання відносин, опосередкованих віртуально - цифровим форматом. Здійснюючи науковий аналіз феномену віртуальності слід виходити з того, що це надскладне глобальне техніко – соціальне явище, яке містить в собі різноманітні аспекти і характеризується поліваріантністю об’єктивних форм та проявів, дослідження яких може бути предметом подальших досліджень в цьому нарямку.

Використана література:

1. SutherlandI.Theultimatedisplay// InformationProcessing: Proceedingsofthe IFIP Congress1965. Washington, DC : SpartanBooks. pp.506–508.–URL: https://www.wired.com/2009/09/augmented-reality-the-ultimate-display-by-ivan-sutherland-1965
2. LunenfeldP.TheDigitalDialectic: NewEssaysonNewMedia/P.Lunenfeld. –London. –MitPress. –1999. – 284 c.
3. Кутырев В.А. Оправданиебытия (явлениенигитологии и его критика) // Вопросы философии. – 2000. – № 5. – С. 17 – 26.
4. Loomis, J.M. Distalattributionandpresence / J.M. Loomis // Presence: TeleoperatorsandVirtualEnvironments. –1992. –№ 1. – p. 113 –118.
5. Cline, M. S. Power, madness, andimmortality: Thefutureofvirtualreality. [Online]. Available: http://virtualreality.universityvillagepress.com/index.php
6. Дзьобань О. П. Правовий дискурс справедливості як віртуальна реальність права / О. П. Дзьобань, Ю. В. Мелякова // Інформація і право. – 2013. – № 2. – С. 5-16.
7. Баранов О. А. Віртуальність і правове регулювання / О. А. Баранов // Публічне право. –2017. –№ 1. –С. 210-218.
8. Бєляков К. І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин: "віртуальні правовідносини" / К. І. Бєляков // LexPortus. –2016. –№ 2. –С. 47-63.
9. MurrayA. LookingBackattheLawoftheHorse: WhyCyberlawandtheRuleofLawareImportant //*SCRIPTed*. – 2013. –10:3 URL: http://script-ed.org.
10. Medic Z., Zivadinovic J. Iinternetandinternetlaw// Implementationofinformationtechnology: it, marketing, education and business working to gether for businesssuccess. –2018. –№10. – с.105 - 128.

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

Андрієнко О. В.,
к. психол. н., керівник юридичного відділу ДП «ССМ»(PublicisGroupe), адвокат ORCIDID 0000-0002-9452-8126

ВІРТУАЛІЗАЦІЯ ЯК ПРАВОВА КАТЕГОРІЯ

Суб'єктивно стрімкість розвитку технологій співвідносна з розширенням Всесвіту після Великого вибуху. Ця стрімкість трансформує всі сторони буття людства, включаючи регульовані правом. Проте і національне, і міжнародне законодавство відстають від технічного розвитку. А розмаїття термінології у вітчизняних та англомовних джерелах на позначення самої сфери:кібер-, електронна, інформаційна, IT, цифрова (з'явилося навіть слово цифровізія), діджитал- та просто "і-", – вказує на відсутність правової доктрини, яка б стала відправною точкою для побудови органічної системи нормативного регулювання.

Проте розробка уніфікованого понятійного апарату (тезаурусу) є необхідною передумовою для синхронізації зусиль фахівців дуже різних сфер людського пізнання і практики, а, отже, для ефективного регулювання взаємодії з технологією, не відпускаючи її на самоплин та не даючи їй взяти нас під контроль.

Поточний стан розвитку техносфери добре ілюструють два джерела: звіт Прайс Уотерхаус Куперс «Вісім ключових технологій для бізнесу: як підготуватися до їх впливу» [1] та щорічний прогноз розвитку підключеного світу у 2019 р. [2] за десятьма напрямками: технології, наука, медицина, оточуюче середовище, енергетика, урядування, пристрої, бізнес, мистецтво і мас-медіа, безпека.

Незважаючи на різноманітність згаданих напрямків і технологій, їх аналіз у межах традиційного для права підходу дозволяє виділити такі спільні ознаки:

1) Об'єктивна сторона постійно розширюється:масштабування (автоматизація) у просторі й часі відбувається одночасно як у напрямку глобалізації та стабільності (тобто збільшення просторових масштабів та практично нескінченної відтворюваності), так і в напрямку мініатюризації і прискорення (тобто ущільнення на одиницю простору-часу);

2) Об'єкти трансформуються і стають все більш потоковими, плинними, процесуальними [3]. Зростає неприв'язаність до матеріальних носіїв і меншою стає залежність від жорстких об'єктивних обмежень, які задаються законами фізики. На це вказує і відв'язування основних одиниць вимірювання від матеріальних носіїв-еталонів, так, з 20.05.2019 р. кілограм буде виражатися через постійну Планка. Отже,людство наближається до тієї межі, коли за наявності достатньої кількості інформації й енергії будь-що можна створити із будь-чого. Як наслідок, відбувається постійна інтенсифікація інформаційно-енергетично обміну зі зростаючим колом суб'єктів та об'єктів.

3) Суб'єкти трансформуються: розвиток технологій і сучасного світу неможливий без колективного інтелекту [4]. Це призводить до появи нових

суб’єктів, передусім, колективних, як-то групи у соціальних мережах, учасники краудфандингових кампаній, багатотисячні авторські колективи (Вікіпедія).

Формування сучасних технологій первісно потребувало **усвідомленої** участі людини як носія психіки. Таке формування було фізично й інтелектуально надзвичайно ресурсоємним. Завдяки колективному інтелекту нам вдалося усвідомити ключові закономірності буття природи і втілити це розуміння у технологіях [4], перевівши його на новий якісний рівень через автоматизацію й віртуалізацію. Як наслідок, індивідуальна поствідомість асимілює колективне свідоме: людина використовує технології на операційному рівні без глибокого розуміння «як це працює» (користується мобільним зв’язком, Інтернетом чи системою GPS-навігації тощо), проте завдяки доступу до накопичених людством знань має можливість їх усвідомити, якщо буде така необхідність.

4) Роль суб’єктивної сторони (розуміння, здатності до критичної оцінки, бажань, рішень) суб’єктів права різного масштабу постійно зростає. Адже віртуальні світи все менше залежать від фізично заданих законів і все більше – від уяви і волі суб’єктів соціальної (і правової) взаємодії, які створюють закони функціонування таких віртуальних реальностей, будь-то криптовалюти, користування дронами чи модерація груп у соціальних мережах.

Це повинно покладати на всіх суб’єктів, дотичних до інформаційних технологій (як розробників, так і користувачів), посилену відповідальність за наслідки їх використання. Адже з розвитком технологій конструюються як нові можливості та способи буття, так і нові загрози, бо самі такі технології є джерелом підвищеної небезпеки. Як ілюстрацію наведемо роль неформальних лідерів громадської думки у поширенні неперевіреної інформації, генерованої соціальними ботами, причому чим неймовірніша за своїм змістом інформація, тим більшою довірою вона користується [5].

Отже, розмиваються не лише межі об’єктів, але й суб’єктів, що безпосередньо впливає на право. Так, володіння об’єктом права інтелектуальної власності витісняється послугою надання доступу на вимогу (сервіс Netflix); між раніше жорсткими електоральними групами відбувається міграція як реакція на поточні події та інформацію різного ступеню верифікації; а концепція бенефіціарного власника постійно ускладнюється як у корпоративному праві й відносинахз довірчого управління майном, так і у міжнародному податковому законодавстві. Така плинність всього і вся спонукає також до трансформації правових доктрин (наприклад, поняття права власності чи виборчого законодавства) в умовах перманентної віртуалізації людського буття.

Відповідно до словника «віртуалізація – це перехід на вищий рівень абстракції в управлінні конкретними конфігураціями обчислювальної системи» [6, с. 189]. У той же час, «абстрагувати – уявно (в думках) відривати, відокремлювати одні (окремі) аспекти явищ чи властивості предметів від інших» [6, с. 3.].

Свою етимологію слово «віртуалізація» веде від латинського virtus, яке, зокрема, означає: 1) мужність; стійкість, *енергія*; сила; 2) доблесні справи;3)

найвища якість; відмінні властивості; вартість, талант; дар» [7, с. 685]. Латинське □□□ (vrtti: професія, залежність, спосіб буття, існування, характер, настрій, поведінка), □○□□□□ (virya: енергія), а також аватар – □□□□□ (спускатися; бути; долати; інкарнація, вхід, переклад, можливість, сходження) [8].

Отже, **віртуалізація – це квінтесенція попереднього рівня розвитку, яка отримує стрибкоподібний розвиток на наступному рівні** (згідно другого закону діалектики щодо переходу кількісних змін у якісні). Поява хімічних реакцій на базі фізичних елементів, біологічного життя на основі хімічних реакцій, еволюція мови, винайдення букв і цифр, поява обчислювальних машин – все це етапи віртуалізації.

Зауважимо, що поняття з коренем «віртуал-» вже використовуються у вітчизняних нормативних актах (Стратегія електронного парламентаризму на 2018 – 2020 р.;Концепціярозвитку цифрової економіки та суспільства України на 2018 – 2020 роки; Національна транспортна стратегія України на період до 2030 року).

Водночас семантичні корені альтернативних назвдля галузі є менш ємними:

- кібер- – походить відлатинізованого грецького слова «мистецтво навігації» через французьке cybernétique «мистецтво управління»[9];
- електронне – запозичене через латинську (electrum) від грецького «ἤλεκτρον» «бурштин»[9], і, можливо, пов’язане з санскритським □□□□□ (ulka, “метеор”) або грецьким ἠλέκτωρ (ēléktōr, «сонце, що сяє”) від ἥλιος (*hḗlios*, “сонце”) [10];
- інформаційне – походить від латинського «informare»– «тренувати, навчати; надавати форму» [9];
- і- – цей префікс вперше з’явився у 1994 р. у назвісайту інтернет-спільноти жінок iVillage, а у 1998 вжитий AppleInc.для iMac зі значенням «Інтернет»; однаквін використовується не лише IT-компаніями, (скажімо, icoke.com).Хоча реклама фільму «Я, робот» (“I, Robot”) за мотивами творів Азімова використала маленьке і як культурний мем [10], він приходить і в науку (наприклад, iMinds);
- Інтернет- – термін з’явився у 1984 році на позначення «мережі пов’язаних комп’ютерів Департаменту оборони США [9];
- цифрове – слово пройшло довгий шлях від санскриту (sunya-s – «порожній») через арабську (sifr – «нуль, нічого» від «safara» – «бути порожнім»), середньовічну латину та французьку, італійську, іспанську («арифметичний символ для нуля»). До речі, має спільне походження зі словом «шифр» [9];
- діджитал – первинно походить від латинського «digitus» – «палець» і пізнішого «digitalis» – «стосуватися номерів до 10». Наразі може використовуватися як антонім до аналогового [9].

З огляду на проведений аналіз,слово «віртуальний» є найбільш адекватною назвою для галузі (а з часом – сукупності галузей) права, покликаної врегулювати аспекти життя окремої людини і людства в цілому, пов'язані з переходом від домінуючої взаємодії з реальним світом до буття у віртуальному світі технологій.

При цьому можна прогнозувати, що глобальний поділ галузей на публічне та приватне право буде доповнений дихотомією «реальне право – віртуальне право».

Використана література:

1. PWC Global. The Essential Eight. Your guide to the emerging technologies revolutionizing business now URL : – Mode of access: https://www.pwc.com/gx/en/issues/technology/essential-eight-technologies.html. – Last access: 2018. – Title from the screen.
2. The Wired World UK. Annual2018 – 2019. – London: The Conde Nast Publications, 2018. – 128 p.
3. Келлі, Кевін. Невідворотне. 12 технологій, що формують наше майбутнє [Текст] / Кевін Келлі ; переклад з англійської Наталії Валевської. – К.: Наш формат, 2018. – 304 с.
4. Сломен, Стівен. Ілюзія знання. Чому ми ніколи не думаємо на самоті [Текст] / Стівен Сломен, Філіп Фернбак ; переклад з англійської Мирослави Лузіної. – К.: Yakaboo Publishing, 2018. – 344 с.
5. Shao, Chengcheng. The spread of low-credibility content by social bots [Text] / Ch. Shao, G.L. Ciampaglia, O. Varol, K.-Ch. Yang, A. Flammini, F. Menczer //Nature Communications, 2018. – Volume 9. – Article number: 4787.
6. Великий тлумачний словник сучасної української мови [Текст] / Уклад. і голов. ред. В. Т. Бусел. – К.: Ірпінь: ВТФ «Перун», 2007. – 1736 с.: іл.
7. Трофимчук, Мирослав. Латинсько-український словник [Текст] / М. Трофимчук, О. Трофимчук. – Львів: Видавництво ЛБА, 2001. – VIII + 694 с.
8. Кочергина, В. А. Санскритско-русский словарь : около 30 000 слов[Текст]/Под ред. В. О. Кальянова.– 2-е изд., испр. и доп. – М.: Рус. Яз., 1987. – 944 с.
9. Online Etymology Dictionary URL: – Mode of access: https://www.etymonline.com/word/. – Last access: 2018.
10. Wikipedia URL: – Mode of access: https://en.wikipedia.org/wiki/Internet-related_prefixes. – Last access: 2018.

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

Бруслік А. В.,
студент І курсу Національного університету біоресурсів і природокористування України
Хвіст В. О.,
к.і.н., доцент, кафедри міжнародних відносин та суспільних наук

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ В УМОВАХ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

В останні роки у перспективах розвитку Інтернет-сфери набуває активного поширення словосполучення «Інтернет речей». Як зазначається у понятті

«Інтернет речі» (скорочено ІТ, англ. – Internet of Things) розглядається як фізично реальні системи і комплекси, функціонування яких базується на використанні величезної кількості датчиків, комп'ютерних і телекомунікаційних технологій, робототехніки, штучного інтелекту, хмарних обчислень, мережі Інтернет, застосування яких надає можливості за участю або без участі людей приймати і реалізовувати рішення. Завдяки інтернету задовольняються інформаційні, економічні та інші потреби. З появою ІТ у людства з'явились великі можливості, але з приходом можливостей приходить і велика відповідальність. З'явилась потреба в ефективному правовому регулюванні, що забезпечить безпечне використання ІТ по всьому світу. Метою даної роботи є розгляд можливих проблем правового регулювання в умовах застосування технологій інтернету речей та пошук можливих рішень.

Провідні позиції у світі щодо правового забезпечення використання технологій ІТ займають країни Європейського Союзу, США, Японія, КНР, Італія. Безумовно, правове регулювання маєсприяти використанню технологій ІТ в інтересах людей. Але, нажаль, інтереси людей не завжди бувають законними та правомірними. Ознайомившись з працями Баранова О.А. не можна не згадати правові проблеми використання нових технологій які безпосередньо взаємодіють в умовах інтернет речей. Для вирішення таких проблем в першу чергу необхідно встановити правові вимоги, щодо запобігання незаконному перехвату програм, що відповідають за дії тих самих 3Dпринтерів, дронів, робомобілів тощо [5, с. 10].Зараз гостро стоїть питання правового регулювання щодо використання людьми ІТ. Погоджуючись з Пилипчуком В.Г., треба дійсно наголосити на тому, що в різноманітних системах Інтернет речей використовується і буде використовуватися багато персональних даних. До ключових проблем Інтернету речей можна віднести саме безпеку і захист персональних даних. 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, с. 17]. Ще більшою проблемою є правове регулювання всіх процесів в електронній мережі, які здійснює та чи інша персона. На даний момент не існує ефективного, єдиного методу ідентифікації конкретних осіб причетних до незаконних діянь що призвели до втрати персональних даних конкретної особи. Адже лише використання проксі-серверів вже робить користувача анонімним. Згідно основоположних принципів міжнародного права про захист персональних даних, затвердженими першою у світі Конвенцією Ради Європи № 108 від 28.01.81 р. та рядом директив Європейського Союзу, зокрема Директивою Європейського Парламенту і Ради 95/46/ЄС від 24.10.95 р., стосовно захисту персональних даних, захист прав людини у сфері персональних даних передбачає, зокрема, наступне: «Персональні дані, що піддаються

автоматизованій обробці: a) отримуються та обробляються сумлінно та законно; b) зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями; c) мають бути адекватними, відповідними і не надмірними з точки зору цілей, для яких вони зберігаються» [2, с. 10].

Близько 8 років тому була створена перша криптовалюта світу «біткоїн». Специфічна природа криптовалюти зумовлює те, що відповідне питання не є першочерговим для вирішення. Але необхідність втручання держави в особі її органів була зумовлена тим, що біткоїн став платіжним засобом діяльності Даркнету, анонімна мережа, яка на сьогодні активно функціонує в мережі Інтернет по всьому світу, яка схожа на чорний ринок, де можна придбати зброю, наркотики, людей, фальшиві гроші та документи. США, Німеччина, Японія, Франція, Фінляндія та інші країни не тільки дозволили обіг відповідної валюти, але й законодавчо закріпили чи підкріпили правовий режим, роз'яснили поняття біткоїнів та аналогів сформували відповідну судову практику.На жаль, піддаючись загальній тенденції чимало держав все-таки не встановлює режиму щодо криптовалюти через її специфічну природу. До таких держав відноситься і Україна. Проблемою, яка є найбільш фундаментальною і очевидною, є правова природа криптовалюти.

З вище описаного можна зробити висновок, що на міжнародному рівні сьогодні відсутня єдність в розумінні правової природи криптовалюти, тому держави по-різному визначають поняття біткоїна і його аналогам. Європейська судова практика по суті прирівняла криптовалюту до законного платіжного засобу, а обмін грошових коштів – «валютно-обмінною операцією». Але все-таки, згідно чинного законодавства ЄС цифрова валюта вважається товаром і підпадає під регулювання Цивільного законодавства і Директиви ЄС про ПДФ як товар, а договір купівлі–продажу щодо криптовалюти є договором купівлі–продажу товару [3, с. 2].

Щодо застосування штучного інтелекту, необхідно буде вирішити дуже багато правових проблем в регулюванні пов'язаних з тією обставиною, що людина – біологічна істота, а робот – ні. Перш за все, це проблеми визначення для роботів понять, критеріїв, змісту та обсягів правоздатності, дієздатності і деліктоздатності; вирішення проблеми встановлення для роботів спеціальної або загальної правосуб'єктності і багато інших. Іншими словами, роботи розглядаються як людиноподібні суб'єкти, які здійснюють людиноподібні дії в процесі відносин з традиційними суб'єктами. Якщо дії традиційних суб'єктів в таких відносинах підлягають правовому регулюванню, то логічно припустити, що інша сторона також є суб'єктом цих правовідносин. Якщо робот-андроїд або андроїд повинен нести юридичну відповідальність за свої дії, тоді він повинен мати фізичну, юридичну та цифрову ідентичність, подібну людині. І якщо у робота є ті ж юридичні обов'язки, що і у людини, хіба в нього не повинні бути такі ж юридичні права, як у людини?[1, с. 14]

Розглянувши дану тему, можна стверджувати що без чіткого механізму правового регулювання, сучасні технології перетворять наше життя на хаос, за яким може прийти не тільки стагнація, але й війна. Завершити хотілося б словами Річарда Хукера, які як ніколи описують розвиток сучасних технологій: «Будь-яка зміна, навіть зміна на краще, завжди пов'язана з незручностями» [3, с. 1].

Використана література:

1) Інтернет речей: проблеми правового регулювання та впровадження / Баранов О. А. // Інтернет речей (IoT): огляд правових проблем. – 2017. - № 2, 3. – С. 14.

2) Баранов О.А. Інтернет речей (IoT): мета застосування та правові проблеми / О.А. Баранов // Інформація і право. – 2017. – № 2. – С. 7-15.

3) Плита А.І. Есе з права ІТ: криптовалюта: її правовий режим, проблеми застосування. – 2017. - абзац 2-7.

4) Баранов О.А., Захист персональних даних в сфері Інтернет речей. – 2017. - С. 85-91

5) Інтернет речей: проблеми правового регулювання та впровадження / Баранов О. А. // Інтернет речей (IoT): огляд правових проблем. – 2017. – № 3. – С. 11-12.

6) Інтернет речей: проблеми правового регулювання та впровадження / Пилипчук В. Г. // Становлення і регулювання суспільних відносин у сфері новітніх інформаційних технологій. – 2017. - № 2. – С. 17.

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

Ашихмін І. М.,
аспірант кафедри міжнародного та європейського права Національного університету «Одеська юридична академія»

ІНВЕСТИЦІЇ В ХМАРНІ ТЕХНОЛОГІЇ: ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ В УКРАЇНІ

На сьогоднішній день найбільш популярними галузями для інвестування, безсумнівно, є інтернет-проекти (близько 30 % в загальній кількості угод). Вони найменш капіталомісткі, при цьому мають потенціал вкрай швидкого зростання, що дозволяє інвесторові розраховувати на позитивний ефект у короткостроковій перспективі (1-3 роки).Хмарні сервіси відіграють ключову роль в IT-витратах – витрати на них виростуть на 19 % [1]. Більш того, очікується ще більший зсув фокусу уваги інвесторів з електронної торгівлі в підсектори хмарних технологій. Інвестори проявляють все більшу впевненість в хмарних і мобільних інвестиціях, ніж в інших секторах, таких як обладнання. З огляду на зазначене, належне правове регулювання використання хмарних технологій є запорукою нарощування інвестицій в розвиток хмарного ринку.

Завдяки швидкому розвитку інформаційних технологій та появі дедалі нових можливостей миттєвої передачі інформації у будь-який куток світу зберігання інформації на носіях зберігання втрачає актуальність. Хмарні сховища надають можливість користувачу мережі Інтернет не тільки зберігати величезні потоки даних, але й надавати доступ іншим користувачам до власної

інформації;більш того, не виникає необхідності у придбанні додаткових девайсів та залучення фахівців для обслуговування таких ресурсів. Іншими словами, можна визначити хмарне сховище, як вільний простір у мережі Інтернет, куди надається можливість завантажувати власні ресурси (програма, матеріали) і у будь-який час з будь-кого місця мати доступ до таких ресурсів.

У зв'язку з тим, що ринок хмарних технологій знаходиться в процесі становлення, правове регулювання даної сфери на даний час не сформовано, та спірні моменти щодо надання хмарних послуг у повному обсязі не врегульовані. Потреба у стандартизації захисту зберігання та передачі інформації, оцінці рівня наданих послуг потребує комплексного правового регулювання даної сфери відносин. Цей сектор, у більшості випадків, регулюється за аналогією закону та поодинокими суміжними правовими актами, і цього, звісно, недостатньо. На даний момент, вимог щодо здійснення діяльності із надання хмарних послуг у відповідності до стандартів ISO та обов'язкової сертифікації провайдерів з боку держави ніяк не врегульовано. Листом Комітету Верховної Ради України з питань інформатизації та зв'язку від 13.02.2017 р. № 04-21/13-74(34081) було визначено основні моделі використання та обліку програмного забезпечення при використанні та надані хмарних послуг відповідно. При оподаткуванні таке програмне забезпечення може визнаватись як об'єкт:

1) основних засобів (у разі, коли така програма є системною);

2) нематеріальних активів (купуються майнові права на комп'ютерну програму);

3) роялті для власного використання (у разі, коли ліцензіату надано право користування комп'ютерною програмою без можливості її продажу (або відчуження), умови використання програми не обмежені її функціональним призначенням, а відтворення програми – певною кількістю копій, плата за користування такою програмою вважається роялті);

4) роялті для власного використання та надання послуг, у разі коли оплачується обслуговування програми, але сама програма не придбається, така плата вважається платою за послуги.

Постановою Верховної Ради України від 20.09.2016 року було прийнято за основу проект Закону України про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень і доручено Комітету Верховної Ради України з питань інформатизації та зв'язку доопрацювати зазначений законопроект з урахуванням зауважень і пропозицій суб'єктів права законодавчої ініціативи та внести його на розгляд Верховної Ради України у другому читанні. Документом поставлено вирішити наступні протиріччя:

– ввести до законодавства поняття «система хмарних обчислень» і «надавач хмарних послуг»;

– розширити можливості щодо використання різних засобів захисту при обробці в системі хмарних обчислень інформації, яка не становить державної таємниці;

– впровадити можливості використання систем хмарних обчислень, які мають сертифікати відповідності національним або міжнародним стандартам у сфері захисту інформації;

– впровадити концепцію зобов'язань надавача хмарних послуг;

– розширити коло суб'єктів, які можуть обробляти персональні дані, володільцями яких є органи державної влади чи органи місцевого самоврядування;

– визначити особливості обробки інформації в системах хмарних обчислень [3].

Таким чином, прийняття такого проекту можна пов'язувати із появою початкового врегулювання сфери надання хмарних послуг. Цей процес створює передумови нормативного врегулювання надання хмарних послуг та сприяє привабливості інвестування в зазначену сферу. Прийняття спеціального закону надасть певні гарантії захисту у договірних відносинах між провайдером та користувачем таких послуг:будуть улагоджені питань щодо відповідальності сторін договору про надання хмарних послуг, порядку видалення інформації із хмарного сховища, порядку вступу у даний тип правовідносин тощо. Така чисельність істотних умов, що мають бути нормативно закріплені дасть змогу якісно та ефективно захищати свої права користувачу у випадку їх порушення та встановити певні умови для провадження господарської діяльності із надання таких послуг.

Використана література:

1. Ravindranath M. Investorsconfidentincloudventures, surveyshows. *The Washington Post*. 2013. August 14. URL: https://www.washingtonpost.com/business/ on-it/investors-confident-in-cloud-ventures-survey-shows/2013/08/14/544c687a-0461-11e3-9259-e2aafe5a5f84_story.html?noredirect=on&utm_term=.4a6f1c0a85da

2. Системи хмарних обчислень та ЕЦП регулюватимуться по-новому. URL: http://www.interbuh.com.ua/ru/documents/onenews/101337.

3. Листвід 13.02.2017 р. N 04-21/13-74(34081)/ Комітет Верховної Ради України з питань інформатизації та зв'язку. URL: https://zakon.help/article/nadannya -hmarnih-poslug/.

4. Постанова Верховної Ради України від 20.09.2016 року «Про прийняття проекту Закону України про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень»/ Верховна Рада України. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T161 523.html.

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

Дубняк М. В.,
к.ю.н., старший викладач кафедри
ІППІВ, КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ БІЗНЕС МОДЕЛЕЙ СТАРТАП ПРОЕКТІВ НА БАЗІ ХМАРНИХ ТЕХНОЛОГІЙ

На ранньому етапі життя стартапу віртуальна інфраструктура - розумне рішення, оскільки, заздалегідь невідомий обсяг ресурсів для обслуговування бізнесу, а отже і статті інвестиційних видатків на забезпечення таких ресурсів є критичним питанням для бюджету стартап проекту.

Із появою хмарних технологій бізнес моделі зазнали значних змін. Зокрема, мова іде про хмарні послуги як сервіс - SaaS, IaaS і PaaS. Програмне забезпечення як послуга: (SaaS) модель, за якої, програмне забезпечення (ПЗ) знаходиться на сервері розробника або провайдера, а користувач отримує до нього віддалений доступ за допомогою мережі інтернет. Послуга полягає у тому, що розробник або провайдер надають свій сервер, на якому працює програма, підтримку цього сервера та ПЗ. А користувачі знижують витрати на інфраструктуру та утримання IT-спеціалістів. Інфраструктура як послуга: (IaaS) модель, в якій клієнт може встановлювати будь-яке програмне забезпечення і додатки на віртуальні сервери і віртуальну мережу. Платформа як послуга: (PaaS), модель в якій клієнт управляє програми (веб-сервер або база даних), а операційною системою управляє провайдер [1].

Використання будь-якої моделі хмарних сервісів для початку господарської діяльності значно мінімізують кількість транзакційних витрат. Інвестор та консультант Ендрю Чен (Andrew Chen), вказує що стартапи дешевше побудувати, ніж масштабувати - витрати на співробітників і маркетинг ростуть [2].

До основних переваг хмарних сервісів відноситься: гнучка можливість масштабування, яка дозволяє додавати тисячі віртуальних серверів і петабайт пам'яті за декілька хвилин; доступність; вивільнення ресурсів; що дозволяє реалізовувати бізнес план замість адміністрування сервісів; динамічна робота з даними.

У той же час не все так безхмарно на ринку хмарних технологій, до основних технологічних ризиків відноситься: проблема довіри до постачальника послуг (в частині захищеності і безпеки при обробці даних, їх підконтрольності саме клієнту, ризик монополізації даних провайдером послуги тощо); ризик нестабільної технологічної підтримки, проблеми забезпечення продуктивності і безпеки, проблеми ліцензування при зміні платформ, ризик втрати контролю над бізнесом.

Різниця у цих моделях полягає у ступені контролю користувача над власними даними. Тобто, кому належить бізнес-логіка запропонованих сервісів.

У разі використання стартапом існуючих SaaS-платформ, відбувається збагачення їх інформацією, що становить ядро бізнес-процесу компанії

(наприклад, комерційна таємниця у вигляді бази даних клієнтів/контрагентів, фінансового плану, тощо).

У разі коли стартап наймає власних розробників і використовує PaaS лише як провайдера технологічних потужностей, зберігається інтелектуальний суверенітет, оскільки, провайдер хмарних сервісів не має відношення до бізнес-процесу стартапу.

Кожна із цих моделей має свої переваги та недоліки, однак, у даному досліджені спробуємо знайти правові шляхи мінімізації цих ризиків для SaaS моделі.

З моменту створення чимало відомих стартапів розвивались за схемою віртуальної інфраструктури на базі Amazon Web Services (далі - AWS) - сервіси виконання високо масштабованих програмних додатків, для зберігання інформації на віддалених серверах компанії Amazon, що надають всі моделі SaaS, IaaS і PaaS. Зокрема, такі проекти як Dropbox, Instagram, WhatsApp та інші. Однак, згодом ці проекти стали самодостатніми бізнесами, які інвестують у власну інфраструктуру та переносять її з хмарних сховищ AWS у власні дата-центри. Для цього є декілька причин: 1. Забезпечення контролю над бізнесом. На початковому етапі стартапи фокусуються на прискоренні розвитку та реалізації бізнес-плану, а у стадії масштабування починають думати про повну незалежність, залучаючи необхідні ресурси на розвиток власної інфраструктури. 2. Конфлікт інтересів. На базі хмарних сервісів стартапи часто розвивають власні програмні додатки, які знаходяться на одному ринку із постачальником хмарних послуг, тому бізнес-процес який знаходиться під контролем конкурента — не краща стратегія розвитку. Наприклад, компанія Wal-Mart, що керує найбільшою в світі роздрібною мережею, вимагає від своїх постачальників технологічних рішень покинути хмари AWS, оскільки, Amazon та Wal-Mart є конкурентами в роздрібній торгівлі товарами [3]. Усі зазначені приклади, ілюструють загрозу монополізації фактичного розпорядника базами даних та ризик втрати контролю над власним бізнес-проектом.

Крім того, в SaaS моделі існує проблема неконтрольованої зміни програмного забезпечення, яке використовує стартап як бізнес-процес на початковому етапі. У класичній моделі власної інфраструктури та IT-спеціалістів будь-яка зміна програмного забезпечення (далі ПЗ) для покращення бізнес процесу може відбуватись шляхом: 1. Тестування нової версії ПЗ в ізольованому середовищі (тестовій зоні) з метою відпрацювання основних ризикових сценаріїв; 2. Повернення на попередню версію ПЗ, якщо в новій виявлені критичні для бізнесу недоліки. Аналогічні способи можна використовувати і при PaaS моделі. За таких умов, тестування покращень не впливає на бізнес-процес та функції інших співробітників, які продовжують вирішувати поточні завдання.

