Комітет Верховної Ради України з питань інформатизації та зв'язку
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет соціології і права

ІНТЕРНЕТ РЕЧЕЙ: ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ТА ВПРОВАДЖЕННЯ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
24 жовтня 2017 року

Київ
КПІ ім. Ігоря Сікорського
2017

УДК - 34:004.738.5](063)
І - 73

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.

Матеріали конференції 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 інетнету речей. Доповіді учасників конференції можуть бути корисними для спеціалістів у сферах правотворення, правозастосування та правоохоронної, вчених, фахівців та експертів різних галузей права, науково-педагогічних працівників, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться сучасними суспільно-правовими тенденціями і проблемами наслідків сучасного науково-технічного прогресу, в першу чергу, з позицій забезпечення інформаційної безпеки людини, суспільства та держави, забезпечення прав і свобод людини.

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

ISBN 978-966-622-861-4

Матеріали подано у авторській редакції.
Упорядники: **Фурашев В. М., Петряєв С. Ю.**

Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП КПІ ім. Ігоря Сікорського
designlab.kpi.ua@gmail.com
Балашов Д. В. (balashov.dim@gmail.com)

Рекомендовано до друку:
Вченою радою Науково-дослідного інституту інформатики і права
Національної академії правових наук України.
Протокол № 7 від 01.11.2017 р.

Вченою радою факультету соціології і права
Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Протокол № 3 від 30.10.2017 р.

ISBN 978-966-622-861-4

ЗМІСТ

Баранов О. А.,
д. ю. н., с.н.с., керівник Центру теоретико–правових проблем інформаційної сфери НДІ інформатики и права НАПрН України

ІНТЕРНЕТ РЕЧЕЙ (IoT): ОГЛЯД ПРАВОВИХ ПРОБЛЕМ

Людство у 20 - х роках XXI століття має невтішні результати свого господарювання на планеті: практично вичерпано ресурси чистого повітря, вуглеводів, корисних копалин, лісів, прісної води, родючих земель тощо. Окрім того до списку додалось глобальне потепління, нестача продовольства, перенаселенні міста, перевантажена інфраструктура. Це все є наслідком невдалих рішень, які приймало людство протягом всієї своєї історії. Таким чином воно вичерпало ліміт на свої помилки. Дійсно, 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 (IoT) 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.

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).

За даними експертів в 2025-2030 роках буде:

- 80-100 мільярдів підключень до мережі Інтернет (сьогодні – біля 16 млрд.);
- $ 7-19 трильйонів буде складати світовий ринок IoT;
- 1 трлн. євро буде складати ринок технологій IoT у Європі;
- Індустрія 4.0 – дозволить отримати додатковий дохід: 30 млрд євро (Німеччина) та 110 млрд євро (Євросоюз).

Вбачається, що у 2030-2040 році технології Інтернету речей дозволять:

- 10-15% - економії бюджету на охорону здоров'я;
- 10-15 років – збільшення тривалості життя;
- 40-50 % - збільшення врожайності;
- 15-20% збільшення пропускної здатності доріг у містах;
- 85-90 % зменшення кількості автомобілів;
- 10-15 разів зменшення витрат на логістику.

З врахуванням думок багатьох вчених, фахівців, експертів та на основі аналізу тенденцій розробки та впровадження технологій Інтернету речей (IP) можна стверджувати, що після 2020 року (початку офіційного запуску технології мобільної передачі даних 5G) траєкторію розвитку людства, країн, бізнесу, окремих людей може бути спрямовано у двох стратегічних напрямах: або до успіху та розквіту за умови використання технологій IoT, або до стагнації та занепаду за умови невикористання технологій IoT.

З огляду на це, багато країн приділяють значну увагу формуванню державної політики у сфері Інтернету речей:

США: прийнято рішення про розробку національної стратегії Інтернету речей (2016 р.); подано до Сенату законопроект «Розвиток інновацій и 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 роста 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.).

На шляху розвитку технологій IP існують певні бар'єри та ризики. До системних бар'єрів можна віднести наступні: відсутність державної стратегії та національного лідера змін; слабке розуміння цінностей IP керівниками компаній і галузей, фахівцями та пересічними громадянами. До решти таких бар'єрів належать : політичні, фінансово-економічні, техніко-технологічні, забезпечення безпеки, конфіденційності, сумісності, стандартизації, правового регулювання, освітянські та мотиваційні.

Вважаємо, що правове регулювання суспільних відносин, пов'язаних з IoT, має відбуватись за базовим принципом: правове регулювання має сприяти використанню технологій IP в інтересах людей.

У правовій сфері в умовах використання технологій IP основні бар'єри та ризики полягають у необхідності розроблення нових правових моделей регулювання: цивільних відносин; телекомунікацій та використання спектра; забезпечення конкуренції; використання штучного інтелекту та роботів; використання smart - контрактів; захисту інтелектуальної власності; захисту приватної власності; забезпечення конфіденційності тощо.

Звернення до загальної пошукової системи Google та бази наукових праць Google Академія дає наступні результати: за словами «internet of things» близько 553 млн. та біля 3 млн. посилань, а за словами «legal regulation of the Internet of things» – біля 173 млн. та понад 291 тис. посилань. Це свідчить про неабияку цікавість у світі до проблеми Інтернету речей, зокрема з правової площини.

З аналізу наукових джерел та із дослідження правової тематики можна припустити, що існують три підходи до вирішення проблем правового регулювання в умовах використання ІЗ:

•чинного законодавства достатньо для регулювання відносин, пов’язаних з IP;

•потрібне лише деяке вдосконалення існуючих законів;

•необхідно створення нових правових інститутів або навіть нової галузі права.

На наш погляд, проблем правового регулювання дуже багато, що потребує диференційованого підходу до кожної з них з урахуванням можливостей трьох вище названих пунктів.

Наприклад, впровадження та використання технологій IP в медицині робить нагально актуальними такі правові дослідження:

1. Законодавче регулювання надання послуг е-медицини, зокрема, надання їх в дистанційному режимі.

2. Встановлення меж та змісту юридичної відповідальності для медичного персоналу, операторів телекомунікацій, виробників обладнання та розробників програмного забезпечення.

3. Правовий режим допуску на ринок медичних послуг автономного програмного забезпечення для мобільних засобів, дистанційній діагностики, інноваційних засобів, що керуються дистанційно тощо.

4. Правовий режим допуску на ринок медичних послуг, приборів та діагностичних апаратів.

5. Визначення законодавчих вимог щодо прозорості інформування населення про всі особливості надання медичних послуг з використання технологій IoT.

6. Правове регулювання збору інформації та дистанційного доступу до е-картки пацієнта.

Якщо говорити про інші сфер суспільних відносин то, до прикладу, у сфері телекомунікацій – це правові дослідження , котрі спрямовані на:

- відміну ліцензування діяльності, лібералізацію ринку та введення економічних санкцій за порушення вимог законодавства;
- створення прозорих умов для конкуренції;

- посилення захисту прав споживачів;
- посилення регуляторної влади НКРЗІ;
- посилення повноважень ЦОВЗ у формуванні державної та технічної політики;
- введення правового режиму Sharing при користуванні РЧР, можливість створення операторів MVNO;
- законодавчого введення принципу технологічної нейтральності у використанні РЧР;
- введення правового режиму колективного та спільного користування спектром, використання білих діапазонів (White Space) РЧР, вторинного ринку (Spectrum trading) РЧР.

Якщо вести мову при розгортанні робіт з перетворення міст України на «smart city» , то варто зауважити про необхідність докласти зусилля з правових досліджень та зосередити увагу на:

1. юридичному визначенні терміну «розумне місто»;
2. прискоренні адміністративних процедур прийняття рішень органами місцевого самоврядування щодо інфраструктурних проектів;
3. визначенні правового режиму сумісного використання інфраструктурних об'єктів – електроенергетики, водопостачання, газопостачання, опалення, телекомунікацій, освітлення, відеоспостереження;
4. визначенні юридичних вимог щодо застосування сучасних технологій при новому будівництві або капітальному ремонті житлових та інфраструктурних об'єктів;
5. вдосконаленні муніципального законодавства в частині сприяння впровадженню технологій IoT;
6. законодавчих змінах щодо регулювання містобудівної діяльності, землекористування тощо.

В умовах Інтернету речей з’являється багато нових технологій та засобів, використання яких потребує відповідного правового супроводження, наприклад:

1. 3D принтери: визначення правових умов для захисту права на інтелектуальну власність; встановлення правових вимог щодо запобігання незаконному перехвату програм, які вони виконують.

2. Робомобіль: зміни Віденської Конвенції щодо дорожнього руху; ліцензування допуску до експлуатації; правова регламентація перевірки системи автоматичного керування та програмного забезпечення; встановлення юридичної відповідальності за ДТП; правовий режим створення та функціонування дорожньої інфраструктури; регламентація керування використанням персональними даними тощо.

3. Дрони: правове регулювання безпеки польотів по відношенню до суб'єктів і об'єктів, що знаходяться в повітрі та на землі; правовий режим введення оперативних обмежень; правовий режим надання дозволів на політ, на збір даних, ліцензій пілотам тощо.

В повній мірі це стосується й новел, які привносять технології IP у юридичну сферу діяльності. Актуальними будуть наступні дослідження, наприклад, для smart-контрактів:

1. Інтеграція правового регулювання їх застосування в традиційну правову систему.
2. Визначення юридичного статусу, вимог до його форми і змісту.
3. Встановлення юрисдикції (за наявності транскордонних транзакцій).
4. Вивчення особливостей правовідносин, об'єкту та змісту.
5. Визначення юридичних ризиків та обмежень використання.
6. Встановлення правових механізмів нагляду, визначення відповідальності, зокрема, при наявності помилок в комп'ютерній програмі.
7. Визначення правових вимог щодо забезпечення достовірності фіксації подій в реальному світі, які є причиною для здійснення певних дій сторін.
8. Встановлення правових механізмів верифікації сторін контракту.
9. Вирішення правовими засобами протиріччя між захистом персональних даних і відкритістю інформації по всіх транзакціях мережі блокчейнов, яка є базою для smart-контрактів.

10. Пропозицій щодо удосконалення процесуальних кодексів.

Особливу групу правових проблем складають ті, що виникнуть при застосування технологій ІР зі штучним інтелектом ШІ, які в сучасній літературі мають назву роботів.

Виходячи зі змісту дискусій про перспективи правового регулювання в умовах застосування технологій ІВ і використання ШІ, можна констатувати наявність трьох основних гіпотез, які власне і визначають основний зміст наукових підходів 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.

Практично третя гіпотеза є суперпозицією двох перших і якщо вони будуть справедливі, то третя також буде мати місце, тому в подальшому будемо розглядати тільки дві перші гіпотези.

Звичайно, багато дослідників, в тому числі й юристи, перш за все, на підставі багатовікового досвіду з надією звертають свою увагу на історично підтверджені правові механізми регулювання суспільних відносин припускаючи, що саме вони дозволять з одного боку - уникнути загроз, які можуть виникати завдяки використанню роботів, і про які останнім часом стали говорити лідери сучасної науки і техніки, а з іншого – створити максимально сприятливі умови для інвестицій і досягнення всього того позитивного, що дає широкомасштабне використання роботів. Але з іншого боку багато вчених припускають, що в недалекому майбутньому роботи можуть бути суб'єктом правових відносин.

Підставою для формулювання перших двох гіпотез є такі узагальнені варіанти уявлень про роль роботів в суспільних відносинах:

1. Роботи, в тому числі з штучним інтелектом, виключно тільки допомагають реалізовувати звичайні суспільні відносини, в яких суб'єктами виступають традиційні юридичні і фізичні особи. При цьому, ці суспільні відносини принципово можуть бути здійснені й без роботів, функція яких може бути реалізована іншим способом, але швидше за все, менш ефективним.

2. Роботи-андроїди або андроїди можуть виступати «стороною» у відносинах, в яких інша сторона - це традиційні юридичні і фізичні особи. Чому роботи можуть бути стороною відносин? Тому, що вони «самостійно» можуть оцінювати дії інших суб'єктів і в залежності від результатів цієї оцінки також самостійно формувати або змінювати мету та зміст своїх дій. Або тому, що їх дії не можуть бути заздалегідь передбачені, так як вони здійснюються під впливом непередбачуваних мінливих обставин або під впливом емоцій і свідомості робота. Іншими словами, роботи в цьому випадку 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.

Визнання справедливості другої гіпотези означає визнання необхідності досить серйозного реформування традиційного законодавства. Цілком ймовірно, що при цьому не вдасться обмежиться простою зміною суб'єктного складу правовідносин за рахунок додавання роботів з ШІ. 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. 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?

Узагальнюючи результати аналізу процесу розвитку та впровадження технологій IP, стан дискусії з правових питань застосування технологій IP можна сформувати загальні напрями майбутніх правових досліджень в частині напрацювання теоретико-методологічних основ та практичних рекомендацій щодо:

1. Визначення засад правового регулювання суспільних відносин в умовах «взаємодії»:

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

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

Крім того, необхідно проводити науковий пошук у напрямах:

1. Проведення правових досліджень відносно всіх сфер діяльності в соціумі, пов'язаних із забезпеченням:

- лібералізації та конкуренції на багатьох ринках;
- захисту прав споживачів;
- визначення відповідальності;
- приватності (захисту персональних даних);
- безпеки, зокрема кібербезпеки;
- захисту інтелектуальної власності та авторського права;

2. наданням телекомунікаційних послуг.