Однак, в SaaS моделі оновлення програмного забезпечення - це процедура, прихована від клієнтів, наслідком якої є повна зміна роботи сервісу та зміни у збережених клієнтських даних (наприклад, коли видаляється функція управління

даними з їх відображення, структурування, групування). Від користувача не залежить момент прийняття рішення про зміну технічного функціоналу програмного забезпечення, яке надається як послуга. Користувач у такому разі не має можливості ні повернутись до попередньої версії, ні відтермінувати оновлення. Таке оновлення ПЗ сервісу може призвести до знищення бізнес-процесу, який був критичним для стартапу.

З об'єктивних причин, компанія SaaS не може задовольнити 100% вимог всіх своїх клієнтів, а отже останнім залишається вибір: адаптація бізнес-процесу до нових функцій сервісу, чи зміна сервісу. У будь-якому випадку це додаткові транзакційні витрати.

Зазначені ризики можуть бути мінімізовані у випадку укладення договорів із постачальниками хмарного сервісу. Правова природа цих договорів має комплексний характер, і розглядається з трьох основних позицій [4].

На перший погляд може здаватись, що вказана проблема може бути вирішена за допомогою ліцензійних договорів. Однак, за ліцензійним договором (в розумінні ЦК) передаються права на примірники ПЗ, а використання за функціональним призначенням ліцензійним договором не регулюється. При виборі правового регулювання цих відносин важливо враховувати технологічну складову, а саме те, що різним сервісами інформаційної системи SaaS включає у себе програмне забезпечення, обладнання та інформацію в базах даних. Тобто програмне забезпечення використовується в сукупності і нерозривному зв'язку з іншими елементами інформаційної системи. При цьому екземпляри ПЗ користувачем не завантажуються у пам'ять пристроїв, не модифікуються, тобто в його фактичне володіння і користування не надходять. Всі дії з такими програмними продуктами виконуються на стороні власника сервісу.

Щодо регулювання відносин у моделі SaaS за договором оренди, то відзначимо наступне. Відповідно до ст. 760 ЦКУ предметом договору найму (оренди) може бути річ, яка визначена індивідуальними ознаками і яка зберігає свій первісний вигляд при неодноразовому використанні (неспоживна річ). Адже обладнання у хмарному сервісі не може бути індивідуалізоване, а програмне забезпечення не є річчю на відміну від його носія.

Отже, у разі виникнення спору, як ліцензійний договір, так і договір оренди, буде нікчемним в силу приписів закону.

Щодо регулювання за договором про надання інформаційних послуг, то предметом такого договору будуть дії суб'єктів щодо забезпечення споживачів інформаційними продуктами, тобто документованою інформацією призначеною для задоволення потреб користувачів (в розумінні Закону [5]).

З врахуванням проаналізованих ризиків, у SaaS-договорах доцільно вказувати спосіб, строк та порядок проведення удосконалення ПЗ, вимоги щодо попереднього погодження технічних умов майбутніх змін, гарантії та компенсації у випадку невідворотної зміни функціоналу, що стала наслідком проведених

удосконалень, вимоги щодо періодичності кешування даних та їх перенесення на інші платформи у разі зміни бізнес-процесу, та інші.

Висновки. Поява технологічних рішень та їх використання неминуче впливає на розвиток суспільних відносин, в тому числі і процес організації і ведення бізнесу. Дослідження технологічних особливостей функціонування новітніх інформаційних технологій забезпечує ідентифікацію ризиків їх використання, що, в свою чергу впливає, на побудову правових моделей регулювання суспільних відносин, які здійснюються з використанням цих технологій.

Використана література:

1. Облачные вычисления. Матеріал з Вікіпедії вільої енциклопедії URL:https://ru.wikipedia.org/wiki/ Облачные_вычисления
2. Andrew Chen Startups are cheaper to build, but more expensive to grow – here's why URL: https://andrewchen.co/startups-are-cheaper-to-build-more-expensive-to-grow/
3. Кто «покидает облака»: западные ИТ-стартапы, которые отказались от виртуальной инфраструктуры URL: https://habr.com/company/ it-grad/blog/346070/
4. Как составить договор SaaS без правовых рисков URL:http://www.it-lex.ru/article/sostavit_dogovor_saas
5. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР. URL: http://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

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

Камінський О. Є.,
кандидат економічних наук,
доцент кафедри інформаційного менеджменту, ДВНЗ Київський національний економічний університет, doc-web@ukr.net

ПОБУДОВА ДЕРЖАВНОЇ ХМАРНОЇ ПЛАТФОРМИ ДЛЯ РЕГУЛЮВАННЯ РИНКУ КРИПТОАКТИВІВ В УКРАЇНІ

Біткойн – це криптовалюта, яка нещодавно виникла як популярний засіб обміну, з багатими та великими екосистемами. Мережа Bitcoin працює на більш ніж 42 × 10 флопс, а його загальна ринкова капіталізація дорівнює близько 12 млрд. долл. США, від січня 2014 року [1]. В основі фінансових операційкріптовалют лежить глобальний загальнодоступний журнал, який називається блокчейном та фіксує всі транзакції між клієнтами Bitcoin. Технологія блокчейна з'явилась як частина розподіленої бази даних, в якій повинні були зберігатись операції в електронній валюті. Вона повинна убезпечити розрахунки від несанкціонованого втручання і одночасно забезпечити контроль всіх операцій на рівні окремих грошових одиниць. Останнім часом блокчейн привертають увагу дослідників у широкому спектрі галузей промисловості [2] [3]. Таким чином, кожен користувач кріптовалюти має можливість не лише вільно здійснювати купівлю-продаж, а й точно знати, яке походження мають гроші, якими із ним

розплачуються. Величезний обсяг потоків даних виробляється системами блокчейн на високій швидкості. З ефективним і гнучким забезпеченням у хмарних обчисленнях [4], [5] великий об'єм даних, вироблених при виконанні транзакцій кріптовалют, може передаватися до віддаленого хмарного середовища для обробки через Інтернет. Проте, Інтернет не є достатньо ефективним або достатньо захищеним для оброблення цих величезних обсягів даних, а робота систем блокчейну недостатньо урегульована з точки зору права.

Вважаємо, що держава має долучитися до цього процесу і забезпечити побудову такої інфраструктури шляхом реалізації концепції власної інноваційної хмарної платформи.

Основною ідеєю концепції побудови державної хмарної інноваційної платформи є створення гібридної хмари, що дозволить об’єднати постачальників і споживачів інформаційних продуктів та сервісів, інвесторів в сфері ІТ, а також механізми обміну та захисту інформації. Реалізація запропонованої концепції забезпечить підтримку діяльності вітчизняних господарюючих суб’єктів з боку ІТ, що дозволить скоротити їх витрати на даний напрям на 10-15% і підвищити якість бізнес-процесів. Розробники та офіційні дистриб'ютори інформаційних продуктів отримають нових клієнтів, тим самим збільшать обсяг продажів і розвиватимуть ринок ІТ. Важливо, що держава може одночасно виступати і споживачем власних хмарних сервісів. Зокрема, сфери охорони здоров’я, транспорту, житлово-комунальна та інші соціально значимі галузі зможуть безпечно використовувати інформаційні продукти і технології та не залежати від іноземних компаній – хмарних провайдерів, що надають послуги на власний розсуд. Розвиток державних централізованих хмар призведе у свою чергу до розвитку таких передових технологій, як SDN (Software Define Network) та SDDC (Software Define Data Center). Переведення подібних сервісів в програмну площину також дозволить пожвавити і сегмент внутрішньої розробки програмного забезпечення.

За кордоном державний сектор успішно переходить на використання власних хмарних сервісів. Так, Державний департамент США чітко продемонстрував свою мету стати потужним постачальником хмарних послуг через свою системи хмарних сервісів FAN (Foreign Affairs Network). Держава планує збільшити свої послуги через FAN на 15% до кінця 2018 року. Штат Делавер переніс 80 відсотків фізичних серверів державних органів влади в приватну хмару і економія коштів оцінюється приблизно в 4 мільйони доларів на рік. Однак ці програми пропонують створення закритих або окремих хмарних платформ для різних державних органів. На відміну від них, запропонована нами платформа передбачає створення єдиної інфраструктури у вигляді системи державних ЦОД, відкритої для комерційних клієнтів - як найбільш доцільний метод забезпечення економічно обґрунтованих умов для зосередження інформаційних ресурсів, обробки транзакцій кріптовалют.

Складність роботи державних установ буде тільки зростати в найближчі роки, оскільки кількість електронних цифрових послуг для населення стрімко

зростає. Єдина державна хмарний платформа дозволить заощадити кошти за рахунок ліквідації закупівель нових версій програмного забезпечення, обладнання для його розгортання, а також їх постійної технічної підтримки. Плата за розгортання приватних сервісів на базі державної платформи також забезпечить додатковий прибуток держбюджету. Реалізація саме державної хмарної платформи здатна забезпечити наступні переваги для органів державної влади та населення (див табл.1).

Таблиця 1.

Аналіз переваг державної хмарної платформи

Переваги	**Моделі обслуговування**	
	PaaS	**SaaS**
Економія витрат	скорочення витрат бюджету на придбання програмного забезпечення	скорочення витрат організації на обслуговування програмних додатків
Підвищення керованості IT-інфраструктури	Комплексна автоматизація органів державної влади	Підвищення якості сервісів, систем захисту даних
Підвищення продуктивності роботи користувачів	Єдине середовище з доступом для безлічі сервісів	Скорочення часу реєстрацію та авторизацію
Аналіз даних	Застосування методів BigDate для отримання статистичної інформації для податкових органів	Контроль фінансових транзакції кріптовалют
Централізоване забезпечення вимог законодавства	Централізоване внесення законодавчих змін до державних реєстрів	Оперативне внесення змін до сервісів
Захист інформації	Скорочення витрат на розробку та впровадження систем моніторінгу сервісів	Зменьшення витрат на відновлення сервісів у випадку хакерських атак

В якості технічного рішення інноваційної хмарної платформи може бути обрана модель багатофункціональної хмарної інфраструктури на базі розподіленого хмарного центру оброблення даних (ЦОД), що використовує конвергентну (інтегровану) архітектуру, засновану на хмарних обчисленнях і SDN (Software Define Network, програмно-обумовлені мережі передачі даних); об'єднує географічно розподілені державні ЦОД у віртуальну платформу, завдяки активному інтелектуальному управлінню, і надає ретельно налаштовані IT-сервіси.

Аналогічний проект вже реалізується в Японії. Компанія Ripple на замовлення японського уряду створює єдину систему швидких мобільних платежів. Блокчейн забезпечуватиме не лише ідентифікацію, а й захист від шахрайства. Про приєднання до цієї системи оголосив 61 японський банк (майже 80% японської фінансової системи), старт проекту заплановано на осінь 2018 р.

Впровадження таких систем, втім, має й декілька вузьких місць: автоматичні віртуальні контракти залежать від якості баз даних та від кількості перевірок (валідації) системи захисту даних. На сьогодні валідація недостатньо напрацьована –наприклад, відомий сервіс Prozorro передбачає всього дві перевірки: валідність інформації про фірму і контроль вартості контракту. Для роботи з криптовалютами цього недостатньо.

Для запобігання цьому, стандарти баз даних в Україні мають бути значно вдосконалені, і призведені до одного інтерфейсу віддаленого доступа до даних – наприклад, на основі європейського стандарту ANSI/ISO/IEC 9579-1, що дозволить швидко і ефективно розробляти системи віртуальних контрактів і оперативно підключати до них нові перевірки по мірі готовності нових баз даних. По друге, українська система електронного підпису, фактично представляє собою ручний сервіс. Тобто виданий підприємцю підпис легко може бути переданий третім особам. На цьому засновані, наприклад, маніпуляції з реєстром нерухомості та земельних ділянок. Можливість передачі ключів дозволяє маніпулювати віртуальними контрактами, як і реальними. Щоб уникнути цього, необхідно створити єдину систему ідентифікації громадян, можливо, теж на базі блокчейн-системи – подібної тій, яка розробляється в Японії та ЄС. Тоді кожен громадянин і підприємець зможе бути одночасно і власником і контролером свого ключа.

Нова модель державної розподіленої хмарної платформи заснована на трьох нових технологіях: хмарих обчисленнях, SDN і блокчейнах. Пропонована архітектура призначена для підтримки високої доступності, передачі даних у реальному часі, високої масштабованості, надійності, стійкості та низької затримки. Щоб полегшити регулювання ринку криптовалют України, запропонована платформа може суттєво зменшити затримку від обміну даних для роботи віртуальних контрактів, вартість обчислювальних ресурсів та завантаженнятрафіку в базовій мережі порівняно з традиційною архітектурою. Порівняно з традиційною методами контролю фінансових операцій, така модель є більш ефективним та захищеним рішенням для регулювання транзакцій криптовалют в Україні.

Використана література:

1. Top Strategic Predictions for 2017 and Beyond: Surviving the Storm Winds of Digital Disruption. [Електронний ресурс]. -2017. - URL: https://www.gartner.com/doc/ 3471568?ref=unauthreader

2. F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

Show Context
3. P. K. Sharma, S. Y. Moon, and J. H. Park, “Block-VN: A distributed blockchain based vehicular network architecture in smart city,” J. Inf. Process. Syst., vol. 13, no. 1, pp. 184–195, Mar. 2017.
4. S. Singh, Y.-S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” J. Netw. Comput. Appl., vol. 75, pp. 200–222, Nov. 2016.
5. X. Sun, N. Ansari, and R. Wang, “Optimizing resource utilization of a data center,” IEEE Commun. Surveys Tuts., vol. 18, no. , pp. 2822–2846, 4th Quart., 2016.

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

Бежевець А. М.,
старший викладач КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ВИЗНАЧЕННЯ ПРАВОВОГО СТАТУСУ КРИПТОВАЛЮТИ

Криптовалюта це новий продукт еволюційного розвитку і технічного прогресу, який стає сучасним та актуальним засобом обміну нарівні зі звичайними грошима.

Хоча на сьогодні в Україні статус криптовалюти ще не визначено на законодавчому рівні, але, виходячи із загально-правових принципів, підставно зробити висновок, що криптовалюта та операції з нею не заборонені. Однак, це не означає, що це питання має залишатися поза увагою законодавця.

Питання законодавчого врегулювання статусу криптовалюти є доцільним та необхідним, адже, як свідчить світова практика, криптовалюти набирають все більшу популярність; заборонити їх використання технічно неможливо і економічно недоцільно.

Згідно інформації CoinMarketCap на даний час налічується понад 2000 криптовалют загальною капіталізацією понад 100 млрд. дол. США.

На сьогодні в світі відсутній єдиний підхід до визначення статусу криптовалюти, в тому числі й на законодавчому рівні кожної окремої країни.

На даному етапі підставно вважати США лідером у світі за кількістю транзакцій з криптовалютами. Службою внутрішніх доходів США (IRS) в повідомленні 2014-21 від 25.03.2014 на федеральному рівні визначено, що криптовалюта може використовуватися для оплати товарів чи послуг або для інвестицій. Криптовалюта є цифровим відображенням вартості, яка виступає засобом обміну, одиницею розрахунків, але не має статусу законного платіжного засобу в будь-якій юрисдикції. Для цілей оподаткування криптовалюти в США класифікуються як власність.

Японія є світовим лідером в галузі інновацій і криптовалютної індустрії. Саме ця країна першою визнала, що криптовалюта біткоїн має ту ж функцію, що і гроші, тобто визнала біткоїн законним засобом платежу. Відповідно, уряд вирішив розробити нормативну базу для повноцінної інтеграції криптовалют в банківську

систему Японії. Регулювання відносин з криптовалютою здійснюється на національному рівні Агентством фінансових послуг Японії.

В той же час ряд країн ЄС демонструють повну нездатність адекватно і правильно реагувати на інновації та технічний прогрес. Європейський союз також зіткнувся з необхідністю створення відповідного юридичного регулювання, але не поспішає з його прийняттям. На даний час немає єдиного юридичного визначення криптовалюти (віртуальної валюти) і загального правового регулювання в ЄС, але деякі країни Європи визначили статус криптовалюти (віртуальної валюти) для цілей оподаткування.

Надання офіційного статусу криптовалюті, регулювання правовідносин щодо її обігу, зберігання, володіння, використання тощо та проведення криптовалютних операцій в Україні є необхідною передумовою розбудови нашої держави в сучасних умовах ринкової економіки.

У вересні 2017 року інтернет-спільноту сколихнуло повідомлення про те, що у Києві вперше у світі продали квартиру за криптовалюту Ethereum. Зазначена інформація була відображена на сторінці Facebook радника голови Державного агентства з питань електронного урядування України Костянтина Ярмоленка. Покупцем став засновник інтернет-видання TechCrunch Майкл Аррингтон. З аналізу правової природи договору стає зрозумілим, що насправді відбувся договір міни, а не купівлі-продажу, але при цьому є всі підстави вважати такий правочин законним.

Таким чином, підставно стверджувати, що на даному етапі існування інформаційних правовідносин в Україні правове регулювання таких об’єктів як криптовалюти відсутнє, вона не є законним засобом платежу, проте, виходячи із загальних засад диспозитивності приватно-правових відносин, може виступати предметом договору.

Протягом чотирьох останніх років єдиним актом основного фінансового регулятора країни, який в певній мірі вказував учасникам правовідносин на юридичний статус криптовалюти, був лист Національного банку України від 08 грудня 2014 року № 29-208/72889 щодо віднесення операцій з віртуальною валютою/криптовалютою Bitcoin до операцій з торгівлі іноземною валютою, а також наявності підстав для зарахування на поточний рахунок в іноземній валюті фізичної особи іноземної валюти, отриманої від продажу Bitcoin, НБУ вказав про те, що випуск віртуальної валюти Bitcoin не має будь-якого забезпечення та юридично зобов'язаних за нею осіб, не контролюється державними органами влади жодної із країн. Отже, Bitcoin є грошовим сурогатом, який не має забезпечення реальної вартості. Однак, 22.03.2018 Листом НБУ № 40-0006/16290 зазначений лист № 29-208/72889 визнано таким, що втратив актуальність, а нових роз’яснень НБУ ще не видавав.

Виходячи із визначення речі, що міститься в ст. 179 ЦК України, підставно визначити, що криптовалюта не є річчю, оскільки не має ознак матеріального

світу. Також криптовалюта не є продукцією в розумінні чинного цивільного законодавства.

Відповідно до ст. 3 Закону України «Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» майновими правами визнаються будь-які права, пов'язані з майном, відмінні від права власності, у тому числі права, які є складовими частинами права власності, а також інші специфічні права та права вимоги. Отже, за чинним законодавством криптовалюта не має ознак майнових прав.

Відповідно до ст. 99 Конституції України єдиною грошовою одиницею в Україні є гривня. Отже, до грошей криптовалюту віднести також не можна.

В свою чергу криптовалюти виконують одну із найважливіших функцій грошей – легкість обміну матеріальними цінностями.

Криптовалюта є одним з видів цифрової валюти, електронних грошей. Але на відміну від традиційних систем, де всі дані зберігаються на централізованому сервері, у більшості випадків криптовалюта є децентралізованою. Головною особливістю криптовалюти є те, що копії бази транзакцій лежать на комп'ютерах усіх учасників системи, і вони постійно між собою автоматично звіряються за спеціальними алгоритмами.

Оскільки криптовалюти вже визнані засобом обміну, тому в найближчий час обіг (обмін) і майнінг (видобуток) криптовалют стануть невід'ємною частиною ринкової економіки більшості розвинених країн світу.

Безумовно, проблематичним в правовому регулюванні зазначених відносин є складність з визначення криптовалюти як грошей, електронних грошей, фінансового активу, грошового сурогату або товару.

Процес внесення змін до законодавства України має відбуватись з урахуванням необхідності захисту прав споживачів, протидії відмиванню коштів та інших протиправних дій, ідентифікації суб’єктів операцій (фінансовий моніторинг), створення механізму оподаткування отриманих доходів в криптовалюті, декларування тощо.

Безумовно повноцінне введення в цивільний оборот криптовалют, як законного засобу здійснення платежів, можливе лише після проведення відповідних конституційних змін.

Отже, з урахуванням проведеного аналізу можливо прийти до висновку, що питання правового статусу криптовалют та законодавчого врегулювання операцій з ними має здійснюватися з урахуванням існуючих позицій в законодавстві України, інших країн та останніх тенденцій в розвитку крипто-технологій.

Законодавче врегулювання в жодному разі не повинно стати на заваді використанню та розвитку сучасних ІТ-технологій у фінансовому секторі та має стати потужним засобом залучення інвестицій.

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

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

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ ТА ЗАХИСТУ ПРАВА ВЛАСНОСТІ НА «РОЗУМНІ» РЕЧІ

Оскільки Інтернет речей складається з різноманітних компонентів, перш за все, виникає питання, що саме є об'єктом права власності у сфері Інтернету речей. Для визначення особливих об'єктів права власності у сфері IoT необхідно проаналізувати компоненти, що входять до складу системи IoT.

Усі компоненти зі структури Інтернету речей можуть бути зведені в просту формулу: фізичні об'єкти + контролери, сенсори, виконавчі механізми + Інтернет = IoT Ця формула чітко описує саму суть Інтернету речей. Екземпляр IoT складається з набору фізичних об'єктів, кожний з яких:

- містить мікроконтролер, що забезпечує інтелектуальність;
- містить датчик, що вимірює який-небудь фізичний параметр, та/або виконавчий механізм, що спрацьовує від якого-небудь фізичного параметра;
- має нагоду комунікації по Інтернету або якій-небудь іншій мережі.

Елементом, що не входить в цю формулу є спосіб ідентифікації окремої речі, звичайно званий тегом[1], тобто вона не охоплює простих елементів IoT першого рівня (таких, що ідентифікуються завдяки RFID-міткам).

Звичайно, об'єктами права власності у сфері Інтернету речей є ці самі фізичні об'єкти, оснащені додатковими датчиками та сенсорами, що надають цій речі можливості підключення до мережі або можливості взаємодії з іншими речами з використанням інших протоколів і тим самим перетворюють звичайну фізичну річ на «розумну». Тут необхідно звернути увагу на той факт, що права інтелектуальної власності на програмне забезпечення, завдяки якому забезпечується функціонал речі, залишаються за його розробниками, це сфера дії авторського права. Нагадаємо, що відповідно до ст. 419 ЦК України, право інтелектуальної власності та право власності на річ існують як самостійні правові категорії, передача кожного з цих прав є самостійним юридичним фактом, який породжує, змінює, припиняє самостійні правовідносини. Внаслідок цього перехід права власності на річ, у якій був зафіксований результат інтелектуальної, творчої діяльності, не означає переходу права на об'єкт права інтелектуальної власності, і навпаки.

Сьогодні перед власниками так званих «розумних» речей постає низка проблем, зокрема, це проблеми, пов'язані з невизначеністю правового статусу віртуальних речей у складі Інтернету речей, проблеми, пов'язані з необхідністю забезпечення безпеки персональних даних, з якими тісно пов'язані розумні речі тощо[2, с. 119-129]. Однією з таких проблем є проблема захисту прав власників розумних речей у випадках дистанційного втручання у діяльність розумних речей.

Наприклад, технічно може існувати можливість дистанційного відключення речі, що значно впливає на можливість реалізації правоможності користування такою річчю, оскільки маючи право на фізичну річ, власник позбавляється можливості використовувати її технологічний функціонал, заради якого, власне, і була придбана ця річ. Крім того, такі можливості дистанційного втручання в управління розумними речами можуть бути навіть небезпечними. Наприклад, відомим є випадок, коли внаслідок невнесення чергового внеску в рахунок погашення кредиту на оснащений «розумним» функціоналом автомобіль, він був дистанційно відключений менеджером у той час, коли власниця терміново везла у шпиталь свого сина. Звісно, така ситуація, навіть за умови, коли можливість дистанційного відключення речі передбачена договором, несе в собі значну небезпеку і повинні бути розроблені механізми взаємодії між власником речі та її виробником або особою, яка надає послуги, на такі випадки.

Представляється, що у випадках, коли здійсненню права власності на розумну річ дистанційно заважає особа без достатніх на те правових підстав, з метою захисту прав власника цілком допустимим є застосування класичного негаторного позову згідно зі ст. 391 ЦК України, відповідно до якої власник майна має право вимагати усунення перешкод у здійсненні ним права користування та розпоряджання своїм майном. Ситуація з дистанційним відключенням речі, позбавленням речі її функціоналу, або вчинення перепон для зв'язку фізичних та віртуальних елементів розумної речі, що має наслідком позбавлення власника можливостей використання речі відповідно до її призначення, є аналогічною фізичному втручанню у здійснення права власності.

Слід також зазначити, що у деяких випадках правоможності користування та розпорядження розумною річчю обмежується ліцензійною угодою. Така ситуація викликана тим, що більшість пристроїв IoT постачаються з вбудованим програмним забезпеченням, і без нього належно або взагалі не працюватимуть. Це забезпечення зазвичай ліцензується, а не продається. Пункти ліцензійної згоди можуть перешкоджати користувачам ремонтувати, змінювати чи перепродавати їхні пристрої.«Прив'язування» користувачів до одного бренда та одного постачальника може бути антиконкурентним заходом. Так, наприклад, вже кілька років американські фермери сперечаються з виробниками сільськогосподарської техніки, такими як John Deere, відстоюючи свої права ремонтувати трактори, які містять вбудоване програмне забезпечення.Фермерам було надано трирічне звільнення від виконання законів про авторське право в 2015 році. Проте John Deere продовжує боротися. У жовтні 2016 року компанія випустила нову ліцензійну угоду, яка забороняє майже всі модифікації програмного забезпечення на своїх тракторах. Це рішення є спробою переконатися, що всі ремонтні роботи виконуються підрядниками John Deere [3]. Видається, що такий підхід безпідставно обмежує права власників, неприпустимим є нав'язування споживачам правил поведінки стосовно їх речей, які відповідають інтересам виробника, це також одна з проблем IoT, яка потребує вирішення.

Ще одним відомим випадком порушень прав власників розумних речей є ситуація, коли компанія, що виробляла системи розумного будинку була придбана конкуруючою компанію і через деякий час остання повідомила власникам розумних будинків, придбаних раніше, про те, що їх підтримка більше не буде здійснюватись, системи будуть відключені. Тому у випадках придбання розумних речей особливу увагу потрібно звертати на обов'язки виробника або особи, що надає послуги, щодо технологічної підтримки функціонування таких систем, наслідків припинення юридичних осіб, які здійснюють таку підтримку тощо. Така ситуація повертає нас до питання про необхідність сертифікації IoT-продуктів, стандартизації та уніфікації форматів їх діяльності, що зможе забезпечити безперервність функціонування розумних речей навіть у випадку зміни їх виробників. Допомогти забезпечити права власників IoT-продуктів може також встановлення вимоги щодо поширення програмного забезпечення з відкритим кодом для IoT-продуктів, призначених для кінцевих споживачів.

Використана література:

1. Интернет вещей: сетевая архитектура и архитектура безопасности. – URL:http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/

2. Актуальні проблеми цивілістики у цифрову добу: монографія / за ред. Є.О. Харитонова, О.І. Харитонової; НУ «ОЮА». – Одесса: Юридична література, 2018. – 248 с. – (Серія: Цивілістика та «ІТ-право»).

3. Шість пунктів про інтернет речей, які споживачі повинні знати. – URL : http://tinker.uamper.com/news/shst-punktv-pro-nternet-rechey-yak-spozhivach-povinn-znati.html

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

Пильгун Н. В.,
доцент кафедритеоріїдержави та права,к.ю.н., доцент Навчально-наукового юридичного інституту Національного авіаційного університету
Яцун О. Д.,
студентка Навчально-наукового юридичного інституту Національного авіаційного університету

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Правове регулювання у сфері захисту персональних даних є досить актуальною проблемою на даний момент, оскільки сьогодні суспільство розуміє поняття «персональні дані» як найбільш важливу і не менш вразливу сферу суспільних відносин в Україні і за кордоном. Життєдіяльність людини є неможливою без надання інформації про себе як суспільству, так і державі. Особливо з впровадженням у різні сфери відносин новітніх інформаційних технологій, автоматизованих баз даних, що суттєво полегшують існування. З

іншого боку, існує велика загроза незаконного втручання в особисте життя людини і використання «приватних» даних особи. Тому право на захист персональних даних має бути одним із основних у сучасній державі.

Під правовим регулюванням захисту персональних даних необхідно розуміти те, що держава за допомогою права здійснює розвиток та охорону відносин у сфері захисту персональних даних. Основна роль у формуванні національної моделі механізму правового захисту персональних даних людини й громадянина розкривається через конституційні засади, що містяться у ст. 3, 28, 30, 31, 32, 34, 35, 41, 54, 55, 64 Конституції України та нормативно-правових актах Європейського Союзу. Правову основу забезпечення конфіденційності персональних даних складають Конституція України, Закони України «Про захист персональних даних», «Про інформацію», рішення Конституційного Суду України (далі – КСУ), кодифікаційні акти.

Реалізація норм Закону України «Про захист персональних даних» не завжди узгоджується з положеннями інших нормативних актів. Наприклад, однією з проблем, з якою зіткнулися розпорядники (фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця) персональних даних при їх реєстрації у Державному реєстрі баз персональних даних, це проблема визначення, які відомості належать до персональних даних, а які- ні.

Згідно ст. 11 Закону України «Про інформацію»від 02.10.1992 р. ,інформація про фізичну особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров‘я, а також адреса, дата і місце народження [1]. Відповідно до ст. 2 Закону «Про захист персональних даних» від 01.06.2010 р., персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована[2]. У роз‘ясненні Мінюсту «Деякі питання практичного застосування Закону України «Про захист персональних даних» від 21.12.2011 р. зазначено, що законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону до різноманітних ситуацій, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв’язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя [3].

Зі своєї сторони Конституційний Суд України, даючи офіційне тлумачення частин першої та другої статті 32 Конституції України, вважає, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні

переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [4].

Враховуючи зазначене вище, варто було б включити в Закон України «Про захист персональних даних» як нормативний акт, що містить спеціальні норми, невиключний перелік відомостей, які належать до персональних даних.

Так як наша країна впевнено крокує до Європейського Союзу, то не можна не зазначити про вплив його законодавства на українську систему законодавства про захист персональних даних. Законодавство більшості європейських держав поділяє персональні дані за критерієм їх «чутливості» на дані загального характеру (прізвище, ім'я, по батькові, дата і місце народження, громадянство, місце проживання) та «чутливі» або вразливі (інформація про стан здоров'я, етнічна належність, ставлення до релігії, ідентифікаційні коди чи номери, відбитки пальців, записи голосу, фотографії, дані про судимість тощо). Для чутливих персональних даних передбачається більш високий ступінь захисту. Зокрема, забороняється збирання, зберігання, використання та передавання без згоди суб'єкта даних саме чутливих, а не всіх без винятку персональних даних.