3. Проведення правових досліджень, пов'язаних із використанням технологій IoT у: промисловості, сільському господарстві, банківський сфері, енергетиці, медицині, освіті, державному управлінні, ретейлі, збройних силах тощо.

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

Пилипчук В. Г.,
д. ю. н., професор, член-кореспондент НАПрН України

СТАНОВЛЕННЯ І РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН У СФЕРІ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ІНТЕРНЕТ РЕЧЕЙ)

Протягом останніх років в Україні та світі активного поширення і розвитку набувають нові суспільні відносини, пов'язані зі сферою Інтернет речей. Поняття ***«Інтернет речей»*** (англ. – Internet of Things) розглядається як *мережа різноманітних об'єктів, що збільшується, – від промислових пристроїв до споживацьких товарів і послуг, які можуть обмінюватися інформацією і виконувати свої задачі, поки людина працює, відпочиває або займається спортом*.

Технології Інтернет речей, як відомо, складаються з мільйонів датчиків та різноманітних пристроїв, що генерують безперервні потоки даних, котрі можна застосовувати для поліпшення різноманітних сфер життєдіяльності людини, суспільства і держави.

Питання розробки і впровадження технологій Інтернет речей активно обговорюється в Україні з кінця XX століття. Водночас, системний розгляд проблем становлення і регулювання суспільних відносин у цій сфері лише започатковується вченими НДІ інформатики і права НАПрН України, НТУУ «КПІ» та створеного ними Навчально-наукового центру інформаційного права і правових питань інформаційних технологій за участі Комітету Верховної Ради України з питань інформатизації і зв'язку.

Відповідно, комплексне опрацювання правових проблем у вказаній сфері та шляхів їх вирішення все ще перебуває на початковому етапі. За цих умов, як видається, першочергового розгляду потребують такі питання:

- визначення пріоритетних напрямів розвитку технологій Інтернет речей в Україні та їх юридичного оформлення;
- аналіз та систематизація суспільних відносин, що формуються у цій сфері, та розробка пропозицій стосовно їх правового регулювання;

- забезпечення прав і безпеки людини, насамперед, захист персональних даних у зв'язку із розвитком технологій Інтернет речей.

За результатами аналізу, 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.

В різноманітних системах Інтернет речей використовується і буде використовуватися багато відомостей і даних, що характеризують приватне життя людини. Тому, забезпечення інформаційної безпеки в частині захисту персональних даних в разі застосування Інтернет речей не варто розглядати як просте завдання.

Іншим ризиком є те, що в умовах взаємозв'язку великої кількості систем і комплексів Інтернет речей, які будуть надавати послуги або здійснювати роботи в інтересах великої кількості людей, значно спрощується можливість одержання всебічних персональних даних про людину з різноманітних джерел. Тому цілком очевидним є те, що широкомасштабне використання технологій Інтернет речей призведе до виникнення та подальшої ідентифікації багатьох нових проблем, пов'язаних із захистом персональних даних.

У матеріалах звіту Федеральної торгової палати США (2015 р.) відображено практично увесь спектр думок щодо ***проблеми захисту персональних даних*** у цій сфері, а саме:

- *переваги впровадження Інтернет речей зводяться до мінімуму наявністю негативних наслідків, наприклад, загрозами конфіденційності персональних даних;*
- *зайве регулювання з питань захисту персональних даних може призвести до уповільнення інвестицій у будь-який сектор;*

- *прийняття необхідного регулювання для гарантованого захисту персональних даних підвищить довіру споживачів до нових технологій;*
- *необхідно дочекатися проявів негативних наслідків і, тільки після цього, вживати заходів з регулювання;*
- *доцільно використовувати механізми саморегулювання замість регулювання законодавчими нормами.*

У зазначеному звіті робиться висновок про потребу у спеціальному законодавстві для сфери Інтернету речей.

Результати дослідження проблеми захисту персональних даних при застосуванні технологій Інтернет речей, за нашими оцінками, дають змогу дійти деяких висновків:

а) технології Інтернету речей значно посилюють ризики порушення конфіденційності персональних даних про конкретну людину, що викликає цілком закономірні питання про надійність зберігання таких даних та забезпечення їх захисту від несанкціонованого використання;

б) широке використання технологій Інтернету речей призводить до необхідності вирішення таких основних правових проблем:

- визначення механізмів реалізації принципу попередньої згоди на використання та вилучення персональних даних;
- врегулювання порядку використання персональних даних інтелектуальними комплексами, що функціонують без участі суб'єктів (юридичних або фізичних осіб);
- необхідності створення багаторівневої і багатооб'єктної системи захисту персональних даних та регулювання транскордонних потоків персональних даних в умовах євроінтеграції України.

Щодо останнього йдеться про необхідність імплементації правових стандартів ЄС з питань захисту персональних даних, визначених законодавством ЄС ***(Пакетом захисту даних)***, зокрема, Регламентом (ЄС) 2016/679 від 27.04.2016 р., Директивою (ЄС) 2016/680 від 27.04.2016 р. Європейського Парламенту і Ради, Директивою (ЄС) 2016/681 від 27.04.2016

р. Європейського Парламенту і Ради та внесення необхідних змін до законодавства України. Звернімо увагу, що норми вказаних правових актів ЄС мають застосовуватися з травня 2018 року не лише у країнах-членах ЄС, а також у державах, які співпрацюють з ними.

В контексті євроінтеграції і розвитку новітніх інформаційних технологій також варто звернути увагу на рекомендації «місії Кокса» та розробленої нею дорожньої карти щодо ***реформування*** і підвищення спроможності ***парламенту України***. Вказані рекомендації, окрім низки організаційно-правових, матеріально-технічних та інших заходів, передбачають розвиток новітніх інформаційних технологій для висвітлення діяльності Верховної Ради України і залучення широкої громадськості до обговорення законопроектів, а також створення механізмів активного залучення правової науки та інших галузей науки до аналізу відповідних суспільних відносин та розробки правових шляхів їх регулювання.

Одним із перших кроків для цього може бути впровадження окремої ***бюджетної програми*** щодо здійснення ***наукових експертиз*** стратегій, концепцій, програм, законопроектів, механізмів впровадження новітніх технологій.

Загалом, в контексті розвитку технологій Інтернет речей та суспільних відносин у цій сфері варто звернути увагу на необхідність пошуку шляхів вирішення і правового врегулювання низки актуальних проблем:

1) ***оптимізації системи державного управління*** в умовах формування новітніх суспільних (цифрових) відносин та розвитку системи електронного управління, у т.ч. з використанням складових моделей «розумний дім», «розумне місто» тощо;

2) ***розвитку прогнозної функції права*** як однієї з ключових умов ефективного правового регулювання в контексті стрімкого впровадження Інтернет речей та інших інформаційних технологій;

3) комплексного опрацювання проблеми ***захисту прав і безпеки людини*** в інформаційній сфері та подолання прірви між безпрецедентними можливостями Інтернет-середовища і традиційними, «доцифровими»

юридичними нормами і практиками, базованими на традиційному уявленні про межі й засоби забезпечення приватності життя людини.