Необхідно відзначити важливість Регламенту 679, що набрав чинності 25.05.2018 р. і був предметом широкого обговорення в Україні. Це нормативний акт прямої дії, значний за обсягом документ, який детально визначає фактичну сферу його застосування, територіальну дію, основні принципи, пов'язані з обробкою персональних даних, його мету, термін набрання чинності тощо. Регламент 679 є обов'язковим у повному обсязі та підлягає прямому застосуванню у державах-членах ЄС. На думку багатьох вчених, європейські норми щодо захисту персональних даних та процедури їх обробки мають враховуватися в Україні, яка не є членом ЄС. Регламент 679 встановлює жорсткі норми, пов'язані з відповідальністю за дотримання законності обробки персональних даних та орієнтує на необхідність запровадження якомога більшого обсягу персональних даних, що підлягають захисту. Держави-члени ЄС мають внести зміни до національного законодавства як для гармонізації норм, так і для прийняття більш детальних правил.

Отже, можна зробити висновок,що в українській системі законодавства про захист персональних даних існує досить багато прогалин, що впливає безпосередньо на різні сфери суспільних відносин. Тому Україна має, враховуючи досвід Європейського Союзу, привести національне законодавство у відповідність

з міжнародними стандартами, створити систему незалежних адміністративних, правозастосовних, консультативних та наглядових органів, що забезпечуватимуть дотримання права на захист персональних даних як у приватній, так і в публічній сферах, бо нинішній стан захисту персональних даних українських громадян є незадовільним і загрозливим.

Використана література:

1. Про інформацію: Закон України від 02.10.1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

2. Про захист персональних даних: Закон України від 01.06.2010 р. // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

3. Деякі питання практичного застосування Закону України «Про захист персональних даних: Роз'яснення Мін'юсту» від 21.12.2011 р. / URL: http://zakon2.rada.gov.ua/laws/show/n0076323-1

4. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від О.В. Оніщенко 64 20.01.2012 р. / URL: http://zakon.rada.gov.ua/laws/show/v002p710-12

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

Заярний О. А.,
д.ю.н., доцент кафедри
адміністративного права
юридичний факультет Київського
національного університету
імені Тараса Шевченка,
Член Науково-консультативної ради
при Верховному Суді

ДЕЯКІ ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРАВОМІРНОЇ ОБРОБКИ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ У ПРОЦЕСІ ВИКОРИСТАННЯ ІНТЕРНЕТУ РЕЧЕЙ

В умовах інтенсивного розвитку інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій для оптимізації виробничих, побутових, управлінських процесів, одним із ключових елементів сучасної інформаційної інфраструктури поступово стає система Інтернету речей.

Разом з тим, як справедливо зазначається в юридичній літературі: «Технології Інтернету 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» [1, с. 85].

Серед персональних даних, що обробляються з використанням Інтернету речей значну частину складають біометричні дані. В цьому контексті перед юридичною наукою та правотворчою діяльністю актуалізується проблема щодо

розробки і практичної реалізації механізму правового забезпечення правомірної обробки біометричних персональних даних у процесі використання Інтернету речей.

Слід підкреслити, порушена у цій роботі проблематика була предметом наукового інтересу окремих вчених-правників, зокрема: В. В. Архіпова, О. А. Баранова, В. М. Брижка, С. Грингарда, Е. Гудмэн, О. Джанджакомо, Р. Каміллі, Дж. Кассано, К. Росе, С. Чена, та інших.

Разом з тим, прийняття у новій редакції у 2018 році Страсбурзької Конвенції Про захист фізичної особи у зв'язку з автоматизованою обробкою персональних даних [2]та Загального регламенту захисту даних (GDPR) [3], не вирішило в повній мірі проблему належного правового забезпечення правомірного обігу біометричних даних при використанні Інтернету речей.

Метою цієї роботи є вироблення критеріїв правомірності збирання, зберігання, обробки та використання біометричних персональних даних фізичної особи у зв'язку з використанням або створенням Інтернету речей.

Предмет дослідження складають передбачені в нормах національного та міжнародного законодавства умови та процедури правомірної обробки персональних даних фізичної особи при створенні або використанні Інтернету Речей.

Традиційно, у науковій літературі з кібернетики поняття «Інтернет речі» визначається як: «мережа різних об'єктів, що росте, – від промислових пристроїв до споживацьких товарів, які можуть обмінюватися інформацією і виконувати свої задачі, 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» [4, с. 6].

З наведеного визначення сутності «Інтернет речей» слідує, що основоположними інструментами для організації взаємодії цих об'єктів виступають як сама інформація, так, і технології її обробки.

При цьому, така інформація може бути згенерована як самими Інтернет речами, так, і внесена їх розробниками, власниками, або споживачами.

З урахуванням запропонованого у ст. 2 Страсбурзької Конвенції [3] визначення персональних даних можна припустити, що саме цей вид інформації безпосередньо вноситься власниками, розробниками чи споживачами Інтернету речей з метою їх подальшого використання, вилучення необхідної користі від їх експлуатації, ідентифікації та авторизації в системі, визначення власних потреб, що підлягають задоволенню тощо.

Від так, первинним критерієм забезпечення правомірного обігу персональних даних при використанні Інтернету речей є перед усім мета їх обробки та цілі застосування самих Інтернету речей.

Виходячи із системного тлумачення положень ст. 5 Страсбурзької Конвенції [3] та ст. 8 Європейської Конвенції про захист прав людини

таосновоположних свобод [4], мета обробки персональних даних має бути заздалегідь визначеною власником та/розробником конкретних Інтернет речей, передбачати мінімально необхідну межу збирання та обробки відповідних даних, бути заздалегідь відомою для споживачів відповідних технологій, а також не передбачати юридичну можливість передачі персональних даних третім особам без попередньої, недвозначної згоди їх володільця. Для практичної реалізації окресленого критерія важливою умовою є необхідність закріплення в умовах договорів на використання та технічних регламентах експлуатації Інтернету речей обов'язків розробників та/або власників цих об'єктів прямої заборони на збирання, зберігання та використання біометричних персональних даних для цілей, пов'язаних з відстежуванням фізичних, фізіологічних чи будь-яких інших біологічних змін суб'єктів персональних даних, крім випадків, якщо це безпосередньо випливає з функціонального призначення самих Інтернет речей. В останньому випадку може йтися про медичне обладнання та системи «Електронний лікар», пристрої для зберігання і приготування продуктів харчування, технології контролю здоров'я стану спортсменів тощо.

Інший критерій оцінки правомірності застосування біометричних персональних даних власників та споживачів Інтернету речей випливає із самої юридичної сутності відповідної категорії персональних даних.

Згідно з легальним визначенням біометричних персональних даних, наведеним у Загальному регламенті захисту даних (GDPR) [5] -- це особисті дані, отримані внаслідок специфічної технічної обробки, що стосуються фізичних, фізіологічних чи поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи, такі як зображення обличчя особи чи дактилоскопічні (відбитки пальців) дані.

Розвиток наведеного визначення в аспекті створення та використання Інтернету речей дає підстави констатувати, що використання біометричних персональних даних на практиці перед усім відбувається в цілях безпосередньої ідентифікації фізичної особи, її авторизації чи оцінки фізичного, фізіологічного, або психічного стану. Від так, в межах правомірної обробки біометричних персональних даних перебуває не лише кібернетична безпека самих Інтернет речей, але і безпека цих даних, а також інших видів інформації, згенерованих за їх допомогою.

Водночас, здатність біометричних персональних даних до глибокої ідентифікації їх володільців, відображення чутливих біологічних змін у їх організмі накладає на суб'єктів правовідносин, пов'язаних з використанням Інтернету речей окремих додаткових обов'язків. Йдеться про необхідність встановлення в нормах національного законодавства технічних регламентах та умовах договорів про експлуатацію Інтернету речей зобов'язань власників та розробників заборон на використання біометричних персональних даних для цілей, не пов'язаних з ідентифікацією самого володільця відповідних даних або

надання йому послуг, безпосередньо заснованих на використанні біометричних персональних даних.

При цьому, на наш погляд, важливими складовими правового забезпечення правомірної обробки біометричних персональних даних є строковість їх застосування (протягом надання конкретної послуги або в період проведення ідентифікації особи), неможливість використання таких даних в маркетингових чи будь-яких інших комерційних цілях без згоди володільця персональних даних, а також встановлення заборони на дублюванню біометричних даних в цілях паралельного використання іншими, незалежними Інтернет речами.

Таким чином, на сьогоднішній день забезпечення правомірної обробки біометричних персональних даних ґрунтується на законодавчому та/або договірному визначенні мінімально допустимої мети збирання, зберігання та використання цих даних, встановленні прямих заборон на їх дублювання незалежними від первинної речами, а також на обмеженнях використання маркетингових цілях.

Безпосередній зв'язок зазначених критеріїв з умовами забезпечення кібернетичної безпеки Інтернету речей вказує на необхідність встановлення додаткових нормативних вимог щодо технічного захисту біометричних персональних даних при проектуванні, використанні та знищенні Інтернету речей. Важливим кроком в удосконаленні механізму правового забезпечення правомірної обробки біометричних персональних даних є розробка та прийняття порядку обробки та технічного захисту біометричних персональних даних власників та споживачів інтернету речей. Прийняття зазначеного нормативно-правового акту дозволить не лише встановити спеціальні (більш жорсткі) умови обігу біометричних персональних даних, але і буде сприяти їх правомірній обробці, забезпеченню кібернетичної безпеки Інтернету речей загалом.

Використана література:

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. Страсбурзька Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 [телектронний ресурс]: р. URL: http://conventions.coe.int/Treaty/EN/Treaties/PDF/Ukrainian/108-Ukrainian.pdf.

3. Regulation (eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natu- ral persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC/ European Union; Regulation, International document of 24.04.2016 № 2016/679/ — URL: https://gdpr-info.eu.

4. Сэмюэл Грингард. Интернет вещей: будущее уже здесь. / Сэмюэл Грингард. – изд. МАН Иванов и Ферберг. М. – 2016. – 381 с.

5. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р., ратифікована Законом України „Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 р., Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції" № 475/97-ВР від 17 липня 1997р. Відомості Верховної Ради України. 1997. № 40. Ст. 263.

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

Каньовський Р. А.,
студент магістратури юридичного факультету Київського національного університету імені Тараса Шевченка

СИСТЕМА СОЦІАЛЬНОГО РЕЙТИНГУ В КНР: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ

Суспільство завжди шукало ефективних способів для встановлення належного правопорядку. Такими механізмами виступали державний примус, релігія, норми суспільної моралі, які використовували принципи заохочення порядних осіб та жорсткого осуду порушників.

Сучасний рівень розвитку технологій, зокрема інтернету речей (англ. Internet of Things), штучного інтелекту (англ. Artifical Inteligence), великих даних (англ. BigData) вже сьогодні дозволяє вивести контроль за порядністю громадян на принципово новий рівень.

Піонером в даній сфері є Китай, де 14 липня 2014 року було прийнято Програму «Про планування будівництва системи соціального кредиту (2014-2020 рр.)». Основна мета, і це прямим текстом вказується в Програмі, щоб "ті, хто виправдав довіру, користувалися всіма благами, а ті, хто втратив довіру, не могли зробити ні кроку"[1].

У згаданій Системі соціального кредиту (рейтингу) (далі: ССК) все пов’язано з так званою благонадійністю (англ. trustworthiness). Умовою для оцінки благонадійності є рейтинг особи, який залежить від таких показників, як чесність у державних справах, комерційна цілісність, громадська цілісність, судова достовірність.

Схематично система працює наступним чином: особі присвоюється певний початковий рейтинг, наприклад 1000 балів. Далі визначаються види діяльності (вчинки), за які передбачається зниження чи підвищення рейтингу на певну кількість балів. Якщо рейтинг більше 1050 балів, то це зразковий громадянин і маркується трьома буквами А; з тисячею балів можна розраховувати на АА; дев’ятистами - на В; якщо рейтинг впав нижче 849 - це вже підозрілий носій рейтингу С. А тих, у кого 599 балів і нижче, записують в чорний список з приписку D, вони стають вигнанцями суспільства.

Від розміру рейтингу і залежить наступне становище особи в соціумі та доступ до певних благ: отримавши штраф за порушення ПДР, можна втратити 5 балів; водіння за кермом в нетверезому стані знижує рейтинг відразу до рівня С; зниження рейтингу спричинить і надмірно проведений час за відеоіграми, систематичні покупки алкогольних напоїв, невиконання судових рішень, неприхильні висловлювання про діяльність уряду та навіть спілкування з особами категорії D. З іншого боку, наприклад, за здійснення героїчного вчинку, ведення чесного бізнесу або допомогу родині в надзвичайних складних обставинах, можна збільшити рейтинг на 30 балів. А також можна заробити кредит, пожертвувавши

на благодійність або добровільну участь у програмі міста. Людина з рівнем ААА отримує у винагороду такі пільги, як можливість взяти на прокат громадські велосипеди без сплати депозиту та безкоштовно кататися на них; отримувати пільги на опалювання взимку та більш вигідні умови для банківських кредитів[2].

Також рейтинг впливає і на такі сфери, як доступність навчання та стипендій, доступу до готелів вищого класу, поїздок закордон, розмірів страхових премій, доступності соціальних послуг, тощо. До особливих санкцій щодо неблагонадійних варто віднести оприлюднення т.зв. «чорних списків» неблагонадійних громадян.

Тобто, ССК вже сьогодні претендує на широке розповсюдження в різноманітних аспектах життя. Технічні можливості, зокрема активне розповсюдження технологій Інтернету речей в повсякденне життя, також сприяють цьому. Доступ до місцезнаходження, всеохоплююче відеоспостереження, історії пошуків браузера, споживацькі інтереси користувачів, і навіть матеріали приватних бесід - всі ці персональні дані становлять неабиякий інтерес для держави у її прагненні створити повноцінне портфоліо на кожну особу. Причому доступ до персональних даних є прямо пропорційним до ефективності системи соціального кредиту як засобу забезпечення транспарентності та суспільної довіри – чим більше інформації є в розпорядженні, тим правдоподібніший профіль особи.

З правової точки зору важливо з’ясувати, яким чином в умовах ССК захищені персональні дані. Для цього слід дослідити три критерії: принцип збору даних, принцип використання даних, та право суб'єктів даних на доступ та корегування власних даних.

Більшість аспектів функціонування ССК в Китаї на загальнодержавному рівні нормативно врегульовані досить погано. Ця умова дозволяє наділяти місцеві органи влади широкими дискреційними повноваженнями у вирішенні таких питань.Незважаючи на прийняття Закону про Кібербезпеку в 2016 році стосовно онлайн - даних, посилення цивільно-правового захисту даних споживачів у 2013 році та криміналізації незаконного збору, отримання та продажу персональних даних у 2009 році, персональні дані як загальний предмет ще чітко не визначені та ефективно не захищені [3, ст.357].

При зборі персональних даних, за загальним правилом, повинна бути чітко окреслена мета такого збору, і в межах якої допускається використання даних. Однак, і загальнодержавні акти КНР, і локальні акти цю мету визначають дуже розпливчасто, вона може відрізнятися від цілей, для яких ці записи спочатку були створені державною установою та зібрані від приватних осіб [3, ст. 365].

Згода суб’єктів на отримання інформації для цілей ССК, передачу їх від розпорядників такої інформації до відповідних платформ за законодавством не потрібна, що теж можна вважати суттєвим недоліком [3, ст.365].

В КНР на сьогодні не існує уніфікованої системи персональних даних та єдиної відповідальної установи. Такі повноваження розподілені між державними

структурами та приватними компаніями, такими як Alibabaз його SesameCredit, Tencent та його месенджер WeChat. Можливості обміну приватною інформацією між цими учасниками та межі використання такої інформації лежить поза контролем суб'єкта такої інформації [3, ст.369].

З 1 травня 2018 року починає діяти нова інструкція щодо захисту персональних даних в КНР. Це важлива спроба перевірити здатність компаній збирати, обробляти та розповсюджувати персональні дані. Документ містить детальні вимоги для згоди користувача, включаючи вимоги щодо де-ідентифікації даних, якщо користувачі не погоджуються на обмін даними. Дані в широкому розумінні вважаються "чутливою особистою інформацією", і необхідна явна згода користувачів перед тим, як компанії можуть обробляти їх. Інструкція також накладає суворі обмеження"Вторинне використання" даних поза первісною метою [4].

Ефективність впровадження таких нововведень на сьогодні не досліджена, однак можна припустити, що правляча партія навряд чи допустить ефективний захист персональних даних приватними особами, якщо це загрожуватиме Системі соціального рейтингу.

В цілому ж, система соціального кредиту в КНР за 4 роки свого існування показала як позитивні так і негативні свої сторони. Позитивними можна вважати загальне зростання порядності громадян, можливість відслідковувати та активно запобігати злочинам, відчуття безпеки та стабільності кожного члена соціуму. До недоліків системи варто віднести втручання в приватне життя; тотальний контроль за діями та навіть думками населення; ризики пов'язані із кібербезпекою такого роду даних; неточності при виявленні порушників; можливість звуження прав за політичними мотивами, і часта непропорційність таких позбавлень.

Особливості китайської культури та філософії протягом століть створювали підґрунтя для існування різних прототипів системи масового контролю. Проте схожа до існуючої сьогодні в Китаї ССК вже довгий час існує в США. Щоправда, там вона носить характер приватних ініціатив. Так, оцінка FICO (кредитне бюро) впливає на те, як швидко особа потрапляє на літак (і чи взагалі потрапить), а рейтинги соціальних мереж від Facebook або комерційних "репутаційних" сайтів впливають на те, чи отримає людина роботу. Але в США це поки не носить загальнодержавного тотального характеру, а персональні дані, попри періодичні скандали із неправомірним їх використанням IT-гігантами, там захищаються з усією суворістю закону [5].

Якщо говорити про потенціал впровадження ССК в країнах Заходу загалом, деякі вчені не виключають такої можливості в майбутньому. Професор історії з Дартмутського коледжу Памелла Кайл Крослі вважає, що китайська модель контролю за суспільством, яку багато хто вважає тоталітарною, з часом встановиться і в демократичних країнах: «Різниця лиш в тому, що китайське суспільство більш підготовлене до інтеграції комерційних, військових та правоохоронних даних. В результаті китайці ретельніше контролюють шляхом

залякування та самоцензури, ніж будуть контролювати американців протягом ще кількох десятиліть » [5].

В українському аспекті для вирішення питання про перспективи впровадження системи соціального кредиту слід розглянути в наступному ключі. Згідно з останнім опитуванням Центру Разумкова від червня 2018 року, українці категорично не довіряють державним та більшості громадських інституцій. Найбільшою довірою користуються церква та волонтерські організації [6].

Можливо, саме зараз ми вступили в період, коли зможемо використати всі найкращі технічні рішення для побудови більш ефективного суспільного механізму, всі деталі якого працюють злагоджено та який об'єднаний спільними ідеями взаємодовіри. При цьому у вершині кута мають залишатися права людини, і мають враховуватися перестороги, проголошені такими умами, як Оруел, Гакслі, Бредбері, Азимов, та інші.

Використана література:

1. Planning Outline for the Construction of a Social Credit System (2014-2020) URL: https://chinacopyrightandmedia. wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/.
2. S. MISTREANU. LifeInside China's Social Credit Laboratory URL: https://foreignpolicy.com/2018/ 04/03/life-inside-chinas-social-credit-laboratory/.
3. Chen, Yongxiand Cheung, Anne S. Y. The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislationon the Social Credit System [Електронний ресурс] Vol. 12, No. 2, The Journal of Comparative Law (2017) 356-378; University of Hong Kong Faculty of Law Research Paper No. 2017/011 – URL: https://ssrn.com/abstract=2992537 or http://dx.doi.org/10.2139/ssrn.2992537.
4. M. Chorzempa, P. Triolo, S. Sacks. China's Social Credit System: A Mark of Progressor a Threat to Privacy? [Електронний ресурс] Policy Brief 18-14 URL: https://piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy.
5. What Could China's 'Social Credit System' Meanforits Citizens? URL: https://foreignpolicy.com/2016/08/15/what-could-chinas-social-credit-system-mean-for-its-citizens/.
6. Довіра громадян України до суспільних інститутів URL: http://razumkov.org.ua/uploads/socio/2018_06_ press_release_ua.pdf.

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

Самчинська О.А.
студент ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Фурашев В.М.
к.т.н., доцент, с.н.с.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК ІНСТРУМЕНТ ЗАПОБІГАННЮ МАНІПУЛЯЦІЙ СУСПІЛЬНОЮ СВІДОМІСТЮ

Напевно ніхто просто не уявляє собі повсякденне життя без Інтернету. Сьогодні практично усі процеси життєдіяльності людини перемістилися у

віртуальний простір. За допомогою Всесвітньої мережі щоденно ми спілкуємось з друзями і колегами, користуємося послугами таксі та інтернет-банкінгу, здійснюємо покупки, оплачуємо комунальні послуги, замовляємо їжу і це далеко невичерпний можливостей, які надає нам Інтернет.

Всі ці дії ми виконуємо з легкістю, просто надавши згоду на доступ до нашого місцезнаходження, до камери, контактів та іншої інформації про нас та про наше життя. Однак, мало хто із нас задумується, до чого в майбутньому може призвести така собі необдумане та легке натиснення на «згоден».

Напевно, у кожного з нас була ситуація, коли ми вподобували запис у Фейсбуці і практично через невеликий проміжок часу нам пропонувались записи зі схожим контентом. Або коли ми авторизувались на тому чи іншому сайті і після цього регулярно отримували повідомлення з різноманітними акціями та спеціальними пропозиціями.

З одного боку, це дуже зручно, думаємо ми, що Гугл практично завжди знає де ми, чого ми хочемо та що нам запропонувати саме в цей момент часу, а з іншого, реклама настільки настирлива, що нерідко приносить нам дискомфорт та роздратування.

Сьогодні, згода на обробку персональних даних, яку кожен з нас хоча б раз надавав, стала фундаментом побудови бізнесу і досить ефективним інструментом маніпуляції свідомістю громадян.

В умовах правової несвідомості громадян, необережне ставлення до згоди на оброблення та поширення персональних даних має наслідком маніпулювання свідомістю, поширення шахрайства та вчинення інших злочинів. Саме тому важливим питанням, яке підлягає правовому регулюванню є захист персональних даних громадян.

Проблема захисту персональних даних притаманна не тільки для нашої держави, вона є глобальною. Саме тому в 2016 році Європарламент прийняв Загальний регламент Європейського Союзу про захист персональних даних.

Цей документ був спрямований на врегулювання проблеми з якою зіткнулася уся світова спільнота. Основними положеннями Регламенту стало, по – перше, виділення категорії «sensitive personal data», до якої належать дані про релігійну, расову, етнічну приналежність, біометричні дані, дані про філософські погляди, тобто ті дані, використання яких може стати інструментом для впливу та маніпуляцій. Для даної перебачений особливий, більш суворий, режим збирання, обробки та поширення.

По – друге, даним документом було передбачено «право на забуття», яке полягало в можливості суб’єкта персональних даних заборонити використовувати та мусити видалити свої персональні дані. Всі положення даного Регламенту були спрямовані на створення якнайпрозорішої процедури збирання та обробки персональних даних, а також на надійний їх захист від використання в цілях маніпуляцій.

Не можна не розглянути практику Естонії, де захист персональних даних здійснюється досить на високому рівні. Кожен громадянин держави має ідентифікаційні карти, які слугують не лише для встановлення особи, а й містять досить велике коло інформації для здійснення різноманітних операцій, зокрема фінансових. Всі дані, які вміщені у ці ідентифікаційні картки зберігаються у спеціальній базі до якої мають доступ лише правоохоронні органи та спеціальні особи. Крім того, кожен громадянин може зайти у цю базу даних та дізнатися хто саме цікавився їх даними та з якою метою і у разі необґрунтованості зацікавлення їх даними отримати відповідний захист.

Що стосується України, то наша держава не так давно почала запроваджувати політику захисту прав громадян в інтернеті, зокрема, питань персональних даних. Основними документами у цій сфері є Закон України «Про захист персональних даних» та Закон України «Про основні засади забезпечення кібербезпеки України». Однак, що стосується закону про основні засади кібербезпеки, то його положення спрямовані на захист інтересі держави та суспільства в кіберпросторі. Закон про захист персональних даних теж не передбачає всіх аспектів, які потребують регулюванню.

В нашій державі здійснюються заходи щодо захисту персональних даних громадян. Однак, враховуючи сучасний рівень технологій, цього недостатньо. Тому для ефективного врегулювання даного питання та запобігання різноманітних маніпуляцій свідомістю потрібно, насамперед, спрямувати всі заходу на розвиток правової культури та свідомості громадян та на застосування практики іноземних держав.

Використана література:

1. Закон України «Про захист персональних даних» – URL: http://zakon.rada.gov.ua/laws/show/2297-17.
2. Закон України «Про основні засади забезпечення кібербезпеки України». – URL: http://zakon.rada.gov.ua/laws/ show/2163-19.
3. Захист особистих та персональних даних в інтернеті: проблеми законодавчого врегулювання. – URL: http://ukrainepravo.com/scientific-thought/legal_analyst/zakhist-osobistikh-ta-personalnikh-danikh-v-interneti-problemi-zakonodavchogo-vregulyuvannya/

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

Неділько Я. В.,
студент 2 курсу юридичного факультету Київського національного університету імені Тараса Шевченка

ПОНЯТТЯ КІБЕРЗЛОЧИНУ ТА ОСОБЛИВОСТІ ЙОГО ЗАКРІПЛЕННЯ В НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ

Стрімкий розвиток інформаційно-комунікаційних технологій надає безпрецедентні можливості доступу до інформації, індивідуального та колективного її використання, взаємного обміну, а також впливає на всі сфери

суспільного життя. Сьогодні не можливо уявити суспільство, яке б не використовувало сучасні інформаційні технології.

У проголошеній резолюцією 3384 (XXX) Генеральної Асамблеї ООН від 10 листопада 1975 року Декларації про використання науково-технічного прогресу в інтересах миру і для добробуту людства наголошується, що всі держави повинні сприяти міжнародному співробітництву з метою використання результатів науково-технічного прогресу в інтересах міжнародного миру і безпеки, свободи і незалежності, економічного і соціального розвитку народів та забезпечення прав і основних свобод людини у відповідності до Загальної декларації прав людини та інших міжнародних документів [1].

Позитивні результати інформатизації супроводжуються і низкою негативних проявів. Формування цієї сфери діяльності людини зумовило виникнення нового виду правопорушень, пов'язаних з використанням комп'ютерних систем та інформаційних технологій. Частина з цих правопорушень сягає такого рівня суспільної небезпечності, що спричинило визнання їх злочинними та включення в коло заборонених кримінальним законодавством діянь. Нині в особливій частині Кримінального кодексу України міститься цілий розділ, в якому передбачено кримінальну відповідальність за злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (комп'ютерні злочини). Протидія комп'ютерним злочинам в сучасній Україні постає одним з першочергових завдань.

В національному законодавстві України, поняття кіберзлочину є новим. Ратифікувавши в 2005 році Конвенцію про кіберзлочинність, Україна не вирішила головного питання – визначення поняття кіберзлочину та закріплення його на нормативному рівні.

В юридичній науці, багато вчених давали визначення поняття кіберзлочину по різному. Як зазначає А. Важеніна, кіберзлочин становить собою навмисні винні дії, вчинені за допомогою комп'ютерної системи чи мережі, у рамках комп'ютерної системи чи мережі, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, їхніх мереж і комп'ютерних даних, що спричинили істотне порушення прав і охоронюваних законом інтересів особи, суспільства і держави [2]. На думку Н.М. Ахтирської, кіберзлочин – це кримінальне правопорушення, яке вчиняється з використанням комп'ютерної техніки (комп'ютерів, пристроїв та іншого обладнення), інформаційних технологій, комп'ютерних систем та мереж з порушенням встановленого законом порядку інформаційної безпеки, незалежно від предмету посягання та сфери застосування [3]. Як стверджують М. Погорецький та В. Шеломенцев, дане визначення потрібно розглядати у широкому та вузькому розумінні. У широкому розумінні кіберзлочин (кібернетичні злочини) пропонується розглядати як кримінальні посягання, об'єктивна сторона яких відбувається у кіберпросторі, а об'єктом посягання є суспільні відносини у різноманітних сферах людської

діяльності, пов’язані з використанням ресурсів кіберпростору. У вузькому розумінні під кіберзлочинами пропонується розуміти кримінальні посягання з використанням кіберпростору на відносини керування певними процесами, пов’язаними з використанням комп’ютерних систем [4].

Водночас, в правовому полі, зокрема у Законі України «Про основні засади забезпечення кібербезпеки України» (2017 р.), термін кіберзлочин (комп’ютерний злочин) визначається 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 [5].

На нашу думку, дане твердження не зовсім розкриває поняття кіберзлочину. Оскільки, однією з головних ознак кіберзлочину, є вчинення даного злочину за допомогою комп’ютерної техніки та інших електронних приладів, які мають змогу вільного доступу до кіберпростіру. Загалом, зазначене визначення є надто спрощеним та не повною мірою відображає його кримінально-правовий характер, а також теоретичні здобутки юридичної науки, що наводилися вище.

Враховуючи викладене пропонується удосконалити зазначену дефініцію та розуміти кіберзлочин (комп’ютерний злочин) як суспільно небезпечне винне діяння у кіберпросторі, яке вчиняється за допомогою комп’ютерної техніки та інших електронних приладів, які мають доступ до кіберпростіру, та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або визнано злочином міжнародними договорами України. Саме таке визначення має бути закріплене і в законі України про кримінальну відповідальність.

Використана література:

1. Декларація про використання науково-технічного прогресу в інтересах миру і для добробуту людства: Резолюція 3384 (XXX) Генеральної Асамблеї ООН від 10 листопада 1975 року URL: https://undocs.org/ru/A/RES/3384(XXX)

2. Важенин А.Г. Интернет и преступность: криминологические и правовые аспекты взаимосвязи URL: http://www.crime.vl.ru/index.php?p=1007&print=1&more=1

3. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів : навч. Посіб. / Н.М. Ахтирська. – К. : ВПЦ «Київський університет» , 2018. – 229 с.

4. Погорецький М. Кіберзлочини: до визначення поняття / М. Погорецький, В. Шеломенцев // Вісник прокуратури. – 2012. – № 8. – С. 89–96.

5. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року URL: http://zakon.rada.gov.ua/laws/show/2163-19.

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

Щербак Д. С.,
Студентка 6 курсу ННІПП НУ
«Львівська політехніка»
Науковий керівник: ***Радейко Р. І.***
к.ю.н., асистент кафедри адміністративного та інформаційного права ННІПП

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ В КРИМІНАЛЬНОМУ СУДОЧИНСТВІ

Використання web-технологій у рамках здійснення кримінального правосуддя покращить обмін інформацією та здійснення захисту. Є потреба в розробці загальних схем записів та каталогізації злочинної історії, створенні можливостей перекладу мови в режимі реального часу та дисплеїв («інформаційних панелей») для задоволення вимог посадових осіб, динамічних інформаційних потреб.

Laura J. Moriarty в праці «Criminal justice technology in the 21st century: third edition» зазначає, що основними потребами сьогодення є:

1) в кримінальному правозастосуванні – політика процедури використання безпілотних і автоматизованих транспортних засобів; віртуальний каталог судимості; біомедичні датчики для посадових осіб; розпізнавання посадових осіб у безпосередній близькості; покращення відстеження посадових осіб у будівлях;

2) в кримінальному судочинстві – відео зв'язок з виправними закладами; контрольний список закупівель інформаційних технологій судів; високошвидкісні підключення до Інтернету для судів; віртуальні зали суду; навчальні матеріали з ключових веб-технологій [1, с. 27].

John S. Hollywood, Dulani Woods, Richard Silberglitt, Brian A. Jackson виокремлюють три основні дискусійні блоки, щодо проблем застосування Інтернету речей (Internet of things, далі IoT) в кримінальному судочинстві.

1) використання технології IoT для покращення обміну інформацією передбачає: інтерпретацію мови в режимі реального часу; створення каталогу віртуальних злочинів; технологічну інфраструктуру для інтерфейсів кримінального правосуддя; інструменти для підвищення якості та цілісності даних; поліпшення обміну інформацією про правопорушників з третіми сторонами (зацікавленими особами); кращий доступ до даних для ідентифікації осіб; дослідження перевантаження інформацією; демонстрація обстановки та картографічних показників, розроблених для окремих посадових осіб [2, с. 10].

Використання IoT полегшує пошук даних історії про кримінальні справи через ряд спеціально створених систем. Знаходження потрібного запису також буде простішим, оскільки посадовець зможе спеціально шукати інформацію про особу – ім'я, адресу, шрами/знаки/татуювання або будь-які інші дані. Складання кримінальної історії стане доступнішим, оскільки майже все це буде частиною одного документального запису, можливо, з посиланнями на відповідну інформацію (фотографії, докладні звіти про конкретні інциденти тощо). Нарешті,

спроститься пошук та перегляд пов’язаної інформації, оскільки така інформація буде виражена в термінах зв’язаних текстових документів [2, с. 12].

2) покращення практичних навиків у web-технологіях – друга з найважливіших проблем сьогодення в кримінальному судочинстві. Зокрема тут виділяють необхідність в навчальних матеріалах з ключових web-технологій; в коштах для придбання технології IoT; розроблення політики та процедури використання для IoT, Semantic Web (напрямок розвитку Всесвітньої павутини, що дозволяє машинам не тільки відображати інформацію в інтернеті, але і розуміти її сенс) та безпілотних, автоматизованих транспортних засобів (більш затребувана в діяльності правоохоронних органів) [2, с. 14].

3) розвиток інфраструктури. Існує необхідність у забезпеченні відео зв’язку з виправними установами, для того, щоб зацікавлені сторони корегували виправлення ув’язнених та могли зустрічатися з ними до їх звільнення від відбування покарання.

У 2014 році в Управлінні з питань науки та технологій Адміністрації Президента США відбувся семінар з використання технологій для покращення адаптації в’язнів. Однією з основних тем дискусії на семінарі було використання дистанційних технологій навчання для надання освітніх послуг ув’язненим. Обговорювані технології та інфраструктура можуть проводитись включенням телеконференцій з незалежними пробаційними та службовими особами, постачальниками послуг.

У місцевостях, де відсутнє високошвидкісне з’єднання (наприклад, у сільській місцевості) або мобільні комунікаційні пакети до залів для судів, можна створити віртуальні зали суду, якщо постачатиметься високошвидкісний Інтернет, тому що більша частина витрат для створення залів судів та пов’язаних з ними витрат зникнуть [2, с. 15].

Для того, щоб визначити, чи знаходиться особа в небезпеці, можна носити датчик, прикріплений до її одягу. Ці пристрої відчувають серцебиття та температуру власника тіла. Однак точність емоцій може бути неоднозначною. Наприклад, серцебиття здивованої людини може бути ідентичним серцебиттю людини, яка знаходиться в небезпеці. Таким чином, для підвищення точності виявлення емоцій, необхідний контроль через камери відеоспостереження.

Корейські дослідники Jeong-Yong Byun, Aziz Nasridinov запрограмували застосування камери відеоспостереження для розпізнавання понад 36 емоційних станів особи. Для того, щоб розкрити злочин у режимі реального часу, застосовується алгоритм k-means. K – середній алгоритм кластерів Сеульських районів на k-груп, так що це загальна відстань між членами групи та її відповідним центром. Після викриття злочину повідомляються відповідні сторони, такі як поліція, департамент надзвичайних ситуацій та батьки. Зареєстровані в базі даних злочини візуалізуються через web-геоінформаційну систему. Вона має корисні функції не лише для поліцейських установ, але і для

звичайних користувачів. Наприклад, вона видає попереджувальне повідомлення про потенційний ризик, коли особа входить до небезпечного місця.

Аналізуючи дані злочинів за допомогою алгоритмів машинного навчання, можна виявити значущі моделі та тенденції у сфері інформаційних технологій, які будуть ефективними для поліцейських установ та громадян [3, с. 752].

Правоохоронні органи готуються до проведення обшуків у місцях вчинення злочинів із застосуванням новітніх технологій, таких як IoT, а також оброблення цифрових доказів. Ігрові приставки, пристрої Echo (управляються за допомогою голосу та реагують на ім'я «Алекс», після чого мова користувача записується і відправляється в «хмару» для аналізу і реакції) і навіть Fitbits (фітнес-трекери, а також «розумні» Wi-Fi-ваги) забезпечили цінну інформацію, щоб допомогти розкрити злочини. Більшість людей не розуміють принципів роботи цих пристроїв, тому вміло використовуючи дані технології, правоохоронні органи легше розпізнаватимуть неправдиві показання, алібі осіб. Оскільки залежність від використання цифрових пристроїв продовжує зростати – годинники, телефони, телевізори, кардіостимулятори та інші – дають більше можливостей для слідчих, які аналізують дані пристроїв при розслідуванні злочину.

Доступною є технологія оснащення автомобіля GPS-обладнанням, яке за допомогою пульта дистанційного керування можна контролювати та закріплювати на задній панелі автомобіля потенційного злочинця. Це дозволить в короткі терміни дізнаватись, де знаходиться підозрюваний, і запобігати небезпечним переслідуванням автомобілів. Розроблені інтелектуальні датчики, які можна закріпити зсередини офіцерського знаряддя, щоб стежити за тим, як використовується пістолет. Ця інформація може виявитися корисною у кримінальних справах [4].

Вважаємо, що застосування IoT в кримінальному судочинстві допоможе комплексно розглядати кримінальну ситуацію, не витрачаючи часу на пошуки, акумуляцію та систематизацію інформації, необхідної для аналізу і розкриття злочину. Також дана технологія в умовах фінансової кризи може суттєво зменшити видатки на функціонування системи кримінального судочинства, звести до мінімуму ризики, які виникають при виконанні посадовими особами своїх обов'язків.

Використана література:

1. Laura J. Moriarty. Criminal justice technology in the 21st century: third edition // Charles C Thomas Publisher. – Springfield, Illinois. – 2017. – 275 p.

2. John S. Hollywood, Dulani Woods, Richard Silberglitt, Brian A. Jackson. Using Future Internet Technologies to Strengthen Criminal Justice // RAND Corporation. – 2015. – 33 p.

3. Jeong-Yong Byun, Aziz Nasridinov. Internet of Things for Smart Crime Detection // Contemporary Engineering Sciences, Dongguk University Gyeongju. – 2014. – №15. – PP. 749-754.

4. Bernard Marr. How robots, IoT and artificial intelligence are transforming the police [Електронний ресурс]. – Режим доступу : https://www.forbes.com/sites/ bernardmarr/2017/ 09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/#659311d55d61.

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

Данілов О. В.,
магістрант Запорізький Національний
Технічний Університет, Запоріжжя

ФОРМИ ТА МЕТОДИ ПРОТИДІЇ ДЕФОРМАЦІЇ СИСТЕМИ ПРАВООХОРОННИХ ОРГАНІВ В УМОВАХ ТОТАЛІТАРНИХ РЕЖИМІВ

Протягом XX сторіччя світ пережив низку тоталітарних та авторитарних режимів. У Європі, Азії, Латинській Америці, Африці виникали та розвалювались диктатури, винищувались цілі народи, організовувались геноциди, етноциди, масові репресії за ідеологічної, релігійною, національною та іншими ознаками. Диктатори, які прийшли до влади або демократичним шляхом, або шляхом переворотів, використовували для вирішення завдання утримання влади різноманітні інструменти, в том числі правоохоронні органи або формування, які виконували їх функції.

Основною відмінністю тоталітарного режиму є домінування правоохоронних органів над державою. Це стосується не тільки контрольних, але й нормотворчих та розпорядчих функцій, які або повністю, або значною мірою від демократичних інституцій (парламент, виконавча влада, суди) до конституційних або навіть неконституційних органів правопорядку. Тобто головним орієнтиром функціонування внутрішніх органів в тоталітарній державі є не закон, а воля «фюрера» або правлячої партії, які або прямо формують нормативну базу, або передають ці повноваження повністю або частково у правоохоронні органи.

С цієї важливої ознаки тоталітарного режиму витікають інши спотворення функцій правоохоронних органів. Стратегічною метою їх існування є вже не забезпечення прав та свобод громадян, інтересів суспільства і держави, а забезпечення безпечної влади того суб'єкту, який формує «легітимність» правоохоронців, їх добробут та суспільний статус. І стратегічне планування в такому разі орієнтується не на протидії кримінальній злочинності та порушенням правопорядку, а на пошуку, виявленні та «знешкодженні» тим чи іншим шляхом противників тоталітарного режиму як такого.

До кінця XX століття склалася трирівнева система контролю за дотриманням прав людини: міжнародна, національна, громадянська.

Розгалужена система міжнародних організацій, діяльність яких спрямована на надання сприяння, організацію співпраці та захист прав людини, включає органи ООН, ОБСЄ, Ради Європи, Міжамериканську комісію з прав людини та ін. Національна система має різні механізми державного контролю, серед яких важливу роль відіграють національні інституції з прав людини (наприклад, інститут уповноваженого з прав людини). Цивільний контроль здійснюють недержавні (громадські) організації - правозахисні НДО та їх міжнародні об'єднання.

При цьому, на відміну від системи національного контролю, система цивільного контролю розглядає порушення прав людини тільки з боку держави.

Іншими словами, діяльність громадянського контролю спрямована на поліпшення державного устрою і надає дієву допомогу відповідним державним органам у здійсненні головної мети демократичної держави - захист і реалізації інтересів кожної людини.

Правозахисна діяльність НУО, її форми, масштаби, цілі і завдання залежать від цілого ряду чинників: політичної структури суспільства, історичних традицій, рівня розуміння населенням своїх прав, обізнаності про їх реалізацію, розвиненості всіх рівнів системи захисту прав людини - як цивільної, так і національної і міжнародної, і, звичайно, від фінансування. Всі ці фактори в тій чи іншій мірі є важливими у правозахисній діяльності НУО. Однак головною у визначенні цілей, завдань, форм і методів їх роботи залишається залежність від політичної структури суспільства.

Можна умовно виділити три типи таких структур: країни з розвиненою демократією, країни, що знаходяться на шляху відновлення або на початку розвитку демократії, країни з елементами тоталітарних і авторитарних структур.

В демократичній державі з більшою або меншою інтенсивністю функціонують всі три вищевказаних механізму. В умовах демократії міжнародний і цивільний контроль доповнюють і коректують діяльність державного, який є основним. Головне завдання правозахисних організацій тут - допомога конкретним громадянам з тих верств населення (наприклад, біженцям, безробітним і т. Д.), Які в силу різних причин не знайомі з особливостями діяльності національної системи захисту прав людини.

У країнах з розвиненою демократією правозахисні організації та їх лідери є невід'ємною частиною громадянського суспільства, користуються авторитетом і повагою. Вони мають вільний доступ до засобів масової інформації, оприлюднені ними відомості стають предметом вивчення та обговорення у відповідних державних структурах.

Правозахисні організації концентрують свої зусилля на захисті цивільних і політичних прав, боротьбі за дотримання належної процедури в ході судових процесів, на захист окремих особистостей, а не соціальних груп або шарів. Вони віддані традиційним ліберальним цінностям, які, як вважається, є джерелами правозахисного руху.

Відстоюючи дотримання в першу чергу цивільних і політичних прав і тільки в цьому сенсі займаючи певну політичну позицію, НВО в країнах з розвиненою демократією, в тому числі і впливові міжнародні правозахисні організації, дистанціюються від боротьби політичних партій, є неупередженими аналітиками, що порівнюють конкретну ситуацію в конкретній країні з міжнародними стандартами.

Використана література:

1. Андерсон Р.Д. Тоталитаризм: концепт илиидеология? // Полис. –1993. -№ 3.
2. Фромм Э. Проблема свободы и подчинения // Психология господства и подчинения /Сост. А.Г. Чернявская. Минск: Харвест, 1998. 19 с.

3. Diamond L., Developing Democracy: Toward Consolidation, Baltimore: Johns Hopkins University Press, 1999.
4. Domínguez J. I., Lowenthal A. F. Constructing democratic governance: South America in the 1990s. Santiago, 2001.
5. Fridman M. Two Lucky People. Chicago, 1998.

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

Ткачук Н. А.,
кандидат юридичних наук,
старший науковий співробітник
НДІІП НАПрН України

ВИКОРИСТАННЯ ІНТЕРНЕТУ РЕЧЕЙ В РОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ

Невпинне поширення Інтернету речей (IoT), як наслідок процесів інформатизації суспільства та розвитку новітніх технологій, обумовило поступову трансформацію багатьох соціальних інститутів. Призначені, в першу чергу, для покращення якості життя людини, оптимізації виробництва, розвитку промисловості та бізнесу шляхом управління ресурсами та підвищення продуктивності праці, технології IoT вплинули і на більш закриті суспільні сфери – діяльність спецслужб та розвідувальних органів.

Інтернет речей за своєю суттю є необмеженим джерелом даних, які у разі їх накопичення, комплексної інтеграції та аналізу відповідатимуть основним критеріям розвідувальної інформації та можуть бути безпосередньо чи опосередковано використані національними розвідками для забезпечення інтересів власних держав і підриву позицій країн-супротивників. При цьому, враховуючи транскордонність Інтернету речей та включення потоку даних IoT в єдину глобальну кібермережу, набагато зменшується витратна складова, притаманна традиційним видам розвідки, а також ризики, пов’язані із отриманням розвідінформації з територій інших країн.

Відповідно до класифікації, яку використовують розвідувальні органи США, на сьогодні, виділяють шість базових моделей збору розвідданих: радіоелектронна розвідка (SIGINT), видова розвідка (IMINT), вимірювально-сигнатурна розвідка (MASINT), агентурна розвідка (HUMINT), розвідка на основі відкритих джерел (OSINT) і геопросторова розвідка (GEOINT) [1]. На думку західних експертів, впровадження Інтернету речей призведе до формування сьомої моделі – «темпоральної» розвідки (temporal intelligence, TEMPINT), яка полягатиме у комплексному підході до збору й аналізу даних. При цьому під наглядом опиниться велика частина населення та об'єктів інфраструктури, дані про які можна буде збирати, зберігати і аналізувати [2].

Директор Національної розвідки США вперше офіційно визнав можливість використання Інтернету речей для стеження за їх власниками ще у лютому 2016 року під час заслуховувань у Конгресі, зауваживши, що у майбутньому

розвідувальні органи будуть широко використовувати IoT для ідентифікації, стеження, спостереження, визначення місця розташування, вербування агентів, отримання доступу до мереж та персональних даних користувачів [3].

У жовтні 2018 року видання «Блумберг» опублікувало резонансну статтю [4], яка містила докази того, що розвідка КНР приховано впровадила шпигунське апаратно-програмне забезпечення в комп'ютерне обладнання, експортоване в США. Ці «закладки» являли собою крихітний мікрочіп, розміром не більше рисового зернятка, вбудований в материнську плату сервера, та дозволяли будь-яким третім особам отримувати прямий доступ до інформації на ньому. Виявилося, що це обладнання довгий час використовувалося на серверах найбільших американських приватних компаній, де міститься величезний обсяг персональних даних – Amazon, Apple, Microsoft, Elemental і 30 інших, а також в структурах ЦРУ та Міністерства оборони США.

Сьогодні Китай є одним із основних виробників комп'ютерної техніки, комплектуючих та мережевого обладнання, що застосовується в IoT. Враховуючи рівень контролю держави над приватним бізнесом можна прогнозувати, що китайські спецслужби і надалі будуть використовувати метод впровадження прихованих апаратних закладок для отримання можливості використовувати Інтернет речей у якості інструменту розвідувальної діяльності.

Усвідомлюючи цю загрозу, країни ЄС та НАТО почали активні заходи із протидії використанню IoT для підриву власних національних інтересів. У першу чергу, вживаються заходи із додаткової технічної перевірки імпортованих з КНР апаратно-програмних засобів, збільшується контроль за діяльністю китайських компаній у сфері зв'язку та Інтернет-технологій, накладаються обмеження на використання китайських апаратно-програмних продуктів на об'єктах критичної інфраструктури [5].

В свою чергу, спецслужби США також здійснюють активні кроки для отримання прихованого контролю над Інтернетом речей але використовуючи інші підходи. Завдяки значним технічним можливостям США щодо контролю над інфраструктурою Інтернету, отримання доступу та перехоплення інформації, що циркулює в кіберпросторі (про що стало відомо громадськості завдяки викриттю методів роботи американських спецслужб Едвардом Сноуденом [6]), теоретично, вся інформація, яка акумулюється в наслідок роботи Інтернету речей стосовно їх користувачів може легко стати надбанням спецслужб США.

Крім того, американські спецслужби намагаються полегшити собі задачу з отримання доступу та контролю над Інтернетом речей шляхом лобіювання впровадження певних стандартів шифрування IoT на рівні Міжнародної організації зі стандартизації (ISO). Так у квітні 2018 року фахівцями АНБ було розроблено криптографічні інструменти (алгоритми Simon та Speck) для шифрування вхідних і вихідних даних з пристроїв і датчиків, що використовуються в технологіях IoT, та запропоновано останні у якості обов'язкових міжнародних стандартів [7].

Інший активний гравець у сфері кіберрозвідки – Російська Федерація, також має широкі можливості щодо збору розвідувальних даних з використанням IoT. В першу чергу, це пов'язано із високим рівнем контролю з боку держави над національним сегментом мережі Інтернет та діяльністю приватних суб'єктів господарювання в IT-сфері (у т.ч. операторами комунікацій та Інтернет-провайдерами), що забезпечує російським спецслужбам безперешкодний доступ до всієї інформації про користувачів IoT, яка зберігається на території РФ [8].

Крім того, ще одним механізмом отримання доступу до інформації, яка акумулюється в наслідок роботи Інтернету речей, а також методом отримання контролю над їх управлінням в інтересах проведення спецоперацій є використання прямих кібератак, які наразі, широко використовуються в діяльності спецслужб РФ та інших держав. Причому, вдалим реалізаціям таких атак сприяє низька цифрова грамотність громадян та неусвідомлення всіх тих ризиків, які несе в собі використання Інтеренту речей за умови недотримання базових вимог «цифрової гігієни».

На сьогодні, фактично єдиним проблемним питанням щодо використання IoT у розвідувальній діяльності є потреба забезпечити зберігання величезного обсягу інформації, отриманої внаслідок роботи таких технологій, а також впровадити ефективні апаратно-програмні технології для її обробки та аналізу, що потребуватиме значних обчислювальних та технологічних потужностей.

Водночас, враховуючи тенденції щодо розвитку штучного інтелекту (супер комп'ютерів) за технологією нейронних мереж, які мають здатність розвиватися та самонавчатися за допомогою великої кількості вихідних даних та, у подальшому, можуть використовуватися в інтересах національної безпеки для аналізу країн-супротивників, саме данні, отримані спецслужбами з використанням IoT, власне і можуть слугувати базисом для подальшого розвитку таких технологій. Це припущення може, певною мірою, пояснити глобальну шпигунську діяльність з боку китайських спецслужб в кіберпросторі та впровадження прихованих функцій в китайські електронні пристрої, що використовуються в технологіях IoT по всьому світу.

На сьогодні два найбільш потужних суперкомп'ютера мають саме Китай та США. Так, за годину останній може вирішити задачу, з якою звичайний ПК впорається за 30 років безперервної роботи, його обчислювальні сервери займають площу розміром з два тенісних корти, а кількість енергії, необхідної для його роботи, вистачило б, щоб забезпечити електрикою 8100 будинків [9]. Розробкою та впровадженням суперкомп'ютерів наразі займаються також інші країни – в першу чергу, Японія і країни Західної Європи.

Отже, як бачимо, збирання, аналіз та використання того масиву даних, до яких забезпечується доступ завдяки поширенню технології IoT, поступово перетворюється на невід'ємну складову розвідувальної діяльності. Ця тенденція, безумовно, впливає на стан світового безпекового середовища та потребує вжиття відповідних заходів реагування на національному рівні.

Для зниження рівня цієї загрози для України пропонується переглянути та удосконалити існуючі стандарти сертифікації імпортованої електронної продукції, сприяти розвитку її національного виробництва, обмежити на законодавчому рівні використання апаратно-програмних продуктів країни-агресора в IoT, що використовуються на об'єктах критичної інфраструктури, а також вжити комплексні заходи на загальнодержавному рівні із підвищення цифрової грамотності громадян щодо можливих загроз Інтернету речей та необхідних заходів «цифрової гігієни».

Використана література:

1. Office of the Director of National Intelligence: What is Intelligence? URL: https://www.dni.gov/index.php/what-we-do/what-is-intelligence.
2. Hershkovitz S., Tzezana R. Connected Devices Give Spies a Powerful New Way to Surveil. URL: https://www.wired.com/2017/01/connected-devices-give-spies-powerful-new-way-surveil/.
3. US intelligence chief: we might use the internet of things to spy on you. URL: https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.
4. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. URL: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2%20.
5. Europe raises flags on China's cyber espionage. URL: https://www.politico.eu/article/europe-raises-red-flags-on-chinas-cyber-espionage/.
6. Snowden Revelations URL: https://www.lawfareblog.com/snowden-revelations.
7. The NSA wants its algorithms to be a global IoT standard. But they're simply not trusted. URL: https://www.bitdefender.com/box/blog/iot-news/nsa-wants-algorithms-global-iot-standard-theyre-simply-not-trusted/.
8. Государственный контроль интернета в России. URL: https://tass.ru/info/693531.
9. The US again has the world's most powerful supercomputer. URL: https://www.wired.com/story/the-us-again-has-worlds-most-powerful-supercomputer.

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

Янова Л .О.,
канд. техн. наук, доцент
Пищикова О. В.,
канд. техн. наук, доцент
Сахно С. І.,
канд. техн. наук, доцент

ВИКОРИСТАННЯ ІНТЕРНЕТ РЕЧЕЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦИВІЛЬНОЇ І ПРОМИСЛОВОЇ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ ЛЮДЕЙ ТА ПОКРАЩЕННЯ УМОВ І ОХОРОНИ ПРАЦІ

В соціальному середовищі існують різні сфери діяльності людини: промисловість, транспортні технології, охорона здоров'я, освітні послуги, охорона навколишнього середовища, а у побуті – забезпечення комфортних умов проживання (розумне місто, розумний транспорт, розумний дім). Для кожної зі сфер діяльності, суспільство людей є споживачами послуг електронних

комунікацій. Сучасним напрямком є поширення технологій Інтернету речей (IP, Internet of Things, IoT) і надання послуг, проведення виробничих процесів і робіт без присутності людини шляхом реалізації за допомогою технологій IP. Під поняттям IP розуміється набір датчиків, сенсорів, пристроїв або системних комплексів, які мають між собою зв'язок і передають інформацію, використовуючи Інтернет. Такий процес функціонування речей дозволяє їм працювати дистанційно, без втручання людини, або з її мінімальним знаходженням поряд за умов підключення до мережі Інтернет.

Впровадження в сучасний виробничий процес технологій Інтернету речей дозволить здійснити обстеження щодо дотримання вимог з умов і охорони праці з використанням сенсорних датчиків вимірювання температури, вологості, швидкості руху повітря в приміщенні, або рівня освітленості, вологості, електромагнітних полів, та ін. Отримані дані замірів фізичних величин середовища передаються у вигляді цифрових даних.

Вимоги щодо параметрів мікроклімату виробничих приміщень регламентуються ДСН 3.3.6.042-99. Організм людини здатен пристосовуватись до умов мікроклімату. Верхня межа терморегуляції людини, що перебуває в стані спокою, є 30-31°С при відносній вологості 86%; або 40°С при відносній вологості 30%. При умовах виконання фізичної праці ця межа знижчується, а саме при виконанні важкої роботи теплова рівновага ще зберігається завдяки терморегуляторній функції організму при температурі 25-26°С і відносній вологості 40-60 %. Таким чином, для нормального теплового самопочуття людини важливо, щоб температура, відносна вологість і швидкість руху повітря перебували у певному співвідношенні. Ще до початку роботи такої рівноваги можливо досягнути з використанням встановлених IP сенсорних датчиків вимірювання температури, вологості, швидкості руху повітря в приміщенні за умов підключення до мережі Інтернет.

Допустимі параметри мікроклімату (табл. 1) - для випадів, коли на робочих місцях не можна забезпечити оптимальні величини мікроклімату за технологічними вимогами виробництва, технічною недосяжністю та економічно обґрунтованою недоцільністю, для виробничих приміщень.

Використання Інтернет речей дозволить регулювати межі допустимих параметрів мікроклімату. Допустимі мікрокліматичні умови за умов дії тривалого та систематичного впливу на людину можуть викликати зміни теплового стану організму, що швидко минають і нормалізуються та супроводжуються напруженням механізмів терморегуляції в межах фізіологічної адаптації. При цьому не виникає ушкоджень або порушень стану здоров'я, але можуть спостерігатися дискомфортні тепловідчуття, погіршення самопочуття та зниження працездатності.

Для нормування параметрів мікроклімату календарний рік поділяється на два періоди: холодний період року, коли середньодобова температура зовні приміщення нижча за +10ºС; та теплий року, коли середньодобова температура

зовні приміщення становить +10ºС і вище. Відповідно до вимог проведення вимірювання в холодний період року температура зовнішнього повітря не повинна бути вищою за середню розрахункову температуру, в теплий період -не нижчою за середню розрахункову температуру, що приймається для опалення та кондиціонування за оптимальними та допустимими параметрами.

Таблиця 1 - Допустимі величини температури, відносної вологості та швидкості руху повітря в робочій зоні виробничих приміщень

Період року	Категорія робіт	Температура, С				Відносна вологість (%) на постійних і непостійних робочих місцях	Швидкість руху повітря (м/с) на постійних і непостійних робочих місцях
		Верхня межа		Нижня межа			
		на постійних робочих місцях	на непостійних робочих місцях	на постійних робочих місцях	на непостійних робочих місцях		
Холодний період	Легка Іа	25	26	21	18	75	не більше 0,1
	Легка Іб	24	25	20	17	75	не більше 0,2
	Середньої важкості IIа	23	24	17	15	75	не більше 0,3
	Середньої важкості IIб	21	23	15	13	75	не більше 0,4
	Важка III	19	20	13	12	75	не більше 0,5
Теплий період	Легка Іа	28	30	22	20	55 при 28 С	0,1-0,2
	Легка Іб	28	30	21	19	60 при 27 С	0,1-0,3
	Середньої важкості IIа	27	29	18	17	65 при 26 С	0,2-0,4
	Середньої важкості IIб	27	29	15	15	70 при 25 С	0,2-0,5
	Важка III	26	28	15	13	75 при 24 С	0,5-0,6

Постійне робоче місце - на якому працюючий знаходиться понад 50% робочого часу або більше 2-х годин безперервно. Якщо при цьому робота здійснюється в різних пунктах робочої зони, то вся ця зона вважається постійним робочим місцем. Непостійне робоче місце - на якому працюючий знаходиться менше 50% робочого часу або менше 2-х годин безперервно.

Оптимальні параметри мікроклімату (табл. 2) повинні підтримуватись в приміщеннях, пов’язаних з виконанням нервово-емоційних робіт, що потребують підвищеної уваги (диспетчерські, приміщення, де працюють із комп’ютерами, кабінети діагностики, пульти управління технологічними процесами, хімічні

лабораторії, бухгалтерії, конструкторські бюро). Для таких робіт оптимальна температура повітря в межах +22 +24ºС; його відносна вологість 40 – 60%; швидкість руху не більше 0,1 м/сек.

Таблиця 2 - Оптимальні величини параметрів мікроклімату

Період року	Категорія робіт	Температура повітря, оС	Відносна вологість, %	Швидкість руху повітря, м/с
Холодний період	Легка Іа	22-24	40-60	0,1
	Легка Іб	21-23	40-60	0,1
	Середньої важкості ІІа	19-21	40-60	0,2
	Середньої важкості ІІб	17-19	40-60	0,2
	Важка ІІІ	16-28	40-60	0,3
Теплий період	Легка Іа	23-25	40-60	0,1
	Легка Іб	22-24	40-60	0,2
	Середньої важкості ІІа	21-23	40-60	0,3
	Середньої важкості ІІб	20-22	40-60	0,3
	Важка ІІІ	18-20	40-60	0,4

Вимірювання параметрів мікроклімату на робочих місцях повинно проводитись на висоті 1,0 м. -для сидячих робіт, та 1,5 м - для стоячих робіт (від підлоги, або робочого майданчика). Саме на таких нормованих величинах висоти і потрібно встановлювати датчики ІР, які будуть з заданою періодичністю здійснювати виміри і передачу їх даних для контролю.

Крім спостереження за станом мікрокліматичних умов, можливо контролювати і інші параметри забезпечення умов і охорони праці в галузі цивільної і промислової безпеки для забезпечення безпеки життєдіяльності.

Останнім часом змінилися нормативи щодо електромагнітних випромінювань (наказ Міністерства охорони здоров'я України «Про затвердження Зміни до Державних санітарних норм і правил захисту населення від впливу електромагнітних випромінювань» від 13.03.2017 №266, зареєстрований в Міністерстві юстиції України 16 травня 2017 року за №625/30493. Попередні державні санітарні норми визначали максимальний рівень електромагнітного випромінювання на рівні 2,5 мкВт/кв. см. Відсьогодні гранично допустимий рівень піднявся до 10 мкВт/кв. см. У цьому ж рішенні Міністерство охорони здоров'я скасувало санітарні паспорти, які раніше оператори мусили отримувати для кожної з базових станцій. Відтепер базові станції зможуть працювати з використанням вищої потужності, а це забезпечить краще покриття та кращу якість, стабільність і швидкість передачі даних у мережі. Сучасні термінали стільникового зв'язку випромінюють, в середньому, 0,1-1 Вт, вони перебувають у прямому контакті з організмом людини. Відомо, що рівень ЕМП спадає

пропорційно квадрату відстані, то зрозуміло, що термінали мають більший негативний вплив на стан здоров'я користувача, ніж базові станції, яка не перебуває у прямому контакті з організмом людини. Таким чином, зменшення ризиків тепер можливо забезпечити за рахунок мінімально необхідного підвищення гранично – допустимого рівня електро - магнітних полів базових станцій. Згідно зі Змінами № 266, гранично - допустимий рівень ЕМП для радіотехнічних об'єктів, що працюють у діапазонах дуже високих частот та ультрависоких частот, встановлюється на рівні 10 мкВт/см$^{-2}$ або 6 В/м. Допускаються розміщення та експлуатація радіотехнічних об'єктів на дахах та у приміщеннях житлових, громадських та інших будівель за умови дотримання встановлених вимог.