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

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

ТРАНСФОРМАЦІЇ СИСТЕМИ ОСВІТИ В КОНТЕКСТІ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ

Публікація містить результати досліджень, проведених при грантовій підтримці Держаного фонду фундаментальних досліджень за конкурсним проектом Ф73/24456.

Нещодавнє ухвалення Закону України «Про освіту» спричинило неабиякий суспільний резонанс, але, в першу чергу, саме через негативну реакцію політичних кіл Угорщини та Румунії щодо так званої «мовної статті». Разом з тим, ґрунтовний аналіз Закону з позицій векторів формування якісного людського капіталу залишився поза громадською увагою, за винятком неоднозначних оцінок окремих експертів. Відзначимо, що сфера освіти – це та царина суспільного відтворення, де результатом і продуктом її функціонування є поставання особистості у багатоманітні проявів своїх знань, умінь, навичок, цінностей тощо. Відтак, законодавство про освіту повинне бути не просто таким, яке адекватно відповідає нинішнім реаліям, а воно повинне мати випереджальний характер. Динамічність соціальних перетворень вимагає від законодавця використання бодай спрощених модусів форсайту перспектив розвитку людського потенціалу, майбутньої структури ринку праці і т.д.

Одним з ключових чинників формування нової соціальної реальності став швидкоплинний перехід від Інтернету людей до Інтернету речей (Internet of Things). Величезна кількість публікацій з посиланнями на оцінки аналітиків компанії Cisco засвідчують, що умовною точкою відліку щодо суспільної концептуалізації «Інтернету речей» вважається період з 2008 до

2009 рр., коли кількість пристроїв інтегрованих до глобальної мережі перевищила чисельність населення нашої планети. Звичайно, проблема нерівномірності соціального, технологічного і економічного розвитку між різними країнами світу вносить певні корективи щодо оцінювання глобального характеру Інтернету речей. Але враховуючи той факт, що вже відбулася певна об'єктивація Інтернету речей у системі суспільних відносин, можемо вести мову про зміну характеру діяльності людини у виробничих та інших процесах. Така зміна характеру діяльності, яка буде відбуватиметься й надалі пришвидшеними темпами, вимагатиме релевантної трансформації системи освіти. Сьогодні академічна спільнота повинна дати відповідь на низку питань: які види професійної діяльності можуть «піти у небуття», а які нові з'явитися?, якими компетентностями повинен буде володіти фахівець через 5-10 років, незалежно від отриманої професії?

Відповіді на ці питання можуть дати дослідження перспектив розгортання Інтернету речей у економічному, технологічному, соціальному компонентах суспільного життя. Важливо, що академічна спільнота розвинених країн світу вже почала активно шукати відповіді на вказані запитання. Так, авторитетне американське видання EDUCAUSE Review, яке досліджує проблеми освіти, присвятило у минулому році окремий спецвипуск зі статтями, присвяченими результатам досліджень впливу Інтернету речей на вищу освіту. В Україні показовим прикладом того, що в системі вищої освіти вже є усвідомлення об'єктивності існування феномену Інтернету речей є започаткування у 2017 року в Львівській політехніці освітньої програми «Інтернет речей» в межах спеціальності «Комп'ютерні науки та інформаційні технології». На думку керівника цієї програми, львівського науковця Наконечного А.Й. «сьогодні вища освіта потребує перетворень направлених на задоволення потреб в інженерах і вчених, чия діяльність буде тісно пов'язана з технологією Інтернет речей» [1]. Звичайно, згадана програма спрямована тільки на підготовку технічних фахівців, які будуть удосконалювати ІТ-інфраструктуру. В свою чергу, в нашому

дослідженні ми здебільшого хотіли б сконцентрувати увагу на потенціалі освітньої системи в частині формування у будь-яких фахівців таких професійних і особистісних компетентностей, які б дозволили їм бути більш ефективними у своїй професійній діяльності і, разом з тим, розвивали і утверджували гуманістичну складову суспільних відносин.

Можна виділити декілька складових впливу Інтернету речей на систему освіти. Крім суттєвого впливу на якість освітнього процесу і, відтак, його результату, Інтернет речей дозволяє підвищити рівень безпеки учасників освітнього або наукового процесу. Зокрема, йдеться про проблему безпеки людини і громад. Адже, до прикладу, інтегровані в систему громадської безпеки камери відеоспостереження, які пов’язані з комп’ютерами та девайсами , дозволяють або запобігти протиправній діяльності злочинців, або швидше реагувати на інцидент, що відбувся. З іншого боку, використовуючи вказані можливості заклади освіти повинні враховувати необхідність забезпечення приватності і конфіденційності учасників освітнього процесу на основі принципу дотримання розумного балансу.

З високою ймовірністю інтеграція Інтернету речей у систему освіти буде відбуватися швидкими темпами, незважаючи на те, що за оцінками аналітиків наразі тільки близько 10% установ в розвинених країнах розгортають Інтернет речей у своїй діяльності. У звіті, підготовленому Консорціумом нових медіа «Horizon Report - 2015 Higher Education Edition» за 2015 рік, вказуються очікування того, що «Інтернет речей буде мейнстрімом в університетах та коледжах протягом чотирьох-п'яти років» [2]. З іншого боку, засоби Інтернету речей мають значний потенціал для забезпечення поглибленого навчання. Так, наприклад, бібліотеки на основі накопичених даних можуть сприяти використанню різних моделей використання навчальних матеріалів, оптимальних для конкретного користувача бібліотечних ресурсів. Зокрема, пристрої з е-текстом на основі фіксування кількості часу, який витрачається на вивчення електронних підручників і співвіднесенні цього з успішністю студента, відображеною в

університетських базах даних (результатами атестацій, іспитів тощо), можуть пропонувати моделі активізації навчальної діяльності.

Таким чином, розробляючи стратегію або політику щодо розгортання систем Інтернету речей, варто зважати на складність та відносну новизну цього явища та ймовірне виникнення непередбачуваних соціальних ефектів.

Література:

1. Наконечний А. Й. Інтернет речей, захоплення чи перспективна технологія [Електронний ресурс] / А. Й. Наконечний / / Матеріали XIII міжнародної конференції «Контроль і управління в складних системах (КУСС-2016)», м. Вінниця, 3-6 жовтня 2016 р. - Електрон. текст. дані. - Вінниця : ВНТУ, 2016. - Режим доступу : http://ir.lib.vntu.edu.ua/handle/123456789/13105.