Державні санітарні норми приведені до вимог Євростандартів і допомагають розгортанню мереж 3 G та 4G. Поширення комп'ютерних та Інтернет-технологій, впровадження розробленого Міжнародним союзом телекомунікацій (ITU) стандарту мобільного зв'язку 3G, дозволяють високошвидкісний мобільний доступ до мережі Інтернет і технологію радіозв'язку передачі даних.

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

Кравченко І. А.,
Ст. викладач кафедри філософії ФСП
КПІ ім. Ігоря Сікорського

ДЕРЖАВНІ ЗАХОДИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТ РЕЧЕЙ В СОЦІАЛЬНІЙ СФЕРІ

17 січня 2018 року Україною був здійснений крок на шлях впровадження та використання цифрових технологій, в тому числі, технологій інтернет речей в соціальній сфері. Кабінетом міністрів України було схвалено «Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки» та затвердженно «План заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки» [1]. В Концепції введено поняття *цифровізація* – «насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір». И хоча основний наголос в цих документах робиться саме на розвиток цифрової економіки (цифровізації економічної сфери), але серед передбачених заходів є заходи щодо цифрового розвитку соціальної сфери (цифровізації соціальної сфери).

В Концепції серед основних цілій, в тому числі, заявлені: «доступність для громадян переваг та можливостей цифрового світу»; «реалізація людського ресурсу, розвиток цифрових індустрій та цифрового підприємництва»; створення нових цінностей та якостей в результате цифровізації таких соціальних систем та

сфер життєдіяльності, як освіта та медицина. Головною метою Коцепції встановлено прискорення «сценарію цифрового розвитку, як найбільш релевантного для України з точки зору викликів, потреб та можливостей». Сценарієм цифровізації передбачено: усунення законодавчих, інституційних, фіскальних та інших перешкод; створення попиту та формування потреб серед громадян до цифровізації; створення та розвиток цифрових інфраструктур як основи використання переваг цифрового світу у повсякденному житті; розвиток та поглиблення цифрових компетенцій громадян для забезпечення їх готовності до використання цифрових можливостей, а також подолання супутніх ризиків.

Серед зазначених принципів цифровізації: створення інформаційних структур для забезпечення рівного доступа до послуг, інформації і знань, що забезпечує визнане ООН як фундаментальне право кожной людини – цифрове право; створення переваг у різноманітних сферах повсякденного життя, що передбачає підвищення якості надання послуг з охорони здоров'я та отримання освіти, створення нових робочих місць, розвитку підприємництва, сільського господарства, транспорту, захисту навколишнього природного середовища і керування природними ресурсами, підвищення культури, сприяння подоланню бідності, запобігання катастрофам, гарантування громадської безпеки тощо; вплив цифровізації на розвиток інформаційного суспільства, в тому числі, й в соціальній сфері. Також цифровізація визначена як об'єкт «фокусного та комплексного державного управління» та зазначен основні завдання держави.

Основними напрями цифровізації соціальної сфери на найближчі два роки оголошені: подолання цифрового розриву (цифрової нерівності) шляхом розвитку цифрових інфраструктур; розвиток цифрових компетенцій – цифрова грамотність визначена як одна з головних компетенцій, а створення та викоконання національної програми навчання загальним і професійним цифровим компетенція зафіксовано приоритетним завданням для прискорення розвитку цифрової економіки; впровадження концепції цифрових робочих місць - що для соціальної сфери з точки зору сприяння соціалізації створює й певні переваги, але й певні загрози; цифровізація реального сектору економіки і соціальної сфери, де головне значення надається в тому числі такій технології, як Інтернет речей; реалізація проектів цифрових трансформацій в сферах освіти, охорони здоров'я, гормадської безпеки, екології, життєдіяльністі міст (від проекту «розумний будинок» до проектів «розумне використання ресурсів», «розумне місто» та «розумна країна»), де також передбачено використання технологій Інтернет речей. До окремих напрямків цифровізації віднесено: освіта, де цифрові технології та технології Інтернета речей змінюють підходи до процесу навчання, роблячі більш комфортним в формуванні відповіних навичок та в засвоєнні інформації; сфера охорони здоров'я з впровадженням систем для надання дистанційних послуг як громадянам так й підтримки роботи лікарів. Також зазначені напрямки цифровізації та використання технологій Інтернета речей в сферах екології та охорони навколишнього середовища, життєдіяльністі міст, державного

управління, гармонізації з європейськими та світовими науковими ініціативами тощо.

Планом заходів щодо реалізації Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки, поміж іншим, передбачено: розроблення переліку цифрових прав громадян відповідно до зобов'язань України у сфері європейської інтеграції та інших міжнародних зобов'язань, запровадження принципу "цифровий за замовчуванням" під час підготовки нових або внесення змін до існуючих законодавчих, розроблення пропозиції щодо впровадження базових цифрових послуг для використання громадянами у сфері освіти, охорони здоров'я, транспорту, телекомунікацій, туризму, екології, підготовка пропозицій щодо модернізації освіти для підтримки розвитку цифрової індустрії, подання пропозицій щодо використання цифрових технологій, зокрема Інтернету речей, розроблення проекту акта Кабінету Міністрів України про реалізацію проектів цифрових трансформацій у деяких секторах соціальної сфери, внесення змін до реєстру професій та розроблення програми впровадження цифрових спеціальностей тощо.

Ці заходи, за умови їх втілення, створять подальші умови для впровадження і поширення використання цифрових технологій та технологій Інтренета речей, що, в свою чергу, надасть також можливість запровадити нові моделі та механізми в функціонуванні соціальної сфері для покращення надання доступу до соціальних послуг всім верствам населення.

Використана література:

1. Концепція розвитку цифрової економіки та суспільства України на 2018-2020. – URL: http://zakon.rada.gov.ua/laws/show/67-2018-%D1%80.

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

Новицька Н.Б.,
д.ю.н., старший науковий співробітник
Університет Державної фіскальної служби України

ПРАВОВЕ РЕГУЛЮВАННЯ СОЦІАЛЬНОЇ РЕКЛАМИ В МЕДИЧНІЙ СФЕРІ

З розвитком інформаційних технологій загострюється ціла низка соціальних проблем, особливо пов'язаних із моральним здоров'ям суспільства та здоровим способом життя. Безперечно, розвиток культури здорового способу життя потребує відповідних державних програм та фінансування. Проте основними перевагами цього є підтримка працездатності населення (що впливає на ВВП держави), покращення рівня життя громадян, зниження рівня захворювань на алкоголізм, наркоманію, ВІЛ/СНІД, туберкульоз та інші «соціальні» захворювання. Саме тому актуалізується проблема поширення ідеї ведення здорового способу життя серед населення як один із способів оптимізації галузі

охорони здоров’я України. Як слушно зазначає Овсянецька О.Я., одним із ефективних інструментів досягнення цілі попередження захворюваності населення та популяризацію здорового способу життя є сучасні маркетингові технології: соціальна реклама, пропаганда та PR-технології, різного роду акції та заходи, які сприятимуть поширенню інформації[1].

Власне інформаційне забезпечення населення формує стимули ведення здорового способу життя, а держава повинна стати головним суб’єктом, який за допомогою різних методів та способів здійснює таке інформаційне забезпечення. Одним із таких засобів і є соціальна реклама.

У ст. 1 Закону України “Про рекламу” соціальну рекламу визначено так: “Інформація будь-якого виду, розповсюджена в будь-якій формі, яка спрямована на досягнення суспільно корисних цілей, популяризацію загальнолюдських цінностей і розповсюдження якої не має на меті отримання прибутку”[2].

Б.А. Обритько визначає соціальну рекламу як некомерційну інформацію державних органів і громадських організацій з питань здорового способу життя охорони природи, профілактики правопорушень та соціального захисту населення[3, с. 10]. На нашу думку, місія соціальної реклами – це зміна ставлення людей до проблем суспільства, а в довгостроковій перспективі – пропозиція нових соціальних цінностей, затребуваних суспільством.

У Конституції України чітко зазначено: «Кожен має право на охорону здоров’я, медичну допомогу та медичне страхування. Охорона здоров’я забезпечується державним фінансуванням відповідних соціально-економічних, медико-санітарних та оздоровчо-профілактичних програм». Тобто саме держава зобов’язана здійснювати просвітницько-профілактичні заходи з метою пропагування здорового способу життя та зменшення різного роду «соціальних» хвороб, таких як СНІД, туберкульоз, тютюнопаління, наркоманія та ін.

Слід наголосити, що Основи законодавства України про охорону здоров‘я містять у собі окремий розділ IV, який називається “Забезпечення здорових і безпечних умов життя” де одна з статей стосується сприяння здоровому способу життя населення.

Відзначимо, що Міністерством охорони здоров’я проводиться інформаційно-роз’яснювальна робота щодо популяризації здорового способу життя, у вигляді виступів на радіо, на телебаченні, публікацій у пресі, проведенні прес-конференцій, засідань круглих столів, брифінгів, підготовки прес-релізів та санбюлетнів. Разом з тим можливості соціальної реклами майже не використовуються.

Важливим і перспективним у сфері охорони здоров’я, на наш погляд, є комплекс заходів із створення соціальної реклами, який передбачає забезпечення пріоритетності оздоровлення, фізичної культури, посилення просвітницької діяльності серед населення щодо вимог екологічних норм і стандартів; популяризацію здорового способу життя, культури здоров’я, ранньої діагностики хвороб.

Сьогодні не можна стверджувати, що в інформаційному просторі України повністю відсутня соціальна реклама, яка пропагує здоровий спосіб життя, звертає увагу суспільства на шкідливі звички - наркоманію, тютюнопаління та ін. І хоча законом заборонено розміщувати в соціальній рекламі «посилання на конкретний товар та/або його виробника, на рекламодавця», все ж ми бачимо приклади, коли виробники використовують соціальну рекламу для просування власного бренда. Наприклад, дуже часто можна побачити начебто соціальну рекламу «Ми проти СНІДу» з посиланням на конкретного виробника презервативів.

Законом України «Про рекламу» встановлено норми щодо безкоштовного розміщення соціальної реклами державних органів та органів місцевого самоврядування, громадських організацій у засобах масової інформації - розповсюджувачів реклами, діяльність яких повністю або частково фінансується з державного або місцевих бюджетів, «в обсязі не менше 5 відсотків ефірного часу, друкованої площі, відведених для реклами»[2]. І не менш важливим кроком для вирішення соціальних проблем є те, що засоби масової інформації - розповсюджувачів реклами, які повністю або частково фінансуються з державного або місцевих бюджетів, закон зобов'язує «надавати пільги при розміщенні соціальної реклами, замовником якої є заклади освіти, культури, охорони здоров'я, які утримуються за рахунок державного або місцевих бюджетів, а також благодійні організації»[2].

Не зважаючи на норму закону Міністерство охорони здоров'я надзвичайно мало замовляє створення соціальної реклами. Це здебільшого можна пояснити надто малими обсягами фінансування. Внаслідок того, що в Законі „Про рекламу" не регламентується фінансовий бік соціальної реклами, невідомо, хто має платити за її виробництво та розміщення. Також відсутній єдиний бюджет на державну соціальну рекламу в якому, на нашу думку, повинно бути чітко передбачено видатки державним органам для створення та розміщення соціальної реклами. Доволі цікавим в аспекті розгляду вирішення зазначеної проблеми є досвід Великобританії. При уряді Великобританії ще з 1946 р. існує Центральний офіс інформації (COI) – незалежний маркетинговий центр, цілі якого – координація діяльності урядових структур у галузі комунікацій і взаємодія з рекламними агентствами. Один з найважливіших принципів діяльності COI полягає в тому, що він не є політичною структурою[4, с. 7]. Реклама замовляється урядом і фінансується з його бюджету. Інше вирішується саморегулюванням рекламної індустрії. Влада не намагається змусити ЗМІ розміщувати соціальну рекламу безкоштовно. Те ж стосується і взаємодії з рекламними агентствами: COI не зобов'язує їх працювати безкоштовно, але і не платить підвищених гонорарів, орієнтуючись на стандартні і ринкові розцінки. COI для медіа-ринку – такий же клієнт, як будь-яка інша комунальна або комерційна компанія. Єдиний "бонус" – особливий престиж, пов'язаний з роботою за замовленням уряду.

Ще однією, на нашу думку, важливою проблемою залишається якість соціальної реклами та її вплив на споживачів. Описуючи способи маніпуляції в

соціальній рекламі, дослідниця Г. Ніколайшвілі визнає, що й у такому виді комунікації вплив на масову свідомість може супроводжуватися дисфункціональними ефектами як позитивними так і негативними, такими наприклад, як: ефект "бумеранга" (отримання результату, протилежного очікуваному); ефект "насичення" (звикання аудиторії до негативної, гнітючої інформації, що провокує байдужість до нових трагічних подій); ефект "реактанс" (людина, навіть за відсутності власної позиції, реагує протестом на нав'язування певної поведінки)[5, с. 102]. Тому з метою уникнення дисфукнціональних ефектів Цуканова Є.Г., пропонує дотримуватися етичних і фахових норм при створенні рекламного повідомлення, залучення до їх розробки фахівців дотичних галузей, зокрема психологів, співробітників соціальних центрів, медиків, представників громадськості тощо. Особливу увагу слід приділяти вивченню цільової аудиторії та обов'язкове тестування соціальної реклами до початку розповсюдження [6].

На наше переконання, Міністерство охорони здоров'я якраз і має стати тим державним органом який буде здійснювати обов'язкове попереднє тестування соціальної реклами, моніторинг та оцінку ефективності впливу соціальної реклами в сфері охорони здоров'я, адже всі необхідні фахівці є у розпорядженні даного державного органу.

Держава за допомогою раціонально побудованого законодавства може створити умови, що сприятимуть створенню у членів суспільних відносин мотивацій для певних видів діяльності чи поведінки, які передбачають застосування навичок здорового способу життя і тим самим сприяють охороні здоров'я як на індивідуальному, так і на популяційному рівнях. Наприклад, такі умови мають передбачати забезпечення відповідної поінформованості членів суспільства, формування відповідного освітнього рівня населення, забезпечення фізичної та економічної доступності товарів та послуг, використання яких сприяє збереженню та зміцненню здоров'я, формування моральної та економічної зацікавленості людей вести здоровий спосіб життя тощо.

Використана література:

1. Овсянецька О.Я. Перспективи використання маркетингових інструментів у галузі охорони здоров'я України *Маркетинг і менеджмент інновацій*. 2012. № 1. С. 241-245.
2. Про рекламу : Закон України від 3 липня 1996 р. №270/96 ВР. URL: http://zakon4.rada.gov.ua/laws/show/270/96-вр (дата звернення: 20.11.2018)
3. Обритько, Б.А. Рекламна діяльність : курс лекцій. К. : МАУП, 2002. 240с.
4. Грицюта Н. Етичні регулятиви соціальної реклами в країнах ЄС. *Наукові записки Інституту журналістики.* 2010. Т. 40. С.6–14.
5. Николайшвили Г.Г. Социальная реклама: теория и практика. М. : Аспект-Пресс, 2008. 191с.
6. Цуканова Г.О. Дисфункціональні ефекти соціальної реклами. *Держава та регіони.* 2013. № 1(13). С. 112-115.

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

Гущин О. О.,
к.ю.н., професор кафедри правового забезпечення Військового інституту Київського національного університету імені Тараса Шевченка
Роллер В. М.,
ад'юнкт науково організаційного відділення Військового інституту Київського національного університету імені Тараса Шевченка

КІБЕРПРОСТІР ЯК НОВІТНІЙ ВИМІР БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У двадцять першому сторіччі кіберпростір, разом із сушею, морем, повітрям і космосом, швидко стає новим театром воєнних дій, а світова спільнота, зокрема, НАТО, визнала його новим, п'ятим виміром ведення воєнних операцій.

В цьому аспекті ведення операцій в кібернетичному просторі (кібервійни, кібернетичні операції) можна вважати одним з основних напрямків революції у військовій справі.

У 2003 році на 32-й сесії Генеральної конференції ЮНЕСКО прийнято рекомендації «Про розвиток та використання багатомовності та загальному доступі до кіберпростору», згідно з якою кіберпростір визначено як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою [1].

Згодом, у 2010 році після застосування вірусу Stuxnet у Ірані та визнання світовою спільнотою його як кібер зброї, викликало необхідність правового регулювання здійснення кібероборони окремих об'єктів та мілітаризації кіберпростору загалом.

У 2013 році Північноатлантичним Альянсом було опубліковано "Таллінське Керівництво з міжнародного права щодо методів ведення кібернетичних бойових дій", яким кіберпростір визначено як середовище, що сформовано з фізичних і нефізичних елементів, яке характеризується використанням комп'ютерів та електромагнітного спектру для зберігання, зміни і обміну даними з використанням комп'ютерних мереж[2]. Таким чином були закладені первинні основи застосування норм міжнародного права збройних конфліктів до операцій,що проводяться у кіберпросторі.

Як зазначено у Стратегічній концепції оборони та безпеки членів Організації Північноатлантичного договору "Активне залучення, сучасна оборона", кібератаки стають все більш частими, більш організованими і більш збитковими для державних установ, підприємств, економіки і, можливо, також транспортній та електричній мережам та інших об'єктів критичної інфраструктури; вони можуть досягти критичного рівня, який загрожує національному та Євроатлантичному процвітанню, безпеці і стабільності.

Джерелом таких атак можуть бути іноземні військові та розвідувальні служби, організовані злочинні угруповання, терористичні та/або екстремістські групи [3]. Отже, світова спільнота відкрито говорить про можливість використання кіберсередовища для ведення військових дій.

Варто зазначити, що наша держава не залишається осторонь цих новітніх процесів. Так, Указом Президента України від 15 березня 2016 року № 96/2016 затверджено рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [4], а розпорядженням Кабінету Міністрів України від 10 березня 2017 року затверджено план заходів з її реалізації на 2017 рік. Ним, зокрема, передбачено питання удосконалення нормативно-правової бази шляхом впровадження норм міжнародних стандартів, стандартів ЄС та НАТО у сфері інформаційної безпеки та кіберзахисту [5]. Величезним позитивним моментом слід вважати прийняття 5 жовтня 2017 року Верховною Радою України Закону України "Про основні засади забезпечення кібербезпеки України" [6], яким, зокрема, вводяться такі поняття як "кібербезпека", "кіберзахист", "кібероборона", "кібершпигунство" тощо. Згідно зі статтею 7 цього Закону одним з принципів забезпечення кібербезпеки є пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам та реалізація невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі. Зазначений Закон визначає, наприклад, кібератаку як спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [7]..Це є важливим кроком, для подальшої кваліфікації дій у кіберпросторі України.

Отже фактично вперше на рівні закону у вітчизняній практиці систематизовано та конкретизовано основні терміни, які застосовуються під час забезпечення кібербезпеки держави.

Також цим Законом передбачається, що повноваження із здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони) відповідно до компетенції здійснюють Міністерство оборони України та Генеральний штаб України.

Таким чином в Україні на законодавчому рівні визначено, що до функцій Міністерства оборони України та Генерального штабу Збройних Сил України

віднесено повноваження щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони). Одночасно закріплено функцію Міністерства оборони України, як і інших органів державної влади, щодо здійснення заходів щодо кіберзахисту своєї власної інформаційно - телекомунікаційної мережі від втручання.

Міністерство оборони України здійснило класифікацію наслідків, до яких можуть призвести кібератаки, що використовуються під час проведення кібероперацій:вандалізм - атака, яка не вбиває людей, але завдає удару по авторитету держави як у світі, так і серед населення, завдає репутаційних втрат. До таких кібернетичних атак можна віднести псування офіційних інтернет-сторінок, заміну змісту образливими чи пропагандистськими малюнками;пропаганда - розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення. Пропаганда зосереджена на певній верстві населення, так званій цільовій аудиторії;збір інформації — злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні. У цьому випадку дезінформація та викрадення даних, наприклад, відомостей щодо пересування наших військ у районі ведення бойових дій, призведе до неминучих людських втрат. Інша назва — кібершпигунство; відмова сервісу — атаки з великої кількості комп'ютерів, основна мета яких — порушення функціонування сайтів або комп'ютерних систем; втручання в роботу обладнання — атаки на комп'ютери або сервери, які, наприклад, забезпечують роботу комунікаційних цивільних або військових систем, що, у свою чергу, призведе до відключення або виникнення помилок при обміні даними, а ще гірше — буде втрачено зв'язок, а відтак можливість управління діями підрозділів;атаки на об'єкти критичної інфраструктури — атаки на комп'ютери та системи, що забезпечують життєдіяльність міст, а саме: системи водопостачання, електроенергії, транспорту тощо [8].

У 2016 році в Міністерстві оборони України затверджено План дій щодо впровадження оборонної реформи у 2016-2020 роках (Дорожня карта оборонної реформи).

Цим документом передбачено: створення спільної системи C4ISR на стратегічному рівні на основі стандартів, доктрин і рекомендацій НАТО, та, зокрема, Створення центру оперативного реагування на інциденти кібернетичної безпеки; удосконалення системи кібербезпеки та захисту інформації, включаючи створення в Міністерстві оборони України, інших складових сектору оборони підрозділів з кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC, розробку плану дій згідно зі стратегією кібербезпеки за координації Апарату Ради національної безпеки і оборони України, створення системи реагування на комп'ютерні надзвичайні події для захисту інформації і державних інформаційних ресурсів у кіберпросторі тощо.

Важливим дослідження є правовий аналіз, здійснений під час створення “Талліннського керівництва з міжнародного права, що застосовується до кібероперацій 2.0”, який базується на розумінні того, що міжнародне право, що створено до “кібер-епохи”, застосовується й до кібероперацій, які проводяться державами і спрямовані проти держав. Це означає, що ці “кібер-події” не відбуваються в правовому вакуумі, і держави мають права та несуть зобов’язання за міжнародним правом [9].

Використана література:

1. Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству от 15.10 2003; URL: http://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml;
2. “Таллінське Керівництво з міжнародного права щодо методів ведення кібернетичних бойових дій” 2013 р., за заг. редакцією М. Шмітта; URL:https://ccdcoe.org/tallinn-manual.html;
3. Активне залучення, сучасна оборона.Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору, прийнята главами держав та урядів у Лісабоні 19 листопада 2010 року. URL:https://www.nato.int/cps/uk/natohq/official_texts_68580.htm;
4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” : Указ Президента України від 15 березня 2016 року № 96/2016 // Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua/documents/962016-19836;
5. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 10 березня 2017 року № 155-р // Урядовий портал. URL: https://www.kmu.gov.ua/ua/npas/249807504;
6. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII // База даних “Законодавство України” / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/2163-19;
7. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII // База даних “Законодавство України” / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/2163-19;
8. Кібербезпека як важлива складова всієї системи захисту держави, 07 травня 2018;URL: http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html;
9. “Таллінське керівництво з міжнародного права, що застосовується до кібероперацій 2.0” за заг. ред. М.Шмітта; 2017 URL: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

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

Довгаль Ю. С.,
молодший науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.

БЕЗПЕКА МЕРЕЖЕВИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Відповідно до фундаментальних положень Доктрини інформаційної безпеки України [1] забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб є пріоритетним завданням політикуму нашої країни. Інформаційна безпека держави є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави.

Розглянемо законодавчі ініціативи та практичні заходи, які вживаються євроспільнотою з метою протидії інформаційній експансії та забезпечення власної інформаційної безпеки.

ЄС не стоїть на місці, постійно змінюючи та вдосконалюючи підходи до регулювання сфери інформаційної безпеки. З метою систематизації та встановлення мінімальних вимог для всіх країн-членів ЄС у 2016 році була схвалена Директива Європарламенту та Ради Європи №2016/1148 «Про загальні заходи безпеки мережевих та інформаційних систем» [2], положення якої зобов'язують уряди держав-членів визначати об'єкти критичної інфраструктури в різноманітних сферах. Отже, в ЄС з метою посилення рівня кіберзахисту інформаційно-телекомунікаційних мереж та систем були запроваджені Єдині нові правила.

Виходячи із змісту вказаного документа, саме інформаційні мережі та системи відіграють життєво важливу роль в європейському суспільстві. Зважаючи на те, що глобальні мережі мають транснаціональний характер, істотні порушення штатного функціонування інформаційних систем цивільного або військового управління, незалежно від того, навмисні чи ненавмисні ці дії, а також від місця їхнього скоєння, можуть негативно впливати на окремі держави-члени ЄС.

Причиною прийняття нової Директиви ЄС стала необхідність розробки дієвого механізму запобігання інцидентам у сфері інформаційної безпеки, що стосується обчислювальних мереж, серверів, систем зберігання даних і мережевих вузлів. Таким чином, ефективне реагування на вказані виклики безпеці мережевих та інформаційних систем вимагає глобального підходу на рівні ЄС, що охоплює загальне зміцнення технічного потенціалу, налагодження інформаційного обміну,

співпраці і загальних вимог безпеки для операторів цифрових послуг. Зазначена Директива передбачає впровадження таких заходів щодо підвищення загального рівня кібербезпеки в ЄС, які забезпечать:

- відповідний рівень готовності держав-членів, що передбачає створення Команд швидкого реагування на кіберінциденти (Computer Security Response (CSIRT)), і компетентних відповідальних національних органів;
- комплексну співпрацю між усіма державами-членами ЄС з метою надання підтримки та сприяння обміну інформацією між державами-членами про кіберзагрози та кіберінциденти;
- високий рівень безпеки у всіх секторах, які мають життєво важливе значення для економіки і суспільства і, крім того, в значній мірі залежать від інформаційно-комунікаційних технологій (ІКТ), таких як: енергетика, транспорт, водопостачання, банківська сфера, інфраструктури фінансового ринку, охорони здоров'я та цифрова інфраструктура.

Крім того, ключові постачальники цифрових послуг (пошукові системи, хмарні обчислення і он-лайнові торговельні майданчики) повинні відповідати вимогам безпеки і здійснювати повідомлення про будь-які кіберінциденти. З метою досягнення високого рівня безпеки мережевих та інформаційних систем кожна держава-член ЄС також зобов’язана розробити **Національні стратегії з безпеки мережевих та інформаційних систем**, що визначають цілі і конкретні заходи, які повинні бути реалізовані.

Проте у 2018 році ситуація кардинально змінилася. З травня 2018 року в ЄС запроваджено нові вимоги до захисту персональних даних. З 25 травня 2018 року в юридичному полі Європейського Союзу вступив в силу новий нормативний акт Загальний Регламент Захисту Даних, більш відомий як GDPR (General Data Protection Regulation) [3]. Євросоюз перейшов на нові правила поводження з персональними даними, а Регламент стосується будь-якої роботи з персональними даними, зокрема їх збору, зберігання і передачі. За недотримання вимог GDPR компаніям загрожує втрата європейських клієнтів і ринків, а також штрафи до 20 млн євро, або 2-4% від річного фінансового обігу компанії порушника. Хоча закон прийнятий для захисту європейських даних, глобальний характер Інтернету означає, що GDPR встановлює стандарт конфіденційності даних у всьому світі. Практично всі великі інтернет-компанії, включаючи «Google, Facebook і Twitter», повинні дотриматися вимог GDPR.

У Франції на законодавчому рівні посилюються заходи з метою контролю мас-медіа, для захисту країни від фальшивих новин – усі медіа, соцмережі, пошуковики, інформаційні портали матимуть певні зобов’язання стосовно "спонсорського контенту", який вони розміщують. Крім того очікується збільшення повноважень Вищої наглядової ради радіотелебачення (Conseil supérieur de l’audiovisuel, CSA) для "боротьби зі спробами дестабілізації ситуації телеслужбами, що знаходяться під впливом іноземних держав" [4].

Отже, слід зазначити, що інформаційний простір, на сьогоднішній день, відіграє дуже велику роль у забезпеченні інформаційної безпеки людини,

суспільства, держави. І тому, державні органи повинні впроваджувати та удосконалювати нормативно-правову базу, яка регламентує діяльність правоохоронних органів та військових формувань. Адже від їхньої діяльності залежить безпека громадян на інформаційному рівні.

Використана література:

1. Доктрина інформаційної безпеки України: Затверджена Указом Президента України від 25 лютого 2017 року №47/2017. – Режим доступу: http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru.

2. Директива Європарламенту та Ради Європи №2016/1148 від 6 липня 2016 року «Про загальні заходи безпеки мережевих та інформаційних систем». – Режим доступу: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-20161148.pdf.

3. Директива Захисту GDPR (General Data Protection Regulation) від 27 квітня 2016 року. – Режим доступу: https://eu-ua.org/sites/default/files/inline/files/es-2016679.pdf.

4. Франція, готує новий закон для протидії фейкам на виборах. Пропаганду забанять у Google. – Режим доступу: https://www.eurointegration. com.ua/articles/2018 /03/20/7079007/.

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

Алексєєв М. М.,
Помічник начальника Національного університету оборони України імені Івана Черняховського

КРОКИ ПОЛЬЩІ ЩОДО ПРОТИДІЇ КІБЕРНЕТИЧНИМ ЗАГРОЗАМ: ДОСВІД ДЛЯ УКРАЇНИ

Для протидії "***кібернетичним загрозам***" [1] в національному і міжнародному масштабах істотним є заздалегідь набутий консенсус в питанні, які дії повинні вважатися агресією, наприклад, в ході можливої "***кібернетичної атаки***" [1] чи "***кібернетичного удару***" [1] по об'єктам національної інфраструктури, визначення законних заходів протидії та спроможностей по протидії.

Міністерство національної оборони Польщі завершує роботу над проектом рішення про формування військ оборони кіберпростору. Для їх створення планується виділити два мільярди злотих.

Міністр національної оборони Польщі взяв участь у III Європейському форумі з кібербезпеки. У своєму виступі Antoni Macierewicz підкреслив, що в сучасному світі кіберпростір - це місце війни не менш важливе ніж суша, море, повітря і космічний простір. За його словами Польща прийняла рішення про створення військ оборони кіберпростору, про збільшення спроможностей Національного центру криптології, про створення офісу для організації кібер-армій та повноважного представника Міністерства оборони для забезпечення безпеки кіберпростору.

Antoni Macierewicz зазначив, що в технологічній сфері існує постійна гонка озброєнь, яка породжує все більш складні загрози. Немає ні інституції, ні

організації, які не піддаються нападам у кібернетичній сфері. Навіть функціонування всієї держави може опинитися під загрозою, - підкреслив він. Якщо ми хочемо створити потенціал у кіберпросторі, нам потрібно визначити природу загроз, - зазначив він [2].

Серед прикладів нападів в кіберпросторі міністр оборони нагадав: параліч веб-сайтів парламенту, міністерств та банківських установ в Естонії в 2007 році, хакерські атаки до та під час саміту НАТО у Варшаві, вірус "Пієта", який завдав шкоди Україні та діяльності російських хакерів під час нещодавнього референдуму в Каталонії.

Всі ці випадки не є окремими діями комп'ютерних хакерів. Це ті заходи, які потребують складного процесу організації, активної підтримки країн, які стоять за цими атаками, - сказав Antoni Macierewicz. Він додав, що урядам все більше треба вживати заходів, пов'язаних з їх безпекою у цій сфері. Як приклад він навів уряд США, який вирішив вилучити з своїх комп'ютерних систем встановлене програмне забезпечення Лабораторії Касперського [3].

Міністр нагадав, що 5 грудня 2016 року Президент Росії Володимир Путін підписав нову доктрину безпеки, яка створює інформаційні армії, і що ми нещодавно спостерігали за тим, як через дезінформацію росіяни намагалися впливати на виборчі процеси в США, Франції, Німеччині та Каталонії.

"Будь-яка держава, яка хоче зберегти своє функціонування, щоб зберегти своє функціонування під час кризи або ІТ-атаки, має побудувати суверенний контроль над телекомунікаційними мережами", - сказав Macierewicz. Як він підкреслив, ця частина критично важливої інфраструктури є "не тільки мішенню потенційних нападів", але залишається "нервовим ядром, що дозволить вижити і відновити контроль над кіберпростором".

Питання захисту кіберпростору досліджуються і вітчизняними фахівцями [4, 5]. Ними розглядаються питання створення та розвитку інформаційного простору держави для забезпечення процесів військового управління.

Нині Україна активно співпрацює з міжнародними партнерами у галузі розвитку систем захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах Міноборони та ЗС України. До штаб-квартири НАТО подано 5 проектів щодо розвитку кібербезпеки ЗС України для їхнього впровадження у рамках Трастового фонду Україна-НАТО з кібербезпеки, головним розпорядником якого є СБ України. В рамках угоди USAI ITI Україна отримала допомогу з підвищення рівня кібербезпеки. Спільно з естонськими колегами розроблено проект зі створення кіберлабораторії на базі однієї з військових частин ЗС України. Безпосередньо зараз проводяться роботи з монтажу обладнання та інсталяція програмного забезпечення у Центрі оперативного реагування на кіберінциденти [6].

Використана література:

1. Інформаційна безпека держави у воєнній сфері. Терміни та визначення : ВСТ 01.004.004 – 2014 (01). – [Чинний від 2014-02-27] – (Військовий стандарт)

2. Powstają wojska do walki w cyberprzestrzeni. Kosztują 2 mld zł Сайт Polsatnews. Дата оновлення 09.10.2017. URL: http://www.polsatnews.pl/wiadomosc/2017-10-09/powstaja-wojska-cybernetyczne-do-walki-w-cyberprzestrzeni-beda-kosztowac-2-mld-zl/(дата звернення: 12.11.2018).

3. Oprogramowanie firmy Kaspersky Lab ma być usunięte z systemów rządowych USA. Дата оновлення 13.09.2017. URL: http://www.polsatnews.pl/wiadomosc/2017-09-13/oprogramowanie-firmy-kaspersky-lab-ma-byc-usuniete-z-systemow-rzadowych-usa/?ref=wyszukiwarka (дата звернення: 12.11.2018).

4. Кацалап В. О., Устименко О. В Створення, розвиток та захист кібернетичного простору воєнної сфери України / Гілея: науковий вісник. Збірник наукових праць /Гол. ред. В.М.Вашкевич. – К.: ВІР УАН, 2013. – Випуск 75 (№8). – С. 519–521.

5. Устименко А. В., Кацалап В. О., Сарычев Ю. А. Киберпространство военной сферы / «Информационная безопасность в свете Стратегии Казахстан-2050»: Сборник трудов I Международной научно-практической конференции (12 сентября 2013 г., Астана). – Астана, 2013. – С. 539–545.

6. Створять кіберлабораторію на базі однієї з військових частин ЗСУ. Дата оновлення 05.11.2018. Сайт Gazeta.ua. URL: https://gazeta.ua/articles/science/ _stvoryat-kiberlaboratoriyu-na-bazi-odniyeyi-z-vijskovih-chastin-zsu/867780 (дата звернення: 05.11.2018).

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

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

СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Розвиток людства призвів до виникнення нових технологій. Сьогодні важко знайти сферу життя, яка обходилась би без інформаційно-комп`ютерних технологій. Майже всі сфери суспільного та державного життя: економіка, інфраструктура й транспорт, освіта, медицина, безпека та оборона, енергетика та інші – охоплені використанням ІКТ на різних рівнях: державному, регіональному та локальному. ІКТ активно застосовуються й у роботі на приватних підприємствах, установах та організаціях.
Уявимо, що в один момент певна особа отримала доступ до таких ІКТ та отримала інформацію, що є конфіденційною або особистою, або запустила певний механізм, який призвів до зупинки транспорту, підприємства, аварії на електростанції. Особливо небезпечним є така маніпуляція з об’єктами атомної енергетики та оборони. Наслідки таких дій є тяжкими: значні матеріальні та людські втрати.

Отже, актуальною є проблема забезпечення кібербезпеки людини, суспільства й держави.

На сьогоднішній день в Україні забезпечення кібербезпеки держави покладено на наступні органи:

1. Міністерство оборони України (та його спеціальні підрозділи – зокрема

Головне управління розвідки).

2.Службу безпеки України.

3.Державну службу спеціального зв'язку та захисту інформації.

4.Міністерство внутрішніх справ України.

5.Службу зовнішньої розвідки.

6.Кіберполіція України.

Зважаючи на наявність органів, на яких покладено забезпечення кібербезпеки, боротьба із кіберзлочинністю та протидії кіберзлочинам залишається неорганізованою.

Зокрема, Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» визначає завдання ДССЗЗІУ: «формування та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації». [1]

Однак, таке обмеження суто захистом державних інформаційних ресурсів не відповідає сучасним тенденціям у сфері боротьби із кіберзлочинністю. Сьогодні є необхідність захисту не тільки державних інформаційних ресурсів, а приватних комп'ютерних мереж та окремих ПК.

Обмеженими є можливості ДССЗЗІ. Вважаємо, що наданих прав недостатньо для забезпечення повноцінного стану кібербезпеки.

Актуальною є проблема координації діяльності цих структур та забезпечення взаємодії для реагування на самі загрози кібербезпеці держави так попередження кіберзлочинності.

Ще однією проблемою є недостатнє забезпечення діяльності таких структур: як кадрово, так і матеріально. Хоча й треба зазначити, що ця ситуація дещо покращилася протягом останніх років.

Однак незважаючи на збільшення фінансування та створення нових органів – Кіберполіції – й залучення фахівців, робота таких структур залишається незадовільною. Яскравий приклад з життя: 12 лютого 2017 року Кіберполіція України оприлюднила на сайті Національної поліції України список учасників т.зв. «груп смерті». Однак перейшовши за посиланнями на сторінки окремих осіб, які розмістила Кіберполіція, виявимо, що велика частка таких акаунтів неактивні й жодного відношення до груп смерті не мають. Так само й незрозуміло, чому Кіберполіція вирішила опублікувати ці списки. Адже навряд чи особі, яка через певні труднощі, долучилася до таких груп, чи її рідним буде приємно побачити себе (чи рідних) у списках на сайті Національної поліції. На нашу думку, в цій ситуації виражається імітація діяльності Кіберполіції замість протидії реальним загрозам.

Отже, на нашу думку, на сьогодні забезпечення кібербезпеки в Україні характеризується наступними проблемами:

По-перше, недостатнє правове регулювання. Сьогодні на законодавчому рівні вже врегульовані такі поняття як кіберпростір, кіберзлочинність, кібертероризм в ЗУ «Про основні засади забезпечення кібербезпеки в Україні», але немає

віідповідальності злочини в кіберпросторі. Це негативно відображається на загальному рівні забезпечення кібербезпеки. Вважаємо за необхідне внесення доповнень до кримінального кодексу України, а саме розділу присвяченого злочинам в сфері кіберзлочинносі .

По-друге, не є визначеним перелік об'єктів критичної інфраструктури, до якої треба включити не тільки об'єкти, що є державною власністю, а й ІКТ, що знаходяться у приватній власності.

По-третє, недостатня координація діяльності органів влади, нечітко визначені їх функціональне призначення та перелік повноважень. Ця проблема має бути вирішена, а органи із забезпечення кібербезпеки – отримати всі необхідні повноваження для здійснення повноцінного захисту інтересів людини, суспільства й держави від реальних та потенційних загроз.

По-четверте, недостатнє матеріально-технічне та кадрове забезпечення. На нашу думку, необхідно розширити склад уповноважених органів якісними фахівцями в галузі інформаційної та кібернетичної безпеки та надати всі необхідні матеріально-технічні ресурси. [4]

З поширенням ІКТ особлива увага з боку керівництва держав та науковців стала приділятись питанню кібербезпеки.

На сьогодні немає єдиного підходу до визначення кібербезпеки. До цього поняття по-різному підходять у зарубіжних країнах, визначаючи як стан захищеності від загроз в кіберпросторі, як стан забезпечення захисту інформації від несакціонованого втручання в роботу ЕОМ. Однак одностайної думки немає ані серед зарубіжних країн, ані в науковців України.

На нашу думку, під кібербезпекою варто розуміти стан захищеності інтересів людини, держави й суспільства від реальних та потенційних загроз, що виникають в сфері роботи об'єктів критичної інфраструктури. Важливою особливістю кібербезпеки є те, що вона спрямована на захист від несанкціонованого доступу до критичної інфраструктури, за допомогою якої здійснюється управління повсякденними процесами. До критичної інфраструктури, зокрема, належать об єкти оборони, енергетики, транспорту та інші.

Кібербезпека – це забезпечення стану, коли ризики втручання в роботу таких систем будуть максимально знижені, коли буде забезпечена захищеність від загроз нормальній роботі систем.

Кібербезпека потребує відповідного правового регулювання, кадрового й матеріально-технічного забезпечення. Однак станом на сьогодні спостерігається проблема забезпечення кібербезпеки України. Це зумовлено неврегульованістю правом ряду питань, відсутністю координації та злагодженої роботи компетентних органів та недостатнім їх кадровим та матеріально-технічним забезпеченням.

Використана література:

1. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006

2. Закон України «Про засади забезпечення кібербезпеки в Україні» від 05.10.2017р.

3. Баранов О.А. ПРО ТЛУМАЧЕННЯ ТА ВИЗНАЧЕННЯ ПОНЯТТЯ “КІБЕРБЕЗПЕКА” [Електронний ресурс]. – Режим доступу: http://ippi.org.ua/sites/default/files/14boavpk.pdf

4. Кібербезпека: світові тенденції та виклики для України [Електронний ресурс]. - К.: НІСД, 2011. – Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf

5. Мінін Д.С. Підходи до визначення поняття «кібербезпека» [Електронний ресурс]. – Режим доступу: http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka

6. Шеломенцев, В. П. Кібербезпека: поняття та сутність [Текст] / В. П. Шеломенцев // Моделювання колективної безпеки: інформаційний вимір : матеріали міжнар. круглого столу, 27 квіт. 2011 р. - К. : НДЦ правової інф-ки НАПрН України, 2011. - С. 66-6

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

Тімофєєва Л. Ю.,
молодший науковий співробітник науково-дослідної частини, асистент кафедри кримінального права Національного університету «Одеська юридична академія»

«ІНТЕРНЕТ РЕЧЕЙ»: ВИКЛИКИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

Стрімкий розвиток технологічних процесів в умовах інформаційного суспільства також породив злочинні посягання на безпеку цієї сфери. Актуалізувались проблеми, пов’язані з «Інтернетом речей», «масовим поширенням спаму», питання прав, обов’язків та відповідальності роботів, штучного інтелекту тощо.

Окремі правові питання, пов’язані з використанням технологій Інтернету речей досліджували: О.А. Баранов, М.В. Карчевський, Н.А. Савінова, В.О. Туляков та ін. Однак в умовах євроінтеграції, а також з урахуванням змін дійсності сприйняття цього питання серед вчених та науковців різне та неоднозначне. Використання технологій «Інтернету речей» породжує як позитивні моменти, так і суттєві ризики, що обумовлює актуальність теми дослідження.

Під «Інтернетом речей» розуміють 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 призначені для надання послуг і проведення робіт в інтересах суб'єктів (юридичних або фізичних осіб). Як зазначає О.А. Баранов, «на даний час суспільство не в змозі приймати обґрунтовані рішення, оскільки сучасний процес їх прийняття характеризується тим, що варто враховувати значні обсяги інформації (даних); велика кількість суб'єктів та об'єктів, які дотичні до процесу прийняття рішень; в більшості випадків необхідно вирішувати в режимі реального або обмеженого часу. Вихід вбачається у застосуванні технологій «Інтернету речей» в силу того, що вони дозволяють приймати та виконувати рішення в режимі реального часу на основі використання математичних алгоритмів, зокрема алгоритмів штучного інтелекту, збору і обробки величезної кількості даних, ідентифікації всіх об'єктів, що беруть участь в процесах» [1].

В сучасних умовах дійсно людина вже не в змозі аналізувати такий великий обсяг інформації, або не в змозі робити це в той короткий термін, в який це необхідно. Використання Big Data (прийняття рішень на основі надвеликих обсягів інформації) [3] та технологій «Інтернету речей» могли б допомогти людині.

Наприклад обробка декларацій в короткий термін та з урахуванням багатьох факторів для аналізу одночасно співвідносячи дану інформацію з іншими джерелами сприяла б своєчасному виявленню корупції, корупційних ризиків та відповідно сприяла б протидії та профілактиці корупції. Тобто «Інтернет речей» сприяв би державі виконувати її функцію щодо забезпечення власної безпеки та безпеки суспільства в цілому.

Держава і зараз готова поступитися фундаментальними гуманістичними правами, свободою та безпекою своїх громадян, моральністю заради безпеки від певних злочинів, зокрема особливо тяжких злочинів із транскордонним виміром. Серед яких наприклад, тероризм, торгівля людьми, сексуальна експлуатація жінок і дітей, незаконний оборот наркотиків та зброї, відмивання та підробка грошей, корупція, комп'ютерна та організована злочинність.

Для попередження вчинення злочинів держава на рівні закону дозволяє відступити від абсолютних заборон посягань на власність, здоров'я та навіть життя людини, а також приватність. Держава обґрунтовує такі кроки відсутністю інших засобів для протидії вчиненню злочинів. Разом з тим, необхідно пам'ятати, що подібні відступи допускають з метою забезпечення прав і свобод людини, а не навпаки.

Хоча останні рішення TARICCO II, ECJ 2017, TSEZAR AND OTHERS v. UKRAINE, ECHR 2018, демонструють пріоритетне значення колективного над індивідуальним (європейські і державні цінності) та повноваження карати своїх громадян [4].

Однак у зв'язку з обробкою та доступністю великих даних, зокрема «великих приватних даних» з'являються інші проблеми, пов'язані з безпекою конкретної людини та її приватної інформації.

Вчені та науковці у сфері віктимології для профілактики віктимізації рекомендують не викладати приватну інформацію в соціальних мережах, або робити це як можна менше (В.О. Туляков) з метою забезпечення власної безпеки.

На думку Х. Зера, **порядок і свобода** – два протилежні полюси. Повна свобода, швидше за все була б небезпечною і хаотичною. З іншого боку, повний порядок, навіть якщо б і був можливий, коштував би нам цієї свободи. Зберігаючи ті цінності, які ми особливо цінуємо, ми не можемо жити в цілковитій безпеці. Але разом з тим, якщо ми не залучаємо до відповіді людей, які намагаються здійснювати свою волю за рахунок чужої волі, під загрозою опиняється наша власна свобода [2, с. 96-97].

Наприклад у сучасному Китаї діє система оприлюднення приватної інформації в публічному доступі, відповідно до якої формується «рейтинг людини» та враховується при прийнятті на роботу тощо. В Україні також (хоча і не офіційно) для окремих посад особа перевіряється в тому числі через дані соціальних мереж та ЗМІ (наприклад для роботи в Антикорупційному суді). Але наскільки ми готові поступатись своєю свободою та приватністю в майбутньому заради безпеки та життя в європейській державі.

Людина відчуває себе безпечно, в тому числі тоді, коли у неї є контроль власного життя. Кримінальна відповідальність в даний час складається із взаємних прав та обов'язків між державою (законність і справедливість), правопорушником (покаранням), жертвами (справедливе поводження) і третіми особами (когнітивний контроль). Взаємні права означають, що потрібно будувати кримінальні норми у напрямку ефективної зміни поводження з людиною з урахуванням потреб усіх учасників [4, с. 65]. Якщо мова йде про використання технологій «Інтернету речей», то вони несуть в собі як позитивні моменти, пов'язані з забезпеченням безпеки держави, однак несуть в собі ризики не спроможності контролювати власне життя громадянами нашої держави. Невідомо хто і з якою метою буде використовувати наші дані та яким чином та за яких обставин вони будуть використані проти нас самих.

Прихильники використання «великих даних» в тому числі для протидії злочину (наприклад, В.М. Карчевський) посилаються на те що правослухняній чесній людині нема чого ховати. Але питання пов'язане не стільки з тим чи є людині що ховати, а з тим чи хоче вона відкривати свої особисті дані в загальний доступ, чи може вона в майбутньому контролювати користування її даними (хто дивився, з якою метою тощо), а також хто буде нести відповідальність за використання таких даних з неправомірною метою, в тому числі вчинення злочинів щодо цієї людини за допомогою її персональних даних, щодо яких вона сама відкрила доступ.

Світ мінливий та живе у відповідності з новими тенденціями, в тому числі

інформаційними. Люди хочуть свободи, хочуть брати участь у вирішенні важливих для них питань, хочуть впливати на їх вирішення, контролювати власне життя, самостійно приймати важливі рішення. В умовах євроінтеграції для України важливо формувати легітимне кримінальне право, тобто таке яке сприймається та приймається громадянами держави, яке спрямоване на потреби людини, зокрема забезпечення безпеки та свободи. Бажано, щоб держава дбала про вигідність вибору правослухняної поведінки (щоб такий вибір не суперечив природним потребам людини, в тому числі приватності).

На євроінтеграційному шляху кримінальний кодекс майбутнього має орієнтуватись на сучасні умови та можливості (зокрема можливості технологій «Інтернету речей»), а також актуальні потреби сучасної людини, в тому числі приватність. Уявляється, що слід почати з домовленостей між державою та громадянським суспільством про їх перелік, завдання кримінального законодавства та межі його втручання, перелік принципів законотворчості та правозастосування. Після чого формувати нове законодавство у відповідності з потребами людини, суспільства та держави, а також приводити у відповідність діюче законодавство.

Використана література:

1. Баранов О. А. «Інтернет речей» як правовий термін / О. А. Баранов // Юридична України. 2016. № 5-6. С. 96-103.
2. Зер Х. Восстановительное правосудие: новый взгляд на преступление и наказание: Пер. с анг./ Общ. ред. Л. М. Карнозовой. Коммент. Л. М. Карнозовой и С. А. Пашина М.: МОО Центр «Судебно-правовая реформа», 2002. 328 с.
3. Карчевський В.М. Можливості Big Data та кримінально-правова комунікація // Політика в сфері боротьби зі злочинністю: Міжнародна науково-практична конференція (м. Івано-Франківськ, 9-10 грудня 2016 р.). С. 52-58.
4. Tuliakov V. «Eurocrimpol» project: methodology of analysis. *Кримінальне право в умовах глобалізації:* матеріали Міжнародної науково-практичної конференції, м. Одеса, 25 травня 2018 року. Одеса: НУ «Одеська юридична академія», кафедра кримінального права, 2018. С. 63-65.

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

Дюльгер М. І.,
аспірант Науково-дослідного інституту інформатики і права НАПрН України

ІНФОРМАЦІЙНА БЕЗПЕКА НА МОРІ В КОНТЕКСТІ ЗАГАЛЬНОЇ БЕЗПЕКИ МОРЕПЛАВСТВА

Актуальність. Термін «морська безпека» наразі не має законодавчого визначення. Він часто вживається як синонім терміна «безпека морського судноплавства». Термін «безпека морського судноплавства» є вужчим за змістом, ніж термін «морська безпека», і, поряд з безпекою експлуатації суден та запобіганням забруднення моря, може розглядатися як одна з її складових. Морська безпека займає своє особливе місце в загальній системі національної

безпеки України. На основі цього важливим є дослідження місця інформаційної безпеки в системі заходів безпеки на морі.

Виклад основного матеріалу. Загальне поняття безпеки надзвичайно широке і полягає у відсутності неприпустимого ризику, пов'язаного із можливістю заподіяння будь-якої шкоди життю, здоров'ю та майну громадян, навколишньому природному середовищу, в реалізації комплексу заходів; у використанні людських і матеріальних ресурсів, які призначені для запобігання такій шкоді; у захищеності населення, об'єктів довкілля, суспільного і державного майна від небезпеки при надзвичайних ситуаціях; у безпечній експлуатації обладнання, споруд, механізмів, що усуває можливість створення загроз для життя, здоров'я та інтересів людини, навколишнього середовища та об'єктів господарювання.

Інтерес та стурбованість станом морської безпеки з боку широкого кола «різногалузевих» фахівців пояснюється тим, що система забезпечення безпеки судноплавства включає в себе багато напрямків: економічний, екологічний, інформаційний [1, с. 132]. Охопивши всі сфери діяльності людини, інформація продовжує чинити вплив на морські відносини.

Різні види безпеки та існуючі чи можливі загрози є не тільки взаємопов'язаними, а й у певній мірі взаємозалежними. Неможливо чітко вказати, які загрози є, умовно кажучи, первісними і які наслідки можуть виступати у ролі вторинних факторів. В кожному конкретному випадку загрози шкода можуть змінювати своє місце в ланцюзі порушення безпеки. Посягання на економічну безпеку може потягнути за собою екологічну шкоду, в інших випадках - посягання на екологічну безпеку може потягнути за собою значну економічну шкоду і так далі. І тому саме інформаційна безпека мореплавання має убезпечувати появу загроз та викликів на морі.

Сьогодні світ проходить третю фазу свого розвитку - і науковці погоджуються, що ця фаза - інформаційна. Її характерна особливість - обіг величезного масиву інформації, споживачами якої є як окрема особа, так і суспільство і цілому [2, с.117]. Це зумовлює формування особливих інформаційних сегментів - власне інформаційного права, інформаційної влади, інформаційно-комунікаційних технологій, що безумовно, виводить на рівень інформаційну функцію держави.

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування [3].

Інформаційно-правові норми, що регулюють рятування на морі, відіграють істотну роль у забезпеченні безпеки мореплавства. В небагаточисленних дослідженнях інформаційної безпеки на морі до зони її впливу відносять: охорону й рятування людського життя, систему передачі інформаційних повідомлень про лихо й безпеку на морі, глобальну морську систему зв'язку, інформаційну діяльність, пов'язану з пошуком та рятуванням на морі [4, с. 247].

Оскільки мореплавство є діяльністю, що має головним чином міжнародний характер, на формування правових норм, які відносяться до нього, природно, значний вплив здійснює прогресивний розвиток і кодифікування міжнародного морського права. Стрімкий розвиток науки і техніки, інтенсивність судно плавання, збільшення розмірів морських суден, терористичні загрози на морі - вказані чинники та ряд інших вимагають посиленої уваги світової спільноти.

Інформаційно-правові норми, що регулюють охорону й рятування людського життя на морі мають вагоме значення у забезпеченні безпеки мореплавства, включаючи охорону людських життів. Глобальна морська система зв'язку під час лиха та для забезпечення безпеки заснована на тому, що пошуково-рятувальні організації, так само як і судна, в районі місця лиха повинні бути у можливо короткий термін сповіщені про аварію і відповідно взяти участь у скоординованій пошуково-рятувальній операції з мінімальними витратами часу [5, с.154]. Це означає, що будь-яке судно незалежно від району плавання повинне бути здатне забезпечити зв'язок, надійний з погляду безпеки самого судна та інших суден, що знаходяться у даному районі. І тому висновок - своєчасне оповіщене під час лиха є найважливішою ланкою підвищення ефективності рятувальних робіт. Тривалість і вартість проведення пошукових рятувальних операцій, так само як і ймовірність порятунку людей, багато в чому залежать від точності визначення координат місця лиха і оперативності передачі інформації під час лиха рятувальній службі.

Міжнародний підхід вданому разі проявляється в розробці та схваленні відповідних конвенцій, кодексів та рекомендацій. Істотним внеском у розвиток міжнародного інформаційно-правового забезпечення технічної безпеки мореплавства стали: Конвенція з охорони людського життя на морі 1974 р. і Протокол до неї 1978 р.; Конвенція про вантажну марку; Меморандумі про контроль за іноземними суднами від 26 січня 1982 р.

Система передачі інформаційних повідомлень про лихо й безпеку на морі - координоване використання різних елементів, включаючи радіозв'язок, для цілей охорони людського життя на морі. Для забезпечення зв'язку між екіпажами суден, а також з береговою владою застосовується Міжнародний звід сигналі. Значну увагу питанням безпеки на морі приділяє і Міжнародна конвенція електрозв'язку 1982 р.

Міжнародні служби електрозв'язку повинні надавати абсолютний пріоритет всім повідомленням, що стосуються безпеки людського життя на морі. Радіостанції зобов'язані приймати з наданням абсолютного пріоритету викликам і повідомленням під час лиха, і таким же чином відповідати на ці повідомлення і негайно вживати до них необхідних заходів [6, с.14].

Розвитком космічної техніки сприяв її застосуванню на морському транспорті для забезпечення надійного радіозв'язку, пошуку і визначення координат суден під час лиха. Система зв'язку під час лиха на морі та для забезпечення безпеки відповідно до вимог Конвенції SOLAS грунтувалася па

тому, що певні класи суден в морі повинні постійно нести радіовахту на міжнародних частотах біди, виділених для цієї мети і включених до Регламенту радіозв'язку. Тобто існуюча морська система зв'язку під час лиха представляла собою систему, яка забезпечувала лише зв'язок судно-судно. Недоліком цієї морської системи зв'язку була неможливість надання допомоги судну, що знаходиться поза зоною спостереження берегової радіостанції, у середньохвильовому діапазоні.

Нова глобальна морська система зв’язку під час лиха і для забезпечення безпеки стала результатом широкої міжнародної співпраці, основною метою якої є впровадження нової супутникової і традиційної техніки зв’язку на морі, має значно підвищити безпеку людського життя на морі. За співпраці міжнародних організацій була розроблена Глобальна морська система зв'язку під час лиха та для забезпечення (ГМЗЛБ). Її мета - сповіщення в найкоротші терміни про аварію пошуково-рятувальних служб та суден в районі аварії. ГМЗЛБ забезпечує зв'язок з позиції безпеки і терміновості, а також передачу інформації, що забезпечує безпеку мореплавства, включаючи навігаційні та метеорологічні попередження.

Забезпечення інформаційного зв’язку на морі - серед основних напрямків мирного використання космічної техніки. Це стосується програми створення космічної системи виявлення морських суден та літаків, що зазнають лиха (КОСПАС- САРСАТ).

Таким чином, характерною тенденцією розвитку інформаційних відносин та зв’язку в морському судноплавстві в XX ст. стала міжнародна співпраця у створенні стандартів на системи різного призначення, однак пов’язаних спільною метою - охороною людського життя на морі. До теперішнього часу міжнародна практика накопичила достатню кількість нормативних актів, що регламентують безпеку мореплавання, інформаційна складова в яких є суттєвою, але інтенсивний розвиток судноплавства вимагає їх розробки на рівні новітніх технологій для ефективного застосування.

Використані джерела:

1. Стрельцова Є. Д. Концептуальне визначення морської безпеки та її місце в загальній системі національної безпеки України// Право и экономика.- Одесса: Астропринт, 2008.- С. 130 - 148.
2. .Ткачук Н. Правове регулювання інформаційних відносин як складова розвитку інформаційного суспільства // Бюлетень Міністерства юстиції України.- 2007.- № 1.- С. 116-122.
3. Корзун В. М. Нормативно-правове регулювання інформаційних відносин в Україні / В.М. Корзун // Форум права. – 2010. – № 1. – С. 175–179 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/201 0-1/10kvmvvu.pdf
4. Іванов Д.А. Історія правового регулювання використання радіозв’язку для пошуку та рятування на морі / Д.А. Іванов // Актуальні проблеми держави і права: Зб. наук. пр. – Одеса: Юрид. л-ра, 2005. – Вип. 26. – С. 246-254.
5. Аверочкіна Т.В. Генеза міжнародно-правового регулювання забезпечення безпеки мореплавства // Т.В. Аверочкіна, Т.М. Плачкова // Lex Portus: юридичний науковий журнал. - 2016.- № 2.- С. 150 – 157.
6. Позолотин Л.А. Управление безопасностью в судоходстве / Л.А. Позолотин,

В.Г. Тоский.- Одесса: Астропринт, 2005.- 180 с.

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

Сказко О. М.,
аспірант Науково-дослідного інституту інформатики і права Національної академії правових наук України

ПИТАННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ УПРАВЛІННЯ ДОМЕННИМИ ІМЕНАМИ

Забезпечення інформаційної безпеки держави, суспільства та особистості постає сьогодні наріжним каменем цивілізаційного розвитку сучасної держави. Формування інформаційного суспільства, окрім безумовних переваг та можливостей для суб'єктів інформаційних відносин, сприяє також збільшенню не існуючих раніше загроз, які проявляються на індивідуальному, суспільному, державному і міждержавному рівнях. Як справедливо вказує О. Д. Довгань, вся наявна нині система зберігання національних інформаційних ресурсів має бути об'єктом і, певною мірою, суб'єктом національної безпеки. В цьому процесі мова йде і про недопущення несанкціонованого, всупереч національним інтересам, використання суверенних інформаційних ресурсів [1, с.112].

Рішенням Ради національної безпеки і оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», яке було введено в дію Указом Президента України від 15 травня 2017 року № 133/2017, до товариств з обмеженою відповідальністю «Яндекс», «Яндекс.Україна», «Мэйл.РУ ГРУП» терміном на три роки було застосовано низку санкцій, у тому числі обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування; заборона Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до низки визначених у вказаному документі ресурсів/сервісів [2]. Цілком поділяючи занепокоєність внаслідок можливого негативного інформаційного впливу держави-агресора на українське суспільство, хотілося б звернути увагу на необхідність створення досконалого правового механізму реалізації вказаних санкцій, а також практичного втілення п.4.2 Стратегії кібербезпеки України, яким передбачено, що кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати розробленні вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами [3]. На нашу думку, у такій ситуації досягнення визначених вище цілей значним чином залежатиме від співпраці органів держави, у тому числі правоохоронних, громадянського суспільства, операторів ринку

телекомунікаційних послуг та інших суб'єктів господарської діяльності в інформаційній сфері.

На жаль, така співпраця ще не може бути визнана достатньо результативною і потребує своєї оптимізації. Деякі прогалини правового регулювання потребують свого заповнення на півні підзаконних правових актів, а відсутність останніх викликає необхідність у відповідних роз'ясненнях. Однак отримання повної і обґрунтованої відповіді на запитання, пов'язані з покладанням на операторів ринку обов'язку щодо здійснення певних обмежувальних дій не завжди можливо. Так, наприклад, 13 червня 2017 року Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки направлено листа за №30/3/4-8236 НТ на імя Інтернет Асоціації України, в якому зазначено, що у ході здійснення комплексу зазначених заходів виявлено порушення вимог чинного законодавства з боку власників доменних імен в зоні «*.ua», «*укр», в т.ч. «*gov.ua». Зокрема, для керування доменними іменами використовуються поштові сервіси російських компаній «Яндекс» та «Mail.ru», щодо яких введені спеціальні обмеження відповідно до Указу Президента України від 15.05.2017 № 133 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Враховуючи вищевикладене, з метою недопущення нанесення шкоди інформаційній безпеці України, Служба безпеки України, відповідно до положення «Про доменний комітет Інтернет Асоціації України» від 28.05.2013 року, просить провести роз'яснювальну роботу з реєстраторами доменних імен про обмеження використання російських поштових сервісів при реєстрації та керуванні доменними іменами. Однак, коли Інтернет Асоціація України своїм зверненням від 26.09.2017 року №165 [4] попросила роз'яснити порядок застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) відповідно до Указу Президента України від 15.05.2017 № 133, Служба безпеки України своїм листом від 18.10.2017 р. №30/1/2-8120 повідомила, що надання консультацій і роз'яснень не входить до її компетенції і порадила звернутися за безоплатною правовою допомогою, яку надають «органи виконавчої влади, органи місцевого самоврядування, фізичні та юридичні особи приватного права, спеціалізовані установи» [5].