2. NMC. “Horizon Report - 2015 Higher Education Edition” - Режим доступу: http://cdn.nmc.org/media/2015-nmc-horizon-report-HE-EN.pdf

3. Benson Ch. The Internet of Things, IoT Systems, and Higher Education / Chuck Benson // EDUCAUSE review. – July/August, – 2016. – P.32-45

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

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

ТЕХНОФІЛІЯ VS. ТЕХНОФОБІЯ: РОЗВИТОК ЦИВІЛІЗАЦІЇ ЯК РОЗВЯЗАННЯ СУПЕРЕЧНОСТЕЙ МІЖ НОВІТНІМИ ТЕХНОЛОГІЯМИ ТА КУЛЬТУРНИМИ ТРАДИЦІЯМИ

За ознаками схильності чи неприхильності культур до засвоєння технологічних винаходів їх варто поділити на чотири типи: *технофіли-донори (інноватори); технофіли-адоптери; технофіли-транслятори; технофоби.*

Оскільки перші писемні згадки вказують на винахід колеса в Месопотамії (шумерська цивілізація) за 3,5 тис. років до н.е., то цю культуру, безумовно, варто віднести до технофільно-донорської. Предмет національних гордощів китайців – чотири великі відкриття (компаса, друкарського верстата, паперу й пороху) – теж надає підстави до віднесення цієї культури до того ж *технофільно-донорського* типу.

Арабські народи й Візантія свого часу зіграли історичну роль *технофілів-трансляторів,* передавальної ланки між винахідливим Сходом і технофобним Заходом епохи Середньовіччя, коли під забороною опинилися зокрема дослідники-алхіміки, які намагалися віднайти в лабораторіях таємниці «філософського каменю» та інших потужних модифікаторів недосконалого людського тіла.

Вочевидь, у тих випадках, коли між певною культурою та технологіями виникав взаємокорисний симбіоз, *цивілізації*. В інших випадках, коли цей симбіоз розпадався або ж подібний перехід з певних соціотехнічних причин не відбувався, певні племена й народи, володіючи більш-менш розвиненими культурами, не досягали одначе стадії цивілізованості.

Утрируючи цей момент, Освальд Шпенглер протиставив, як відомо, *культуру* цивілізації, вважаючи що цивілізованість й високі технологічні досягнення є ознакою не прогресу культур, а навпаки - культурного виродження, закостеніння суспільства, до ознак якого відніс: послаблення традицій та релігії; урбанізацію; засилля техніки й технологій; занепад мистецтва; формування масової культури і *«омасовлення» всього життя, що означає його розвиток на основі кількісного принципу, який знаходить свій вияв у глобалізації форм і методів людського існування: господарства, політики, техніки».*

Під *цивілізацією* слід розуміти рівень як культурної, так і техніко-технологічної розвиненості суспільства, досягнутої ним на певному відтинку історичного процесу, що характеризується високими здобутками духовної та матеріальної культури, ступенем освоєння природного середовища, зрілістю соціально-політичних інститутів, структур, зв’язків та відносин.

Варто підкресли конвенційність панівних уявлень про *«цивілізацію»,* які можуть мінятися на догоду правлячим класам. У християнізованій Європі, носії дохристиянських вірувань (погани, язичники) вважалися, наприклад, нецивілізованими. Митрополит Іларіон (Іван Огієнко) навіть виводить звідси етимологію українського слова *«поганий»,* пов’язуючи це

слово з дохристиянським «селом» (латиною звучить як «pago»). Дійсно, християнським місіонерам, християнізувати мешканців сіл було набагато важче, аніж мешканців міст, й вони вочевидь й присвоїли селянам оцей сумнівний титул нецивілізованих *«поганців»* [2].

Цивілізованим французькі просвітники вважали суспільство, засноване на засадах розуму та справедливості, тобто ранньобуржуазне (суспільство раннього капіталізму). У цьому сенсі цивілізація протиставлялась двом більш раннім стадіям у розвитку культури: *варварству* й *дикості.*

Варвар (давньогр. *βάρβαροι* – іноземці, «ті, що бурмочуть») – так зневажливо називали людину, представника певного народу або племені, який дійсно або уявно перебував на доцивілізаційному або нижчому цивілізаційному рівні розвитку. Хоча слово «варвар» має грецьке походження, однак поняття «варвар» і «варварство» мають аналоги в інших світоглядних системах, де центральне місце посідають «зіткнення цивілізацій» (Самуел Гантінгтон).

Китайці, зокрема, уявляли світ «Серединною країною» (Чжунго; Піднебесною імперією, де перебуває китайська цивілізація, тоді як довкола мешкають дикі племена іноземців: іді («карлики й собаки») або сії («четвірка варварів»). Класифікувалася ця четвірка за чотирма сторонами світу: на Заході — *сіжун («західні душогуби*»); на Півночі — *бейді («північні собаки»);* на Сході — *дун'ї («східні карлики»);* на Півдні — *наньмань («південні гадюки»).*

Яскравим прикладом технофілії й навіть таких її крайніх форм як *технократія* та *техноманія* є філософсько-релігійна система марксизму, яка, хоча й ґрунтувалася не на цивілізаційному, а на формаційному підході, становлення й розвиток людини поставила в безпосередню залежність від соціально-економічних формацій, а їхню зміну пояснювала докорінними змінами у структурі продуктивних сил і виробничих відносин.

Згідно з такою логікою, принципово нові технології докорінно змінюють характер продуктивних сил, сприяючи зростанню продуктивності праці. Відтак повинні змінитися й виробничі відносини (передусім власності

на засоби виробництва), оскільки старі перетворюються на гальмо на шляху технологічного прогресу. Згодом цей «базис» мав міняти «ідеологічну надбудову», тобто різні формоутворення духовної культури.

Таке суто технократичне розуміння історії проголошувалось «історичним матеріалізмом». У вельми концентрованій формі цей технократизм передав В.І. Ленін відомою фразою *«Комунізм – це радянська влада плюс електрифікація всієї країни»* (виступ на Московській губернській конференції ВКП(б) 1920 р.). Згодом М.С. Хрущов переписав цю фразу, додавши до електрифікації ще й хімізацію (доповідь на Пленумі ЦК КПРС 09.12.1963 р.). У часи пізнього «горбачовського» СРСР згадана технократична теза формулювалася як органічне й ефективне сполучення досягнень науково-технічної революції (НТР) з перевагами соціалістичного суспільства.

За принципом «якщо вже й бити ворога, то його ж власною зброєю» американський ідеолог Уолтер Ростоу в роботі «Стадії економічного зростання: некомуністичний маніфест» (1960 р.) запропонував ще радикальнішу, порівняно з марксистсько-ленінською, технократичну візію суспільного розвитку [4]. Увесь попередній розвиток людства американський ідеолог звів до процесу індустріалізації, який, досягнувши стадії зрілості, дозволить забезпечити високе масове споживання (*High Mass Consumption*). Країнам Третього світу пропонувався рожевий ідеал **девелопменталізму, -** планомірного розвитку через засвоєння західних стандартів ринку й демократії. На честь такої перспективи їх навіть перейменували на «країни на шляху розвитку», хоча розвитку у західному розумінні цього поняття у цих країнах зазвичай не спостерігається.