В умовах мирного часу недоліки у системі взаємодії суб'єктів інформаційного права негативно позначалися на розвитку інформаційного суспільства, але в умовах ведення проти України гібридної війни проблеми у побудові їх співпраці для досягнення спільних цілей можуть трансформуватися у загрози національній безпеці України. Для того, щоб правовий механізм реалізації таких заходів не суперечив визнаним нашою державою у встановленому порядку міжнародним правовим актам, Конституції та законам України, враховував би позитивний зарубіжний та національний досвід у цій сфері, необхідно проведення у суспільстві широкої дискусії із залученням науковців та практиків, результатами

проведення якої мало б стати напрацювання відповідного правового підґрунтя.

Використані джерела:

1. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право*. 2015. № 2(14). С.111-120.

2. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Указ Президента України від 15 травня 2017 року № 133/2017. URL: https://www.president.gov.ua/documents/1332017-21850.

3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від від 15 березня 2016 року № 96/2016. URL: http://zakon.rada.gov.ua/ laws/show/96/2016#n11

4. Лист Інтернет-асоціації України № 165 від 26.09.2017 щодо прохання ТОВ "Нет Ассіст" надати правові та технічні пояснення щодо ситуації з вимогою блокування деяких ресурсів мережі Інтернет. URL: https://inau.ua/document/lyst-no-165-vid-26092017-zastupnyku-golovy-sbu-shchodo-prohannya-tov-netassist-nadaty.

5. Лист Служби безпеки України від 18.10.2017 р. №30/1/2-8120. URL: https://inau.ua/doclist/2017.

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

Дудіна О. О.,
студент ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Фурашев В. М.,
к.т.н., доцент, с.н.с.

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

В останні роки серед різноманіття сфер забезпечення безпеки державними органами одне з найперших місць займає інформація. Із розвитком технологій поширюються можливості користувачів щодо зберігання, користування та перетворення інформації. Однак, разом із тим, щодо будь-якого об’єкту, чи то предмету матеріального світу (власність), чи то абстрактного поняття (право людини), може бути скоєно злочин. Саме тому наразі стають все більш поширеними правопорушення в сфері інформаційної безпеки. Задля її забезпечення потрібно передбачити ряд заходів, що будуть виконувати превентивну функцію стосовно дій, що можуть посягати на безпеку інформації будь-якого виду. Такі заходи потребують законодавчого закріплення у нормативно-правових актах.

Попри різноманітність та всебічність правової бази досі існує достатня кількість проблемних питань щодо забезпечення інформаційної безпеки, які потребують негайного вирішення.

Разом із науково-технічним прогресом на сучасному етапі поширеним є явище розвитку інформаційних технологій, зокрема всебічне їх використання у всіх сферах життя чи то окремого індивіда, чи то суспільства в цілому, навіть на державному рівні. Більш того інформація стає показником розвиненості та

могутності будь-якого суспільства та має чималий вплив на формування нових багатоманітних сфер життя людини. Таке явище передбачає необхідність забезпечення безпеки інформації у всіх її проявах.

Що ж таке *інформаційна безпека*? В сучасній літературі існує велика кількість визначень цього поняття. Звернімося до роботи «Информационный суверенитет или информационная безопасность?» Олександра Андрійовича Баранова, в якій він визначає інформаційну безпеку як «стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій» [1, с. 72].

А на думку В. Гурковського «національна інформаційна безпека України – це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів» [2 с. 35].

В. Лопатін дає таке визначення інформаційної безпеки: «стан захищеності національних інтересів країни (життєво важливих інтересів особи, суспільства та держави на збалансованій основі) в інформаційній сфері від внутрішніх та зовнішніх загроз» [3, с. 79].

Отже, виходячи із наведених визначень поняття «інформаційна безпека», можна визначити, що його зміст полягає саме у тій практичній діяльності, яку здійснюють задля забезпечення безпеки цієї сфери. Це стосується нормативно-правових актів уряду, науково-дослідних робіт та реальних функцій держави щодо забезпечення виконання законодавчої бази: зокрема, захист інформації та всієї інформаційної інфраструктури. І не дивно, що на сучасному етапі розвитку правового суспільства та в умовах технічного прогресу уряд ставить за пріоритет саме на «технічний бік» проблеми забезпечення інформаційної безпеки. Крім того, зміст цього поняття ґрунтується на суб'єктивних інтересах учасників суспільних відносин у сфері інформації, адже саме їх збалансованість є визначальним фактором забезпечення інформаційної безпеки.

Як і будь-яка інша сфера життя суспільства або держави в цілому, інформаційна сфера потребує законодавчого регулювання.

На думку А. Кузьменка можна виокремити три рівні забезпечення інформаційної безпеки:

– рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);

– суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);

– державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам) [4, с.319].

За роки незалежності український уряд створив чималу кількість нормативно-правовових актів у сфері забезпечення інформаційної безпеки на законодавчому рівні. До таких актів відносяться: Закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних»; Постанови КМУ: «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

Окрім цього існує низка нормативних документів у галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ.

В умовах становлення України як демократичної і правової держави перед органами державної влади стоїть ряд важливих завдань, одним із яких є удосконалення протидії злочинності. Особливу увагу слід звернути на забезпечення ефективної протидії злочинам у сфері інформаційної безпеки.

Підвищена суспільна небезпечність цих злочинів викликана низкою факторів, а саме: складністю їх розслідування, можливістю застосування співучасниками більш ефективних способів підготовки, вчинення, приховування суспільно небезпечних діянь за допомогою використання новітніх технічних засобів.

Незважаючи на значну кількість наукових досліджень, присвячених проблематиці сфери забезпечення інформаційної безпеки, ряд питань так і залишається відкритим.

На сучасному етапі розвитку інформаційного законодавства існує ряд недоліків, а саме: відсутність чіткої ієрархічної єдності законів; велика кількість законів та підзаконних нормативних актів; відсутність узгодження понятійного апарату, термінологічні неточності; нові правові акти в сфері суспільних інформаційних відносин часто не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу. Більш того, все більш гострою стає потреба держави у досвідчених фахівцях з інформаційного права: з кожним роком все більше посилюється беззаперечно негативний вплив ззовні на український інформаційний простір, - виникає загроза так званого «розмивання» моральних

цінностей, етнічних традицій, що відповідають за національну самовизначеність суспільства.

Наступною гострою проблемою правового забезпечення інформаційної безпеки є недостатня конкурентоспроможність України у забезпеченні обсягу вироблення інформаційного продукту, що викликано замалим кількісним складом юристів, що є фахівцями з інформаційного права.

Неналежною є також підготовка нових фахівців у вищих навчальних закладах: їх рівень обізнаності у питаннях інформаційного права та правової інформатики, зокрема правового забезпечення безпеки інформації, є досить низьким, що спричиняє критичний стан застосування технічних засобів та інформаційно-комп'ютерних технологій у галузі державного управління та міжнародних комунікацій.

Враховуючи усе вище сказане, можна стверджувати, що на сучасному етапі розвитку українського суспільства досить поширеним є явище розвитку інформаційних технологій, зокрема всебічне їх використання у всіх сферах, навіть на державному рівні. Більш того інформація стає показником розвиненості та могутності будь-якого суспільства та має чималий вплив на формування нових багатоманітних сфер життя людини. Таке явище передбачає необхідність забезпечення безпеки інформації у всіх її проявах.

Попри різноманітність та всебічність правової бази досі існує достатня кількість проблемних питань щодо забезпечення інформаційної безпеки, які потребують негайного вирішення, а саме: відсутність чіткої ієрархічної єдності законів; велика кількість законів та підзаконних нормативних актів; відсутність узгодження понятійного апарату, термінологічні неточності; нові правові акти в сфері суспільних інформаційних відносин часто не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу. Більш того, все більш гострою стає потреба держави у досвідчених фахівцях з інформаційного права, - їх недостатня кількість спричиняє критичний стан застосування технічних засобів та інформаційно-комп'ютерних технологій у галузі державного управління та міжнародних комунікацій. Тому буде доцільним дослідити зарубіжний та вітчизняний досвід щодо правового забезпечення інформаційної безпеки під час розробки та впровадженні власної національної політики стосовно цієї сфери.

Використана література:

1. Баранов, 2001 – Баранов А. Информационный суверенитет или информационная безопасность? / А. Баранов // Національна безпека і оборона. – 2001. – № 1 (13). – С.70-76.

2. Гурковський В. Т. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дисертація на здобуття наукового ступеня кандидата юридичних наук. Спеціальність : 25.00.02 – механізми державного управління / В. Т. Гурковський. − К., 2004. − 225 с.

3. Лопатин В. Н. Информационная безопасность России : Человек. Общество. Государство / В. Н. Лопатин. − СПб. : Фонд «Университет», 2000. − 428 с.

4. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного

протиборства / А.М. Кузьменко // Часопис Київського університету права. — 2010. — № 4. — С. 317-321.

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

Стародубов В .В.,
студент Гомельського державного університетуімені Франциска Скорини

КІБЕРБЕЗПЕКА В УМОВАХ РОЗВИТКУ ПРАВА РЕСПУБЛІКИ БІЛОРУСЬ

Розвиток інформаційних технологій в сучасних державах послужило величезному ривка комп'ютеризації світового простору. Першою визначальною ідеєю, яка закріпилася в розвитку інформаційних технологій, став упор на вдосконалення ефективності виконання робіт і послуг, діяльності комерційних і державних організацій. Однак створення такого інтернет простору спричинило за собою необхідність забезпечення безпеки, на увазі активного використання інтернет простору злочинним сегментом.

Основним міжнародним документом, який визначив основну концепцію і закріпив важливі тези, стала резолюція ООН від 23 грудня 2015 року, яка відзначила значний прогрес, досягнутий в розробці та впровадженні новітніх інформаційних технологій і засобів телекомунікацій, а також висловила стурбованість, що такі технології можуть бути використані абсолютно в інших цілях. На даний момент держави активно розвивають правову базу регулювання кібербезпеки, проте на увазі дуже швидкої зміни основних складових безпеки в інтернет просторі, державні органи, що відповідають за таку безпеку, а також їх підрозділи повинні бути більш мобільні в такому питанні. Приділяючи питання мобільності та взаємодії окрему категорію, ми стикаємося з проблемою небажання приватного сектора, який розробляє програмні платформи і нові технології, взаємодіяти з державними органами, які здійснюють кібербезпека. Незважаючи на те, що правоохоронний блок готовий допомогти в тому, щоб виключити багато уразливості, приватний бізнес не готовий до цього. Налагодження такого контакту має важливе значення, так як наприклад в іноземних державах існують центри по боротьбі з кіберзлочинністю, що фінансуються приватним сектором. Можливо, приватний сектор Республіки Білорусь ще не готовий контакту з огляду на те, що не вважає кіберзлочинність загрозою. Адже не дивлячись на розвиток такої злочинності, великих масштабів в Республіці Білорусь вона ще не набула і приватний сектор передбачає, що готовий самостійно впорається з такою проблемою. Однак відсутність приватно-державного партнерства в кібербезпеки ставить проблему швидкого і ефективного вирішення проблеми. Такі злочини вимагають швидкої і ефективної реакції на його вчинення, так як процес скоєння злочину і зберігання доказів мають малий проміжок часу [1].

Одними з перших питань, що виникли при регулюванні кібербезпеки стали

співвідношення прав людини і поняття контролю за інтернет простором, державна і комерційна таємниця, загальні питання персональних даних. У Республіці Білорусь дані питання були врегульовані різними законами, що дозволило в короткий термін сформувати чітку правову базу.

Процес здійснення кіберзлочинів включає в себе використання не тільки програмних технологій, але і психології. У разі, якщо безпеку будь-якого об'єкта або бази даних має досить високий рівень і зламати безпосередньо досить складно, то тут застосовуються психологічна методика або виверти.

Основні категорії таких психологічних методик або вивертів:

- Використання суміжного або партнерського об'єкта;

Припустимо, хакер намагається зламати базу даних комерційної організації, однак на увазі якісної системи безпеки у нього не виходить провести злом. Він шляхом елементарного пошуку в інтернеті знаходить комерційні організації або будь-які інші об'єднання, які взаємодіють з такою комерційною організацією і шляхом злому їх електронних систем отримує даних, як першої, так і другої організації в співробітничає організації. Або шляхом проходу через співпрацює організацію, здійснює злом в більш зручній для нього обстановці.

- Використання психології поведінки людей;

Тут мова йде про використання поведінкових реакцій людей або співробітників організації шляхом маніпулювання ними і створення майданчика для таких дій, які необхідні для злому. Тут може бути використана, як банальна розсилка шкідливих програм, з пошти тих осіб, яким користувач відповідного ПК довіряє, так і спроба використання флеш-карт, карт пам'яті співробітників для установки програм шкідливого ПЗ. Простим прикладом таких дій може служити злочин скоєний підлітком, який використавши елементарні прийом психологічного взаємодії різних статей, здійснив установку шкідливого ПО в Мінськійобласті. Підліток створив рейковий сторінку дівчини, після чого зв'язався з викладачем і шляхом спілкування передав йому файл установки MP3 плеєра, давав шкідливою програмою, знайденої їм на профільних форумах, який нібито є дуже якісним. Педагог скачавши файл, встановив його, однак для цієї програми чомусь не працював і підліток зображав дівчину під фейковий аккаунтом, запропонував йому змінити мережеві настройки комп'ютера, після чого отримав доступ до аккаунту викладача і його листуванні. Таким чином, використавши психологію взаємодії різних статей, сформувавши певний довіру шляхом спілкування, погасивши пильність і визначивши уявлення у особи про безпеку файлу він отримав доступ до персональних даних. У такій ситуації чітко показана ефективність взаємодії психології і навичок особи, яка здійснює кібератаки [2].

Використання психології в кіберзлочини багатогранно, тому ми лише обговорили дві тези, для того, щоб зрозуміти яким чином це працює. Безумовно, переважний аспект в організація, які проводять навчання з інформаційної безпеки становлять правила, які забороняють качати будь-які програми, використовувати сторонні карти пам'яті, але маніпулювання дозволяє змушувати людей

порушувати ці правила і найчастіше непомітно для сектора інформаційної безпеки даної організації.

Можна зробити висновок, що інформаційна безпека це багатогранне і постійно змінюється поняття. З огляду на це держава повинна націлюватися на чіткі цілі розвитку кібербезпеки:

- Формування взаємодії правоохоронного і приватного сектора з метою формування спільної протидії кіберзлочинності;

- Формування чітких і жорстких правил контролю, як в державних, так і приватних організаціях, які співпрацюють з відповідними договорами з державними організаціями;

- Постійне інформування співробітників про необхідність дотримання правил інформаційної безпеки, а також постійне інформування про нові методи роботи хакерів, що дозволить актуалізувати кібербезпека.

Використана література:

1. Резолюція, прийнята Генеральною Асамблеєю 23 грудня 2015 року "Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки" URL: https://undocs.org/en/A/RES/ 70/237

2. Інформація УВС Мінoблвиконкомі URL: http://www.belta.by/incident/view/v-minskoj-oblasti-shkolnik-vzlomal-stranitsu-sotsialnogo-pedagoga-i-shantazhiroval-ego-300395-2018/

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

Благодарний А. М.,
к. ю. н.,старший науковий співробітник,
докторант Національної академії
Служби безпеки України

УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ОХОРОНИ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Одним із важливих завдань реформування вітчизняного адміністративного права є модернізація інституту адміністративної відповідальності, зокрема за правопорушення в інформаційній сфері.

Розглядаючи адміністративні правопорушення у сфері обігу інформації, зауважимо, що у чинному законодавстві відсутній нормативний акт, який би містив вичерпний перелік норм, що встановлюють адміністративну відповідальність. Тому у тезах доповіді будуть розглянуті певні особливості адміністративної відповідальності лише за ті правопорушення, які закріплені у Кодексі України про адміністративні правопорушення (далі - КУпАП). Хоча норми, що передбачають відповідальність за правопорушення в інформаційній сфері, містяться і в інших законах, наприклад, ст. 475 Митного кодексу України [1].

При розгляді правопорушень у сфері обігу інформації, відповідальність за вчинення яких передбачена КУпАП, виникають певні складнощі, тому що

зазначений кодекс не має окремої глави, присвяченій саме правопорушенням в інформаційній сфері, а правопорушення, які можна було б включити до цієї глави, розташовані у різних главах Особливої частини КУпАП [2].

У КУпАП, за нашим підрахунком, існує більше 40 статей, що мають безпосереднє відношення до сфери обігу інформації, при цьому, кількість правопорушень значно перевищує кількість статей. Так, наприклад, лише ч. 1 ст. 212-2 КУпАП («Порушення законодавства про державну таємницю») містить дев'ять пунктів, більшість з яких встановлюють відповідальність за декілька різних адміністративних правопорушень у сфері інформаційної безпеки.

Існують різні класифікації правопорушень у сфері обігу інформації, але, на нашу думку, однією з найбільш вдалих є класифікація, відповідно до якої вказані правопорушення поділяються на три групи, що пов’язані: а) з посяганням на інформацію; б) з розповсюдженням інформації, що завдає шкоди; в) правопорушення, пов'язані з посяганням на право громадян та інших суб’єктів на доступ до відкритої інформації [3, с. 71]. Відразу зазначимо, що ця класифікація, як і переважна більшість інших наукових класифікацій, є певною мірою умовною та дискусійною.

Проаналізувавши зміст КУпАП, до першого пункту запропонованої класифікації (**правопорушення, пов’язані із посяганням на інформацію**) можна віднести правопорушення, передбачені ч. 1 ст. 92-1 КУпАП, ч. 2 ст. 163-5 КУпАП; ч. 1 ст. 172-8; ч. 1 ст. 188-39 КУпАП; ч. 1 ст. 195-5 КУпАП; п. 1 ч. 1 ст. 212-2 КУпАП; п. 4 ч. 1 ст. 212-2 КУпАП; п. 5 ч. 1 ст. 212-2 КУпАП; п. 6 ч. 1 ст. 212-2 КУпАП; п. 7 ч. 1 ст. 212-2 КУпАП; п. 8 ч. 1 ст. 212-2 КУпАП; п. 9 ч. 1 ст. 212-2 КУпАП; ч. 1 ст. 212-5 КУпАП; ч. 1 ст. 212-6 КУпАП; ч. 3 ст. 212-6 КУпАП; ч. 4 ст. 212-6 КУпАП; ч. 5 ст. 212-6 КУпАП; ч. 6 ст. 212-6 КУпАП.

До другого пункту класифікації – **поширення інформації, що завдає шкоди**, можна віднести правопорушення, передбачені ч. 3 ст. 96 КУпАП; ч. 1 ст. 148-3 КУпАП; ч. 2 ст. 164-3 КУпАП; ч. 3 ст. 164-3 КУпАП; ч. 2 ст. 166-9 КУпАП; ч. 1 ст. 173-1 КУпАП; ч. 1 ст. 185-7 КУпАП.

Третій пункт класифікації – **правопорушення, пов'язані з посяганням на право громадян та інших суб’єктів на доступ до відкритої інформації**, об’єднує правопорушення, пов'язані з посяганням на право громадян та інших суб’єктів на доступ до відкритої інформації, або на право оприлюднення відкритої інформації. Це правопорушення, передбачені ч. 1 ст. 53-2 КУпАП; ч. 1 ст. 82-3 КУпАП; ч. 1 ст. 91-3 КУпАП; ч. 1 ст. 91-4 КУпАП; ч. 1 ст. 92-1 КУпАП; ч. 5 ст. 96 КУпАП; ч. 1 ст. 163-5 КУпАП; ч. 1 ст. 166-4 КУпАП; ч. 1 ст. 166-6 КУпАП; ч. 1 ст. 166-9 КУпАП; ч. 1 ст. 186-3 КУпАП; п. 2 ч. 1 ст. 212-2 КУпАП; п. 3 ч. 1 ст. 212-2 КУпАП; ч. 1 ст. 212-3 КУпАП; п. 2 ч. 1 ст. 212-4 КУпАП; ч. 1 ст. 212-11 КУпАП.

На нашу думку, законодавцю слід об'єднати всі вказані правопорушення у одному розділі, подібно до того, як це зроблено у КУпАП відносно інших правопорушень, наприклад, правопорушень, що посягають на власність (глава 6 КУпАП).

Вважаємо, що із виділених нами сорока одного адміністративного проступку в інформаційній сфері найбільш шкідливих наслідків обігу інформації

в автоматизованих системах завдають правопорушення, передбачені ст. 212-6 КУпАП «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем».

Як засвідчують матеріали практики провадження в справах про адміністративні проступки, найчастіше об'єктивна сторона правопорушення, передбаченого ст. 212-6 КУпАП, характеризується діяннями у формі незаконного доступу абонентів через мережу Інтернет до інформації, яка зберігається та обробляється в автоматизованих системах інших абонентів (ч. 1 ст. 212-6 КУпАП); незаконного доступу до інформації, яка зберігається, обробляється, передається із застосуванням електронних поштових інтернет-скриньок (ч. 1 ст. 212-6 КУпАП); розміщення без відповідного дозволу копій баз даних на сайтах інтернет-ресурсів (ч. 5 ст. 212-6 КУпАП).

Підсумовуючи зазначимо, що за умови стрімкого розвитку мережі Інтернет особливого значення набуває боротьба з адміністративними правопорушеннями, передбаченими ст. 212-6 КУпАП «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем». Правове регулювання адміністративної відповідальності за правопорушення у сфері обігу інформації в автоматизованих системах має певні недоліки і потребує подальшого вивчення та вдосконалення. Насамперед, необхідно виокремити у КУпАП главу, яка б містила правопорушення у сфері обігу інформації; а також закріпити у чинному законодавстві норми, котрі б передбачали адміністративну відповідальності юридичних осіб за вчинення правопорушень в інформаційній сфері.

Використана література:

1. Митний кодекс України від 13 березня 2012 року № 4495-VI URL: http://zakon.nau.ua.

2. Кодекс України про адміністративні правопорушення від 7 грудня 1984 року № 8073-X URL: http://zakon.nau.ua.

3. Благодарний А. М. Адміністративно-правові заходи охорони інформації в автоматизованих системах / А. М. Благодарний // Інформаційна безпека людини, суспільства, держави. – № 1(14). – 2014. – С. 70-75.

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

Маслова Є. В.,
Аспірант ФСП КПІ імені Ігоря Сікорського

ВІДПОВІДАЛЬНІСТЬ ЗА НЕДОБРОСОВІСНУ ТОРГІВЛЮ В МЕРЕЖІ ІНТЕРНЕТ

Суспільство на сучасному етапі розвитку кожного дня зіштовхується з інформацією, яка впливає та відображається на його розвитку. Це

характеризується неабияким збільшенням використання інформаційних технологій та ролі інформації. Основними чинниками впливу на масову аудиторію є засоби масової інформації та мережа Інтернет, в основі яких лежить головне та основне призначення, а саме задоволення інформаційних потреб окремої людини, суспільства та держави. У зв'язку з приголомшивим розвитком мережі Інтернет стало набато простіше знайти роботу, купити та продати товар, рекламувати продукцію. Та є випадки, коли в мережі поширюється неправдива інформація та й така, що не відповідає дійсності. Тож як особі, яка хоче здійснити покупку через Інтернет бути впевненій в добросовісності продавця, в якості товару, в забезпеченні охорони її споживчих прав та нарешті хто буде нести відповідальність за невиконання своїх зобов'язань. На всі ці та інші питання дає відповідь Конституція України, Цивільний та Господарський кодекси України, Закон України «Про електронну комерцію», Закон України «Про захист прав споживачів», Закон України «Про рекламу», Закон України «Про платіжні системи та переказ коштів в Україні» та інші нормативно – правові акти.

На сьогодні існує багато визаначень поняття «інформація», а проблематиці в інформаційній сфері приділили свою увагу такі вчені як Кормич Б. А., Арістова І. В., Додін Є. В., Олефір В. І., Баранов О. А., Копиленко О. Л. та інші.

Термін «інформація» (informatio) походить з латинської мови, що в перекладі означає ознайомлення, викладення, роз'яснення. У загальному розумінні інформація – це певні відомості, сукупність певних даних, знань [5, с. 6].

На законодавчому рівні в Україні термін «інформація» закріплений в Законі України «Про інформацію» № 2657–XII від 02.10.1992 року. Даний Закон встановлює, що кожен має право на вільне одержання, використання, поширення, зберігання та захист інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Під інформацією слід розуміти будь – які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

Науковець Баранов О.А. в своєму підручнику «Інформаційне право України: стан, проблеми, перспективи» наводить наступне визначення поняттю «інформація»: це відомості, що представлені в будь – якій організаційній формі та вигляді, на будь – яких носіях, про події та явища, які мали або мають місце в суспільстві, державі та навколишньому середовищі. В цьому випадку термін «інформація», як правова катергорія, дозволяє віднести до неї:

– відомості про події і явища, які мали або мають місце в суспільстві, державі і навколишньому середовищі;
– відомості в будь – якій формі і вигляді, на будь-яких носіях;
– відомості, що документовані або публічно оголошені;
– відомості, які не документовані або публічно не оголошені [4, с. 116-117].

Дане визначення більш широко охоплює сферу правовго регулювання суспільних відносин, які пов'язані з інформацією, адже із стрімким розвитком

інформаційних технологій можливість правого регулювання має збільшуватись.

Прийнятий 03.09.2015 року Закон України «Про електронну комерцію» встановлює чіткі обов'язки продавця (постачальника, виконавця) забезпечити прямий, простий, стабільний доступ інших учасників відносин у сфері електронної комерції до такої інформації:

– повне найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи – підприємця;

– місцезнаходження юридичної особи або місце реєстрації та місце фактичного проживання фізичної особи – підприємця;

– адреса електронної пошти та/або адреса інтернет-магазину;

– ідентифікаційний код для юридичної особи або реєстраційний номер облікової картки платника податків для фізичної особи – підприємця;

– відомості про ліцензію (серія, номер, строк дії та дата видачі), якщо господарська діяльність підлягає ліцензуванню;

– щодо включення податків у розрахунок вартості товару, роботи, послуги та, у разі доставки товару, - інформація про вартість доставки;

– інші відомості, що відповідно до законодавства підлягають оприлюдненню [2].

Щодо «інших відомостей», то ця інформація зазначена в Законі України «Про захист прав споживачів» і стосується:

– найменування продавця (виконавця), його місцезнаходження та порядок прийняття претензії;

– основні характеристики продукції;

– ціна, включаючи плату за доставку, та умови оплати;

– гарантійні зобов'язання та інші послуги, пов'язані з утриманням або ремонтом продукції;

– інші умови поставки або виконання договору;

– мінімальна тривалість договору, якщо він передбачає періодичні поставки продукції або послуг;

– вартість телекомунікаційних послуг, якщо вона відрізняється від граничного тарифу;

– період прийняття пропозицій;

– порядок розірвання договору [3].

В тому разі, якщо продавець (постачальник, виконавець) не надав цієї інформації, до нього застосовуються санкції Закону України «Про захист прав споживачів», а саме покупець (споживач) має право: розірвати договір і вимагати відшкодування завданих йому збитків; вимагати надання належної інформації. Також даним Законом до недобросовісних продавців (постачальників, виконавців) застосовуються штрафні санкції [3].

Закон України «Про електронну комерцію» встановлює відповідальність учасників відносин в сфері комерції. Постачальник послуг в інформаційній сфері несе відповідальність за невиконання своїх зобов'язань; забезпечення технічного захисту інформації та здійснення контролю за ним; зміст переданої та отриманої інформації та за шкоду, завдану внаслідок використання результатів таких послуг, за умови відсутності в його діях будь – якої з обставин, що звільняють його від

відповідальності [2].

Отже, на нашу думку, слід зазначити, що купуючи товар через Інтернет покупець унеможливлює своє право на огляд товару, право оцінити його якість та придатність, а тому спрямовує свою увагу та орієнтується тільки на зображення, текстовий опис, відео огляд. Як результат, недобросовісні продавці користуються таким становищем і можуть продавати та реалізовувати неякісний товар, фальсифікат, брак чи контрабанду. Або ж взагалі не надіслати товар чи надіслати товар не з тими технічними характеристиками. Тому, покупцю потрібно звертати увагу на можливість обміну товару, можливість повернення своїх коштів без обміну, а також на опцію «оплата при отриманні» (накладений платіж) будь – то доставка кур'єром чи доставка поштою. Отже, щоб зберегти свої кошти,

убезпечити себе та своє право на скаргу чи звернення із заявою до органів поліції, споживачам (покупцям) потрібно звертати увагу та перевіряти інформацію, яку продавець (постачальник, виконавець) повинен надати згідно до статті 13 Закону України «Про захист прав споживачів».

Використана література:

1. Закон України «Про інформацію» від 02.10.1992 № 2657 – XII // Верховна Рада України. – URL: http://zakon.rada.gov.ua/laws/show/2657-12.

2. Закон України «Про електронну комерцію» від 03.09.2015 № 675-VIII// Верховна Рада України. – URL: http://zakon.rada.gov.ua/laws/show/675-19.

3. Закон України «Про захист прав споживачів» від 12.05.1991№ 1023-XII// Верховна Рада України. – URL: http://zakon.rada.gov.ua/laws/show/1023-12.

4. Баранов О. А.Інформаційне право України: стан, проблеми, перспективи – К.: СофтПрес, 2005. - 316с.

5. Кормич Б. А. Інформаційне право. Підручник. – Харків: БУРУН і К., 2011. – 334 с.

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

Калініченко З. Д.,
к.е.н.,доцент, доцент кафедри цивільно-правових дисциплін Дніпропетровського державного університету внутрішніх справ
Нагорна К. Г.,
здобувач вищої освіти юридичного факультету Дніпропетровського державного університету внутрішніх справ

ПРАВОВІ АСПЕКТИ РОЗВИТКУ КОНКУРЕНЦІЇ НА ФІНАНСОВОМУ РИНКУ

За роки незалежності України в цілому сформовано інституційні засади функціонування фінансового ринку, однак він в певній мірі не відповідає міжнародним стандартам, викликам економіки країни. У цьому аспекті важливим є посилення його відкритості, доступності упорядкованості та конкурентного

розвитку. Тому, актуальним питанням є дослідження функціонального та сутнісного аспекту розвитку вітчизняного фінансового ринку.

У статті 42 Конституції України проголошено, що «держава забезпечує захист конкуренції підприємницькій діяльності. Не допускаються зловживання монопольним становищем на ринку, неправомірне обмеження конкуренції та недобросовісна конкуренція. Види і межі монополії визначаються законом». Таким чином держава взяла на себе функцію захисту конкуренції і проголосила антиконституційними діями зловживання монопольним становищем на ринку, неправомірне обмеження конкуренції та недобросовісну конкуренцію [1].

У науковій літературі державне регулювання фінансового ринку та його складових визначається як система певних методів і прийомів, призначена длявпорядкування діяльності учасників і операцій між ними шляхом встановлення державою певних вимог та правил з метою впорядкування їх взаємовідносин і забезпечення захисту інтересів. Необхідність державного регулювання фінансового ринку обумовлюється такими чинниками: фінансовий ринок є базою для реалізації значної сукупності економічних пріоритетів розвитку країни; забезпечення стабільного функціонування фінансової системи країни в цілому шляхом взаємоузгодження і врівноваження інтересів всіх учасників; правовий захист інтересів інвесторів на фінансовому ринку, що може забезпечити лише держава; зниження інвестиційних ризиків для міжнародних інвесторів; для залучення в процес економічного розвитку вітчизняних інвесторів; координація функціонування фінансових установ і захисту прав споживачів фінансових послуг.

В. М. Сутормiна, В. М. Радзієвська та Б. С. Стеценко зазначають, що фінансовий ринок — це економічний простір, на якому формуються і функціонують відносини між його учасниками з приводу купівлі - продажу фінансових фондів [2].

Функцією держави є регулювання та запобігання подібних ринкових явищ, що повинно здійснюватися шляхом проведення виваженої антимонопольної політики, яку регулює Антимонопольний комітет України, застосовуючи економічні важелі дієвого впливу на підприємства, створення основ політичного, юридичного та соціального характеру, які сприяють ефективному функціонуванню ринку та підприємництва.

Цьому сприяє Закон України “Про захист від недобросовісної конкуренції" від 7 червня 1996 року № 236/96-ВР, який спрямований на встановлення, розвиток і забезпечення торгових та інших чесних звичаїв ведення конкуренції при здійсненні підприємницької діяльності в умовах ринкових відносин [3]. Правові посади підтримки та захисту економічної конкуренції, обмеження монополізму в господарській діяльності й спрямування на забезпечення ефективного функціонування економіки України на основі розвитку конкурентних відносин визначає Закон України “Про захист економічної конкуренції" 2001р. №2210-1[4].

Політика держави у сфері конкуренції спрямована на забезпечення

належних умов, за якими конкуренція могла б виконувати свої позитивні функції повною мірою. Основний принцип державного регулювання - принцип оптимальної інтенсивності конкуренції, - передбачає, що завдяки конкуренції виробничі інновації та науково-технічний прогрес будуть швидко розвиватися. По-друге, - підприємства будуть змушені гнучко адаптуватися та пристосовуватися до зміни умов зовнішнього середовища і, в першу чергу, - до потреб споживачів.

У Законі України "Про фінансові послуги та державне регулювання ринків фінансових послуг" наведено перелік функцій державного регулювання ринку фінансових послуг, які визначають мету і суть регулювання фінансового ринку: проведення єдиної та ефективної державної політики у сфері фінансових послуг; захист інтересів споживачів фінансових послуг; створення сприятливих умов для розвитку та функціонування ринків фінансових послуг; створення умов для ефективної мобілізації і розміщення фінансових ресурсів учасниками ринків фінансових послуг з урахуванням інтересів суспільства; забезпечення рівних можливостей для доступу до ринків фінансових послуг та захисту прав їх учасників; додержання учасниками ринків фінансових послуг вимог законодавства; запобігання монополії та створення умов розвитку добросовісної конкуренції на ринках фінансових послуг [5].

Органи державної влади, органи місцевого самоврядування, органи адміністративно-господарського управління та контролю (далі - уповноважені органи та організації) в межах своєї компетенції ініціюють, розробляють та приймають нормативно-правові акти, адміністративні рішення з метою забезпечення економічних, соціальних, регіональних, природоохоронних та інших напрямів державної політики. Переважна більшість нормативно-правових актів та адміністративних рішень не створює проблем для функціонування конкуренції на товарних ринках, проте в окремих випадках можуть надмірно обмежувати підприємницьку ініціативу, встановлювати завищені вимоги до господарської діяльності в окремих галузях, надавати переваги окремим суб'єктам господарювання чи галузям, і, тим самим, негативно впливати на ефективність та конкурентоспроможність економіки у довгостроковій перспективі.

Поява нових конкурентів зазвичай обумовлюється розробкою нових товарів, більш ефективних методів виробництва, розширенням асортименту та географічних меж реалізації та каналів дистрибуції продукції окремими суб'єктами господарювання. Розширення асортименту товарів та послуг забезпечує встановлення цін на конкурентному рівні [6].

Гарбар Ж.В. зазначає, що перспектива появи нових конкурентів, розширення діяльності існуючими конкурентами, сприймається іншими суб'єктами господарювання як певна загроза їх ринковій позиції, а отже, є джерелом конкурентного тиску. Регулювання кількості або кола учасників ринку знижує рівень конкурентного тиску на учасників ринку і, як наслідок, негативно впливає на конкурентне ціноутворення і, як правило, на якість товарів та послуг.

Крім того, зменшення або обмеження кількості чи кола учасників ринку може сприяти узгодженню ринкової поведінки між суб'єктами господарювання, що залишаються на ринку, спонукати їх до розподілу ринку, узгодження цін, зниження обсягів виробництва та стримування інновацій [7].

Погоджуємось з деякими дослідниками, що конкуренція, з одного боку, — це економічна змагальність за досягнення кращих результатів у сфері якої-небудь діяльності, боротьба товаровиробників за вигідніші умови господарювання, одержання найвищого прибутку. З іншого боку, конкуренція — елемент ринкового механізму, що забезпечує взаємодію ринкових суб'єктів у виробництві та збуті продукції, а також у сфері додавання капіталу.

Використана література:

1. Конституція України (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141) від 30.09.2016 – с. 45
2. Сутормінa В. М. Фінансовий ринок: навч. посібник / В. М. Сутормінa, В. М. Радзієвська, Б. С. Стеценко. — К.: КНЕУ, 2011. — 100 с
3. Закон України "Про захист від недобросовісної конкуренції" від 7 червня 1996 року № 236/96-ВР від 03.03.2016 – с. 45
4. Закон України "Про захист економічної конкуренції" від 11 січня 2001 року №2210-111 від 07.03.2018 – с. 85
5. Закон України Про фінансові послуги та державне регулювання ринків фінансових послуг 2664-III, від 01.10.2018 – с. 56
6. Про затвердження Методичних рекомендацій щодо оцінки впливу нормативно-правових актів та проектів актів на конкуренцію v0117226-17, від 14.11.2017 – с. 78
7. Гарбар Ж.В. Розвиток інститутів інфраструктури фінансового ринку України / Ж.В. Гарбар // Вісник Львівського університету. Серія «Економіка». – 2013. – Вип. 50. – С. 32-42

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

Гапанович Я.В.
к.н.держ.упр.,
керівник Науково-виробничого центру підвищення кваліфікації, працевлаштування та виробничої практики ОНАЗ ім. О.С. Попова

РОЗВИТОК Е-ДЕМОКРАТІЇ ТА Е-УРЯДУВАННЯ: ШЛЯХ ПОШУКУ

На початку XXI століття у світі набули стрімкого розвитку цифрові технології, що обумовило їх використання для інформатизації суспільства, у тому числі для забезпечення розвитку демократичних процесів, державного управління та боротьби з корупцією. Кожна країна йде своїм шляхом у цьому напрямку, що залежить від багатьох впливових факторів. До таких факторів, по-перше, слід віднести форму державного правління та політичний режим. В не демократичній, тоталітарній державі, практично не постає питання застосування інструментів е-демократії. По-друге, це рівень корупції. В корумпованих країнах набагато важче впровадити і розвивати механізми електронного урядування

(далі - е-урядування) та електронної демократії (далі - е-демократії), тому що це не вигідно корумпованим елітам і окремим особам владних повноважень. По-третє, це ступінь розвитку інформаційно-телекомунікаційної інфраструктури. Наявність в адміністративно-територіальних одиницях (село-район-місто-регіон-держава) достатньої кількості телекомунікаційних мереж операторів та якісних інфокомунікаційних послуг, також є впливовим фактором. В-четвертих, значного впливу на розвиток е-урядування та е-демократії має рівень цифрової грамотності населення. Як би стрімко не розвивались технології в середовищі операторів електронних послуг, але можливість отримувати такі послуги залежить від обізнаності громадян, здатності користуватися кібернетичним середовищем та засобами електронної взаємодії, а також від наявності у споживачів послуг відповідних кінцевих пристроїв (технічних засобів телекомунікацій) і програм.

В Україні нормативно-правовий процес забезпечення е-демократії розпочався із прийняття таких нормативно-правових актів, як Законів України «Про національну програму інформатизації» [1], «Про електронні документи та електронний документообіг» [2], «Про електронний цифровий підпис» [3] і набув розвитку з прийняттям Закону України «Про електронні довірчі послуги» [4].

Основні принципи, термінологія, інструменти е-демократії визначені Концепцією розвитку електронної демократії в Україні, що була схвалена Кабінетом Міністрів України у 2018 році [5]. План заходів з її реалізації передбачає: забезпечення застосування єдиної політики у сфері електронної демократії, сприяння підзвітності громадянину суб'єктів владних повноважень, удосконалення механізму висвітлення інформації про діяльність органів державної влади, удосконалення інструментів електронної демократії на загальнодержавному та місцевому рівнях, забезпечення розвитку електронної ідентифікації фізичних і юридичних осіб в державних інформаційно-телекомунікаційних системах, підвищення якості статистичної та аналітичної інформації у сфері електронної демократії, поширення практики використання інструментів електронного голосування, забезпечення відкритості використання публічних коштів, забезпечення розвитку відкритих даних, популяризація електронної демократії, формування знань і навичок користування її інструментами з урахуванням доступності інформації для осіб з інвалідністю, зокрема із сенсорними порушеннями (в тому числі слуху та зору), забезпечення проведення дослідження та візуалізації стану розвитку електронної демократ в Україні.

Аналізуючи готовність суспільства до виконання таких завдань, слід зазначити, що нормативно-правова база з питань е-демократії, інформатизації і розвитку інформаційного суспільства вже є застарілою і потребує удосконалення. Громадськість має запит на комунікацію з фахівцями з метою подолання «цифрового розриву» та оволодіння новими технологіями. Таким чином, процес реалізації політики розвитку е-демократії та е-урядування слід вирішувати і «зверху» і «знизу».

Так, у Законі України Про національну програму інформатизації зазначено, що інформатизація – це сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки [1, с. 1]. Зрозуміло, що питання забезпечення е-демократії теж входять до таких потреб громадян. Проте, ні національна, ні регіональні програми інформатизації не містять багатьох питань, що пов’язані з розвитком е-демократії та е-урядування.

Слід зазначити, що програми також не містять у собі і конкретних заходів із забезпечення: розвитку цифрової економіки і великих даних, побудови єдиної інфокомунікаційної інфраструктури. Поряд із зазначеним, у програмах потребують висвітлення питання розвитку секторів електронної демократії та електронного урядування, такі як: ІТ-архітектура системи е-урядування та е-демократії міст та регіону в цілому; формування ресурсів е-урядування та е-демократії (людських, матеріальних, не матеріальних тощо); створення інструментів електронної демократії у суспільному житті; розробка чистих відкритих даних; застосування комплексної системи захисту інформації з підтвердженою відповідністю (забезпечення кібербезпеки) для соціуму, громад та бізнесу (захист інформації та персональних даних людини, мереж, електронного середовища тощо); електронна взаємодія органів публічної влади, громадян та бізнесу із застосуванням зручних електронних систем; електронні послуги закладів вищої освіти, організацій і бізнесу; створення систем Електронне місто, Електронний регіон; впровадження Електронного документообігу та діловодства в діяльність суб’єктів економічної діяльності, організацій, закладів вищої освіти; розбудова цифрової економіки міст та регіону в цілому; усталення процедур ідентифікації, аутентифікації особи у кібернетичному просторі; опис основних усталених критеріїв та показників гарантування процесів.

В програмах не зазначено засади фінансування на основі державно-приватного партнерства. Не закладено основ залучення наявних бізнес-ресурсів регіону (інформаційні системи, телекомунікаційні мережі, канали зв’язку, авторське програмне забезпечення тощо).

Це означає, що програми за своїм визначенням мають бути спрямовані не лише на інформатизацію органів державної влади, але й на розвиток е-демократії, всіх складових життєдіяльності суспільства із застосуванням ІКТ, а найперше – на інформатизацію громад і громадян, розвиток реального сектору економіки, науки і освіти, медицини тощо. Цей процес повинен підлягати державному та громадському контролю.

Особливо необхідним є сьогодні пошук шляхів для удосконалення цифрових навичок громадян і публічних службовців, працівників бізнесу (цифрового навчання осіб), розвитку навчальної компоненти електронного

урядування та електронної демократії, підготовка фахівців (впровадження в закладах вищої освіти нової спеціальності 281 «Публічне управління та адміністрування»), у тому числі з використанням елементів дистанційного навчання. Цю роботу можливо виконувати на матеріальній базі закладів вищої освіти, або залучати волонтерів, створювати цільові групи із підготовлених фахівців та працювати в регіональних громадах спільно з органами публічної влади та громадянами.

Використана література:

1. Про національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР URL: http://zakon.rada.gov.ua/laws/ show/74/98-%D0%B2%D1%80 . – Назва з екрану.
2. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV URL: http://zakon.rada.gov.ua/laws/show/851-15 . – Назва з екрану.
3. Про електронний цифровий підпис : Закон України від 22.05.2003 № 852-IV URL: http://zakon.rada.gov.ua/laws/show/852-15. – Назва з екрану.
4. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII URL: http://zakon2.rada.gov.ua/laws/show/2155-19 . – Назва з екрану.
5. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації : Постанова Кабінету Міністрів України від 08.11.2017 № 797-р URL: http://zakon2.rada.gov.ua/laws/show/797-2017-%D1%80. – Назва з екрану.

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

Костенко О. В.,
головний науковий співробітник (установи) Інституту спеціальної техніки та судових експертиз Служби безпеки України

ПРАВОВІ ПИТАННЯ РЕГУЛЮВАННЯ ДОВІРЧИХ ПОСЛУГ В МІЖНАРОДННИХ АКТАХ UNCITRAL

Запровадження нових форм міжнародної співпраці, а саме електронного транскордонного співробітництва є одним із пріоритетних напрямків розвитку світового співтовариства. Електронне транскордонне співробітництво, в тому числі із використанням транскордонних довірчих послуг, на сьогодні потребує законодавчого регулювання.

Одним із локомотивів міжнародного правотворчого процесу в галузі електронних довірчих послуг, електронних підписів виступає Комісія ООН з міжнародного торговельного права, Міжнародної торгової палати і Європейської економічної комісії (UNCITRAL, Комісія). UNCITRAL затверджено закон «Про електронну комерцію» («Model Law on Electronic Commerce») та Типовий закон «Про електронні підписи» («Model Law on Electronic Signatures with Guide to Enactment 2001». Ці законодавчі акти стали класичною основою для створення нормативно-правових актів практично всіх країн в галузі електронної торгівлі та електронного підпису, заклали загальні принципи транскордонного визнання сертифікатів електронного цифрового підпису.

Починаючи із 2014 року Робочою групою IV з електронної торгівлі UNCITRAL здійснюються заходи щодо вирішення правових питань, пов'язаних із управлінням ідентифікаційними даними та довірчими послугами. UNCITRAL розглядає процес юридичного визнання довірчих послуг та цифрових підписів як необхідність визначення правових вимог та створення відповідних матеріально-правових норм в будь-якій юрисдикційній системі.

Однак на сучасному етапі розвитку міжнародного та національного права в сфері використання довірчих послуг та цифрового підпису в транскордонному режимі не врегульованим залишається низка глобальних проблем.

Проблема термінології. Проблема полягає в тому, що національні законодавства або міжнародні законодавчі акти містять сукупність понять та визначень, які мають суттєві відмінності та інколи носять надмірно технічний характер, що ускладнює сприйняття простими громадянами [1].

Проблема облікових даних, як складової цифрового підпису та довірчих послуг. Як відомо, з ключових компонентів цифрового підпису є дані про підписувача, які прийнято рахувати як цифрові облікові дані. На сьогодні жодним законодавчим актом не врегульовані питання транскордонного визнання цифрових облікових даних, а саме: хто повинен проводити таке визнання, якою стороною вони повинні підлягати визнанню, яка мета такого взаємного визнання, які характерні елементи повинні бути наявними для взаємного визнання, які обмеження можливо застосувати під час взаємного визнання. Також поза межами правової регуляції наразі знаходиться проблема застосовування взаємного визнання ідентифікаційних даних юридичних осіб, цифрових пристроїв або цифрових об'єктів.

Проблема довіри до електронних послуг та цифрових підписів.

Можливість запровадження технічних механізмів забезпечення надійності довірчих послуг існує і може бути оперативно реалізовано. Однак, на сьогодні відсутні міжнародні правові механізми, що гарантують певний рівень та норми довіри цифровим послугам однієї із сторін, що обмінюються такими послугами. У багатьох національних ідентифікаційних системах, в тому числі і в Україні, визначені так звані «рівні забезпечення довіри», як в Європейському Союзі («низький», «високий» і «основний»). В той час як в Сполучених Штатах і в деяких інших країнах використовується чотири рівні забезпечення довіри.

Проблема транскордонної інтероперабельності. Держави з різною правовою культурою традиційно розходяться в технічній та правовій оцінці цифрового підпису. Країни загального права (США, Великобританія) не пред'являють особливих технічних та юридичних вимог до цифрового підпису, а також не вимагають обов'язкового проставляння цифрового підпису одночасно всіма учасниками довірчої послуги або електронного документа. При цьому електронний підпис може бути створено будь-ким і за будь-якої технології. У романо-германських правових системах (переважно у країнах Європи), де правова доктрина традиційно відігравала істотну роль, склалася інша концепція цифрового

підпису.

З метою вирішення вказаних проблем Робочою групою IV за участю багатьох країн світу вивчаються перспективи правового регулювання визнання транскордонних довірчих послуг та цифрових підписів шляхом розробки загальних, стандартизованих міжнародних правових актів. У своїй діяльності UNCITRAL планує вивчити досвід кількох проектів в сфері електронних довірчих послуг:

- Європейської комісії, Регламент (ЄС) № 910/2014;
- Євразійського економічного союзу, Договір про Євразійський економічний союз та Концепції використання послуг та юридично значимих електронних документів у міждержавній інформаційній взаємодії;
- Азійсько-Тихоокеанського регіону, Паназійський альянс за розвиток електронної торгівлі. [2]

Також Робочою групою IV вивчаються існуючі міжнародні документи, спрямовані на забезпечення взаємного визнання транснаціональних правових наслідків у паперовому середовищі, такі як Конвенція, що скасовує вимогу легалізації іноземних офіційних документів «Конвенція про апостиль» (Гаага, 5 жовтня 1961 року) і Протокол про єдиний порядок дій за дорученням, виконуваних за кордоном (Вашингтон, 17 лютого 1940 року), які можуть містити відповідні рекомендації щодо мінімальних елементів для транскордонного взаємного визнання УІД і довірчих послуг.

Питанню юридичного визнання транскордонних довірчих послуг приділена достатня увага різних країн.

Так, Російською Федерацією запропоновано проект «Вдосконалення системи управління ідентифікаційними даними під час використання транскордонного простору довіри і загальної інфраструктури довіри у застосуванні до транскордонних електронних комерційних угод». В основі проекту закладено модель, яку визначено у Модельному законі «Про транскордонний інформаційний обмін електронними документами» від 25 листопада 2016 року. Згідно проекту пропонується створити багато кластерний вертикально інтегрований «транскордонний простір довіри», який матиме три рівні електронних довірчих послуг (базовий, середній, високий). Кластер може мати єдиного міжнародного регулятора, регуляторів міждержавних союзів та національних регуляторів цифрових довірчих послуг та цифрових підписів. Також передбачається запровадити правові рівні регуляції цифрових довірчих послуг на одно- або багато доменній основі із залученням третьої незалежної довірчої сторони, а також уніфікацію міжнародної та національних нормативних баз [3].

Натомість Сполучні Штати Америки вважають за необхідне в найближчій перспективі розглянути тему юридичного визнання ідентифікаційної інформації, що пройшла автентифікацію в зв'язку з комерційною операцією, а саме, що являє собою юридичне визнання його мета, вимоги, юридичне забезпечення тощо.

Пропозиції Австрії, Бельгії, Італії, Сполученого королівства Великобританії та Європейського Союзу стосуються можливості встановлення узгоджених рівнів

безпеки, які забезпечуються за допомогою довірчих послуг: перший рівень - із застосуванням некваліфікованих довірчих послуг. Другий рівень із використанням кваліфікованих довірчих послуг. За другим рівнем правові наслідки будуть включати асиміляцію, презумпцію, перенесення тягаря доведення на супротивну сторону, а також принцип взаємного транскордонного визнання для довірчих послуг, що мають однаковий рівень безпеки.

Україна, як активний член світового процесу цифровізації здійснює певні кроки в напрямку осучаснення законодавства в галузі цифрового підпису та довірчих послуг, а саме запровадила новий Закон України «Про електронні довірчі послуги». Україна шляхом змін чинного законодавства адаптує нормативно-правову базу відповідно до Регламенту (ЄС) №910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС.

Висновки.

Сьогодні існує безліч національних і регіональних концепцій і ініціатив в сфері довірчих послуг, які вже досить добре опрацьовані. Вони дозволяють виявити відповідні проблеми і можуть служити базою при розробці належних правових рамок на міжнародному рівні, які можна було б перенести в різні вже існуючі правові системи.

Робочою групою IV з електронної торгівлі UNCITRAL здійснюються заходи, спрямовані на досягнення наступних цілей:

- сприяння розвитку права міжнародної торгівлі і задоволення потреби економічних суб'єктів в інструментах, що дозволяють забезпечити юридичну визначеність скоєних ними електронних угод;

- сприяння узгодженню нових правових аспектів проектів, в рамках яких ці питання в даний час вирішуються на національному або міжнародному рівні розрізнено, наданню загальним вимогам, сформульованим у діючих текстах ЮНСІТРАЛ, більш конкретного і функціонального змісту;

- створенні загальної правової основи, яка застосовується до довірчих послуг та цифрових підписів, включаючи відповідні положення, спрямовані на розвиток міжнародної транскордонної оперативної взаємодії в правовій і технічній галузях.

На нашу думку, законотворцям України доцільно більше врахувати світовий досвід в розробці нормативно-правових актів, що регулюють сферу довірчих послуг та цифрових підписів, в тому числі в транскордонному режимі.

Використана література:

1. A/CN.9/WG.IV/WP.150. United Nations. URL: http://undocs.org/ru/A/CN.9/WG.IV/WP.150 (дата звернення 09.11.2018)

2. A/CN.9/902 United Nations. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V17/029/30/PDF/V1702930.pdf?OpenElement (дата звернення 07.11.2018)

3. A/CN.9/WG.IV/WP.143 United Nations. URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V17/008/33/PDF/V1700833.pdf?OpenElement (дата звернення 05.11.2018)

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

Гавловський В. Д.,
к.ю.н., с.н.с. Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України

ДО ПИТАННЯ ПРОТИПРАВНОГО ВИКОРИСТАННЯ ІНТЕРНЕТ РЕЧЕЙ

Інтернет речей (IoT) продовжує зростати прискореними темпами. Відповідно до огляду, підготовленого виданням Forbes, міжнародний ринок IoT до 2020 року збільшиться з 157 млрд до 457 млрд доларів. Аналітики компанії Ericcson вважають що кількість IoT пристроїв до 2022 року досягне позначки в 18 млрд. За деякими прогнозами до 2025 року - може досягти 100 млрд, при цьому значна їх частина буде генерувати великий обсяг даних, що будуть передаватися за допомогою бездротових телекомунікацій [1-3].

З ростом кількості пристроїв, що підключаються, збільшуються і проблеми у сфері їх безпеки. Голова Федеральної торговельної комісії США Едіт Рамірес озвучила три основні проблеми, пов'язані з використанням IoT:

– всеохоплюючий збір даних;
– потенціал несподіваного використання призначених для користувача даних;
– підвищені ризики безпеки [4].

На думку Джона Кука, директора відділу продакт-менеджменту в компанії Symantec, усі ці проблеми у сфері безпеки є результатом гонки на ринку. Він зазначив, що: «Багато виробників IoT пристроїв сьогодні переживають період, який можна порівняти з періодом Золотої Гарячки – кожен поспішає вийти на ринок. Є дійсно багато людей, які не думають про безпеку»[5].

Одна з основних проблем, повзаних з використанням IoT, полягає у великому різноманітті пристроїв, технологій і захисних рішень, через які вкрай складно реалізувати єдиний підхід до забезпечення безпеки середовища. До того ж захист істотно підвищував би їх собівартість.

На відміну від традиційних комп'ютерів і планшетів, підключені до Інтернету речі залишаються вкрай уразливими для вторгнення. Проникнення стає можливим завдяки тому, що більш ніж 70% пристроїв, які входять в IoT, мають уразливості, в 60% з них – небезпечний web-інтерфейс.

Варто зазначити, що на сьогодні Інтернет речей призводить до нових способів вчинення злочинів. На думку фахівців Європолу, найбільшу загрозу в найближчі три-п’ять років будуть становити саме IoT, кількість яких постійно збільшується. Повсюдне поширення Інтернет речей, а потім й імпламентація електронних компонентів в тіло людини, відкривають принципово нові можливості для різного роду злочинів, раніше ніяк не пов’язаних з кіберзлочинністю.

Оскільки пристрої IoT підключаються до домашньої або корпоративної мережі, вони можуть легко забезпечити шлях для хакерів, щоб отримати доступ до інших систем, зокрема банківських рахунків і персональних даних.

Існує багато прикладів вразливостей безпеки в IoT. Найбільш яскравим прикладом є багаторазово збільшені можливості для дистанційних вбивств завдяки втручанню або в мережі «розумних будинків» і електронних приладів, або в електронні пристрої, що регулюють ті чи інші імплантанти або органи життєдіяльності людини. Наприклад, люди використовують кардіостимулятор, в «розумному будинку» підключають його до своєї мережі. Це дозволяє програмі автоматично викликати «швидку допомогу» під час серцевих нападів. Такі програми створюють лікарське замовлення і можуть проводити його самостійно в онлайн-аптеках. Хакер може перехопити таке замовлення, додавши туди небезпечні ліки. Або ще простіше – замкнути кардіостимулятор, вбивши людину. Якщо в програмному забезпеченні стимулятора не виявлять вірус, то смерть будуть констатувати як нещасний випадок.

Сьогодні злочинці для збирання інформації про потенційних жертви використовують найрізноманітніші розумні речі, навіть дитячі іграшки, які все частіше оснащуються різними електронними модулями, та гаджети для тварин (веб-камери, автоматичні годівниці і поїлки, електронні іграшки, датчики температури та ін.), які мають підключення до мережі Інтернет, а отже, можуть стати інструментом у руках кіберзлочинців.

Одним з перспективних напрямів цієї злочинної діяльності в найближчі роки також будуть несанкціоновані проникнення через IoT у «розумні будинки» і ведення спостереження за власниками з подальшою метою подальшого шантажу, пограбування або навіть вбивства. За допомогою камер спостереження зловмисник може повністю відстежити режим дня господарів і з'ясувати, в який час вони бувають вдома, може заздалегідь намітити, що саме він хоче вкрасти. І якщо класичні «злодії-домушники» готують один злочин, то кіберзлочинці можуть паралельно відстежувати відразу кілька будинків чи квартир і в потрібний момент «здійснити напад» на всіх сусідів, не привертаючи уваги.

Усе частіше для виявлення IoT використовуються ботнети, завдяки яких кіберзлочинці отримують можливість швидко просканувати мережу Інтернет в пошуках потрібних цілей.

Варто відмітити, що в розвинених країнах приділяється значна увага формуванню державної політики у сфері Інтернет речей:

США: прийнято рішення про розробку національної стратегії Інтернету речей (2016 р.); подано до Сенату законопроект «Розвиток інновацій і сприяння Інтернету речей» (січень 2017р.);

Велика Британія – прийнята «Цифрова стратегія Великої Британії 2017»;

Південна Корея – прийнято Генеральний план створення IoT (2014 р.);

Японія – прийнято «Стратегію зростання Японії – 2016» (Індустрія 4.0, розвиток IoT, великих даних, робототехніки);

Китай – розроблена та виконується державна програма розвитку Інтернету речей ($ 127,5 млрд) до 2020 року; заплановано перетворення 500 міст на smart city (2017 р.);

ОАЕ – призначено Міністра з питань штучного інтелекту (жовтень 2017 р.) [6].

В Європейському Союзі над законодавством стосовно Інтернету речей, вже працює агентство з кібербезпеки ENISA.

Отже, розвиток Інтернету речей є загальносвітовою тенденцією, що створює нові умови функціонування суспільства. Разом з тим, IoT призводить до нових способів вчинення злочинів. З метою протидії цьому насамперед має бути сформована державна політика у сфері Інтернет речей. Вітчизняні законодавчі та нормативно-правові новації у цій сфері мають враховувати кращі зразки світової практики.

Також для стримування зазначених негативних процесів необхідно вдосконалювати кримінальне законодавство, слідчу, судову та прокурорську практику у кримінальних провадженнях, пов'язаних з вчиненням кіберзлочинів, оперативно-розшукову діяльність, спрямовану на виявлення і припинення діяльності в кіберпросторі як окремих злочинців, так і організованих злочинних груп. Крім того, необхідно вивчити зарубіжний досвід щодо можливостей застосування Інтернет речей для запобігання злочинності й впроваджувати його в практичну діяльність.

Використана література:

1. 2017Roundup Of Internet Of Things Forecasts.URL:https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6ce937a81480

2. Massive Growth in Internet of Things (IoT) Market Evidenced by Skyrocketing Number of Connected Devices. URL: https://www.prnewswire.com/news-releases/massive-growth-in-internet-of-things-iot-market-evidenced-by-skyrocketing-number-of-connected-devices-683570101.html

3. Баранов О.А. Інтернет речей (IoT): правові моделі використання обмеженого радіочастотного ресурсу. URL: http://ippi.org.ua/sites/default/files/7_4.pdf

4. Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. URL: https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

5. IoT Security Concerns Peaking – With No End In Sight. URL: https://threatpost.com/iot-security-concerns-peaking-with-no-end-in-sight/131308/

6. Баранов О.А. Інтернет речей (IoT): огляд правових проблем. URL: http://ipp.kpi.ua/wp-content/uploads/2017/11

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

ДЛЯ НОТАТОК

Наук ове видання

Інтернет речей: проблеми правового регулювання та впровадження

Друга науково-практична конференція
29 листопада 2018 року

В авторській редакції
Комп'ютерна верстка авторська

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Перемоги, 37,
м. Київ, 03056

Підп. до друку 26.12.2018. Формат 60×84$^{1}/_{16}$. Папір офс. Гарнітура Times.
Спосіб друку – ризографічний. Ум. друк. арк. 9,16. Обл.-вид. арк. 16,24. Наклад 55 пр.
Зам. № 18-144.

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