«Золота ера» ліберальної концепції **девелопменталізму** співпала в часі з «золотою ерою» радянського «комунізму» (переважно хрущовський період й далі - до червневого Пленуму ЦК КПРС 1967 року).

Однак, попри всі адміністративно-командні та пропагандистські зусилля радянських вождів, радянський соціум, позбавлений важелів конкуренції й демократії, виявився несприйнятливим для технологічних

інновацій, у цілому **технофобним**, і жодною «кампанійщиною» цьому горю неможливо було зарадити.

На цьому тлі з тодішнім радянським різко контрастує **американське технофільне суспільство**. Відомо, наприклад як масове виробництво військової техніки, яку США постачали в СРСР по «ленд лізу», вирішило, по суті, долю Другої світової війни на користь країн «Великої Трійці».

Теж саме стосується інформаційної революції. Якщо на початку 60-х років XX ст. у США у банківській справі, авіакомпаніями тощо використовувалося декілька універсальних комп'ютерів (ЕОМ), то уже наприкінці 60-х років пересічна американська компанія виділяла на придбання комп'ютерів до 10 % своїх капіталовкладень. Через 30 років, наприкінці 90-х, ця цифра зросла вчетверо – до 45 %. Водночас витрати на програмне забезпечення зросли більш ніж у 100 разів: від 1 млрд. дол. у 1970 р. до 138 млрд. дол.. у 2000 р. [5**Ошибка! Источник ссылки не найден.**].

Зазвичай на початковій стадії ідеології нового соціуму, заснованого на технологіях, принципово відмінних від уже існуючих, пророблюються на рівні філософської і нефілософської, наукової і ненаукової фантастики, яка змальовує привабливі образи майбутнього.

Аналогічні ситуації виникають довкола тематики перспектив розвитку інформаційного соціуму, яка віддавна вийшла за межі фантастичних оповідей і лабораторних досліджень, перетворившись на артефакти масової свідомості. Нині інтерес до цієї «екзотики» підігрівають не тільки автори фантастичних та напівфантастичних оповідей і засновники нетрадиційних релігійних культів, але й організатори рекламних маркетингових кампаній, які розраховують на величезні зиски від впровадження новітніх технологій.

Водночас новітні технології все ще безпосередньо відносяться до футурології, де широко представлені праці з аналізу методів, критеріїв, систем прогнозування майбутнього, коли зачарування утопій примхливо мережаться з розчаруваннями дистопій.

Логіка цих процесів полягає у намаганні перетворити людину на предмет праці з метою вдосконалення самої людини, виховання або «вирощування в пробірці» нових людей.

Звідси - різноманітний, скерований на «поліпшення недосконалої людської істоти» інженіринг, - – технологічний, економічний, політичний, психологічний тощо. Одну з версій такого інженірінгу запропонував американський інженер Фредерік Тейлор (тейлоризм в СРСР отримав назву «наукової організації праці» -– НОП, або «наукового менеджменту»). Основне із запропонованих Фредерік Тейлор положень зводилось до фрагментування трудових операцій до найелементарніших, які не вимагають особливої освіченості та навичок.

З особливим ентузіазмом антропоінженерну логіку (Anthropo-Engineering) підтримав марксизм, наголосивши, щоправда, на соціальності людини (класикою в даному разі є шоста теза Карла Маркса про Фейєрбаха) та її економічній сутності та відкинувши « – про людське око» – крайнощі біологізаторства.

Тобто на ділі на цій стадії технологічного розвитку торжествувала не «природна людина», яка виявилася лише «одновимірним» додатком до різноманітних «моторів», конвеєрів та засобів людського самознищення, до хитрих механізмів інформаційного маніпулювання.

Чимало загроз дегуманізації містять в собі й новітні тенденції у розвитку Інтернету. Сам термін **«Інтернет речей»** («The Internet of Things»), запропонований Кевіном Ештоном в 1999 році, важко визнати вдалим, оскільки в ньому від самого початку закладена опозиція **«людина-річ»,** а це неодмінно провокує на роздуми щодо загроз і викликів перетворення людей на «речі» або «речей» на людей чи, принаймні щось людиноподібне.

Існують не тільки лінгвістичні чи філософські упередження щодо даного терміну, але навіть географічні. Якщо в Європі чи Китаї цей термін набув прав громадянства, то в США віддають перевагу іншим термінам.

У філософському сенсі йдеться про загрози «відчуження» (alienation) й «оречевлення» (reification) людського буття, які «масова людина» пов’язує з новітніми технологіями. Напевно, технофобія і є людською реакцією на подібні загрози й виклики дегуманізації.

Література:

1. Spengler Oswald [Електронний ресурс] // Wikipedia. -– Режим доступу : https://en.wikipedia.org/wiki/Oswald_Spengler

2. Огієнко Іван. Дохристиянські вірування українського народу. [Електронний ресурс] // Електронна бібліотека «Веселка» – Режим доступу :. https://www.e-reading.club/book.php?book=1028029

3. Варвар [Електронний ресурс] // Вікіпедія. – Режим доступу : https://uk.wikipedia.org/wiki

4. Rostow, W. W. The Stages of Economic Growth: A Non-Communist Manifesto. – Cambridge : Cambridge University Press., 1960.

5. Church, George. Perspective: Encourage the innovators // Nature. – December 03, 2015. – № 528,. – P. S7.

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

Грайворонський М. В.,
к.ф-м.н., доцент, в.о. завідувача
кафедри Інформаційної безпеки
Фізико-технічного інституту
КПІ ім. Ігоря Сікорського

БЕЗПЕКА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Сучасний світ інформаційних технологій вимагає постійної взаємодії між своїми компонентами, причому концепція комунікації між пристроями передбачає виконання певних дій взагалі без втручання людини. Для цієї концепції у 1999 році було введено назву «Інтернет речей» (англ. Internet of Things). Під терміном «річ» у даному контексті розуміють фізичні пристрої, предмети, механізми, транспортні засоби (інша назва – «розумні» пристрої) або, навіть, будівлі, що оснащені апаратним та програмним забезпеченням, що уможливлює обмін даними між цими пристроями та комп’ютерними системами.

Конкретними прикладами об’єктів Інтернету речей є побутові пристрої (будильник, кондиціонер, холодильник, кавоварка, пральна машина та інші),

домашні системи (система «розумний дім», система садового поливу, система освітлення, охоронна система, що включає в себе камери спостереження), різноманітні датчики та сенсори (теплові сенсори, давачі освітленості, руху), телекомунікаційні пристрої (зокрема, маршрутизатори і точки доступу Wi-Fi), і навіть елементи інфраструктури керування дорожнім рухом (світлофори).

Зв’язок та взаємодія пристроїв Інтернету речей відбуваються за допомогою стандартних протоколів передачі даних бездротовими та дротовими мережами на різних рівнях, а саме: HHTP/HTTPS, TCP, UDP, IP, XMPP, Ethernet, ICMP, Telnet та інші. Також з’являються нові протоколи взаємодії між «речами», що мають на меті забезпечити передачу даних в умовах низьких швидкостей бездротового зв’язку, прикладами яких є: MQTT, ZeroMQ, ZigBee, WirelessHART, CoAP. Інтеграція з мережею Інтернет передбачає призначення власної IP адреси кожному «розумному» пристрою та її подальше використання в якості ідентифікатора, що змушує використовувати протокол IPv6 замість IPv4, через обмежену кількість унікальних адрес останнього.

Інтернет речей стрімко зростає. За прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме $1,9 трлн. Деякі інші аналітичні агентства висловлюють ще більш оптимістичні прогнози та передрікають 50 мільярдів підключених пристроїв [1].

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

Слід визнати, що з розвитком Інтернету речей разом зі зручностями постають нові загрози. З технічної точки зору, Інтернет речей може використовувати різні шляхи обробки даних, комунікацій, технологій та

методологій в залежності від цільового призначення конкретних пристроїв і технологій. Цей високий рівень неоднорідності у поєднанні з широкою гамою систем Інтернету речей збільшує число загроз безпеці «розумних» пристроїв, нових векторів кібератак та нових можливостей для зловмисників.

Незважаючи на різноманітність своєї природи та обмежений функціонал, а також орієнтацію на роботу в мережі без участі людини, майже всі пристрої Інтернету речей мають інтерфейси користувача та адміністратора. Але через обмеженість інформаційно - обчислювальних ресурсів пристроїв, в таких інтерфейсах часто не передбачаються надійні механізми автентифікації. Крім цього, «розумні» пристрої, у своїй більшості, не мають механізму логування.

Згідно з результатами досліджень фахівців [2-4] можна виділити ще ряд проблем безпеки Інтернету речей:

- збереження усіх вразливостей дротових та бездротових мереж (використовуються ті ж самі протоколи);
- відсутність шифрування даних, що передаються, на багатьох пристроях, або вразливість таких систем шифрування, зокрема, через генерацію слабких ключів;
- слабка політика паролів (безліч пристроїв, що використовують стандартні паролі від розробника);
- доступність інтерфейсів керування «розумними» пристроями для зовнішнього користувача;
- відсутність антивірусного програмного забезпечення на пристроях;
- відкритість портів для віддаленого адміністрування;
- відсутність механізмів протидії перебору паролів;
- зберігання конфіденційної інформації «розумними» пристроями у відкритому вигляді (наприклад, фітнес-браслети, що зберігають інформацію про пересування користувача);
- проблеми точності та надійності «розумних» датчиків.

Можна розглядати безліч сценаріїв атак на пристрої Інтернету речей із зловмисним використанням функцій конкретних пристроїв. Наприклад, вплив на здоров'я людини, що використовує «розумні» пристрої медичного призначення, блокування людей або навпаки безперешкодне проникнення на територію через вплив на замки дверей будинків чи автомобілів, несанкціоноване отримання персональних даних, зокрема, даних про місцезнаходження конкретних осіб або стан їх здоров'я, дезорганізацію руху транспорту тощо. Об'єднані обчислювальні потужності скомпрометованих пристроїв Інтернету речей можуть використовуватись для майнінгу криптовалют або для зламу паролів шляхом побудови «райдужних таблиць».

У нашій роботі [5] ми розглядаємо досить простий випадок, який, як свідчить досвід, має дуже потужний вплив, а саме використання «розумних» пристроїв для проведення розподілених атак на відмову в обслуговуванні (DDoS атак). Одна з найголовніших небезпек таких атак криється у відсутності ефективного засобу боротьби із ними – на сьогоднішній день немає єдиного комплексу заходів щодо упередження та уникнення DDoS атак. Окрім цього, такі атаки відомі своїми руйнівними наслідками.

У вересні 2016 року було здійснено одну з найпотужніших DDoS атак в історії, основу якої склали саме пристрої Інтернету речей. Після цієї атаки, 30 вересня 2016 року, програмний код зловмисного програмного забезпечення «Mirai» (що у перекладі з японської – «майбутнє»), за допомогою якого відбулося зараження пристроїв Інтернету речей, потрапив до мережі Інтернет, де є доступним дотепер [6]. Ця подія слугувала початком цілої низки DDoS атак на різні інформаційні ресурси з використанням «розумних» пристроїв. Одним з найгучніших випадків стала кібератака 21 жовтня 2016 року на компанію Dyn, що є DNS-провайдером у Північній Америці та Європі. Оскільки DNS є основою функціонування Інтернету, внаслідок атаки чимало відомих сервісів, таких як Airbnb, Amazon.com, BBC, CNN, GitHub, Heroku, Netflix, The New York Times, PayPal, Pinterest, Reddit, Slack, Spotify, Tumblr, Twitter та інші, були недоступні певний час [7].

У нашому дослідженні ми проаналізували код Mirai на предмет того, які саме вразливості «розумних» пристроїв це програмне забезпечення використовує для проникнення. Аналіз показав, що одним з перших етапів зараження пристрою є сканування відкритих портів об’єкта атаки. Результат направляється до серверу звітів, де виконується аналіз можливості зараження. Висновок про подальшу доцільність атаки ґрунтується на наявності конкретних портів у числі відкритих. Mirai та його модифікації мають можливість скомпрометувати пристрій, якщо в нього відкриті наступні порти:

- порти, що використовуються протоколом telnet: 23, 2323, 23231
- порти, що використовуються протоколом SSH: 22
- ряд інших портів: 7547, 19058, 5555, 6789, 32, 2222, 37777.

Таким чином, відкритість вищезазначених портів можна вважати одним із факторів, що призводять до зараження «розумного» пристрою.

Інший чинник, що впливає на процес компрометації пристрою, це використання стандартного пароля від розробника. Mirai здійснює підбирання логіна та пароля для входу в інтерфейс керування пристроєм за словником.

Ще одним вектором атаки слугує використання застарілого ПЗ для ОС на основі Linux, вразливості якого дозволяють виконати вхід до командної оболонки пристрою та виконувати команди від імені адміністратора.

У продовження нашого дослідження, ми провели оцінку і порівняння вразливості «розумних» пристроїв на території України, Німеччини, Росії, США та Китаю за ознакою відкритих вразливих портів. Для отримання даних використовували пошуковий сервіс Інтернету речей Shodan [8].

У підсумку можна констатувати, що відносна кількість «розумних» пристроїв на території України є помітно меншою, ніж в інших досліджених країнах, але відносний рівень їх вразливості вищий. Дані оцінок свідчать про те, що закриття портів 23 та 2323 суттєво знижує рівень вразливості пристроїв Інтернету речей. Оскільки обидва порти використовуються

застарілим протоколом telnet, можна зробити висновок про доцільність припинення використання даної технології.

Література:

1. Panda Security. You don’t realize how many devices in your workplace are connected to the Internet [Електронний ресурс]. – 2016. – Режим доступу: http://www.pandasecurity.com/mediacenter/mobile-security/shadow-iot-workplace-internet/;

2. Леонов А.В. Интернет вещей: проблемы безопасности / А.В. Леонов // Омский научный вестник. – Выпуск №2 (140) – 2015;

3. Лаборатория Касперского. Безопасность интернета вещей: прогресс, хайп и головная боль [Електронний ресурс]. – 2016 – Режим доступу: https://habrahabr.ru/company/kaspersky/blog/311076/;

4. Лаборатория Касперского. Интернет вещей и безопасность инфраструктуры [Електронний ресурс]. – 2015 – Режим доступу: https://blog.kaspersky.ru/internet-of-things-and-cybersecurity-of-infrastructure/7394/;

5. Кіфорчук К. О. Оцінка вразливості пристроїв “Інтернету речей” в Україні / К. О. Кіфорчук, М. В. Грайворонський // Безпека інформації в інформаційно-телекомунікаційних системах. Матеріали міжнародної науково-практичної конференції. – 2017. – Вип. 19. – стор. 45-46;

6. Leaked Mirai Source Code for Research/IoC Development Purposes [Електронний ресурс]. Режим доступу: https://github.com/jgamblin/Mirai-Source-Code;

7. Etherington E., Conger K. Many sites including Twitter, Shopify and Spotify suffering outage [Електронний ресурс]. Режим доступу: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

8. Пошуковий сервіс Shodan [Електронний ресурс]. Режим доступу: https://www.shodan.io/

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

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

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТ РЕЧЕЙ (IP): ПРОБЛЕМИ І НАСЛІДКИ

Більшість передових країн світу приділяють велику увагу технологіям Інтернет речей (IP), оскільки усвідомлюють, що у широкому їх застосуванні

закладено величезний потенціал значного підвищення ефективності практично будь-якого виду людської діяльності, зокрема у сферах реальної економіки, промисловості та сільського господарства, в системах охорони здоров'я, державного управління, освіти, фінансового обороту тощо.

В Китаї розвиток Інтернет речей рахується стратегічно важливим і передбачено в державній програмі. Китай збирається до 2020 року вкласти в Інтернет речей $128 млрд.

Не виключенням стали і Об'єднані Арабські Емірати, які стали першою країною в світі, де з'явилося міністерство у справах штучного інтелекту *(19 жовтня 2017р.)*. Передбачається, що новостворене міністерство займеться розвитком знань, підтримкою науки і досліджень в сфері штучного інтелекту. ОАЕ є одним з світових лідерів за обсягом інвестицій в штучний інтелект.

В одній із доповідей на тему «Цифрове життя в 2025 році» вчені зазначили, що Інтернет скоро стане подібним до електрики: менш помітним, але більше зануреним в повсякденне людське життя. З чим це пов'язано. Насамперед, передача інформації стане настільки простою і звичною, що перестане бути помітною. Інтернет буде такою ж невід'ємною частиною нашого повсякденного життя, як і електрика; поширення Інтернету підвищить кількість пов'язаних між собою людей (попри те, що вони розкидані по різних континентах) і зменшить непоінформованість про життя в тих або інших країнах; Інтернет речей, штучний інтелект і великий об'єм даних (Великі дані) зроблять людей обізнанішими в питаннях про навколишній світ і про свою власну поведінку; доповнена реальність і носимі пристрої допоможуть відстежувати повсякденне життя, стан здоров'я і помі-няють погляд на багато звичних занять: співбесіди на роботу, ігри і рейтинг.

Погоджуючись з тим, що технології IP є найпотужнішим стимулюючим фактором для інноваційного розвитку нанотехнологій, мікроелектроніки, напівпровідникових технологій, мікромініатюризації виконавчих пристроїв, телекомунікацій, радіотехнологій, програмних обчислювальних засобів і багато іншого, водночас зазначимо, що постане

питання інтенсивних наукових досліджень по оптимізації тих чи інших видів діяльності в зв'язку з новими функціональними можливостями через впровадження технологій IP. До чого це може призвести?

Насамперед, стрімке поширення Інтернету речей призведе до зростання ризиків і проблем, пов'язаних з безпекою.

1. Інтернет речей надає більше векторів атак, ніж будь-коли. Нові функції і «фічі» для розумних пристроїв відкривають і нові поля для атак. Такі технології -не тільки зручність, але і відповідальність: з боку виробників - за безпеку пристроїв, а користувачів - за збереження своїх даних.

Наприклад, як нам всім відомо, що розумний холодильник став частиною бот-мережі і почав розсилати спам; розумна кавоварка виявилася причиною атаки на індустріальні мережі з подальшим зараженням комп'ютерів для моніторингу технологічного процесу вірусом-здирником.

Тому, на нашу думку, безпека повинна бути передбачена на рівні проектування дизайну нових пристроїв, рішень і технологій це надасть можливість позбутися від цілого ряду класичних проблем і вразливостей.

2. Чи можливе стеження, віртуальне переслідування, або збір інформації?

Трапляються випадки коли розробники навмисно або ненавмисно залишають недокументований канал, який не просто збирає інформацію про застосування пристрою, але і дозволяє проникати в особистий простір кінцевого користувача. З іншого боку, є інтерес зловмисників. Якщо проблеми безпеки не вирішені на етапі дизайну і проектування рішення - такі помилки дозволяють отримати несанкціонований доступ до пристроїв в гігантських масштабах. Безпека повинна бути в основі всього, що тільки з'являється, планується або модернізується. Безпека повинна бути частиною життєвого циклу розробки будь-якого продукту. Серйозні рішення і технології вже мають впроваджені цикли безпечної розробки. Але більшість нових сучасних рішень і технологій з'являються як стартапи, де основна ідея полягає далеко не в безпеці.

Не можна допускати помилок, які призводять до виникнення критичних вразливостей в пристроях, які збирають інформацію про активність в Інтернеті.

Оскільки правопорушення і правопорушники теж розвиватимуться у своїх масштабах, адже людська природа не міняється *(Кібертероризм стане звичайною справою, говорить Левелин Криэл, генеральний директор і головред TopEditor. З'являться онлайн-хвороби, цифрові злочинні мережі і цілі ОЗУ).*

Також повністю погоджуємося з Фрэдом Бейкером з Cisco Systems, який підмітив: «Проблеми безпеки і конфіденційності будуть вирішені, але загрози повністю не викоренені, тому що завжди є відсоток людей з бажанням завдати комусь шкоди».

Наступна із проблем, яка може виникнути із впровадженням технологій IP, а скоріше посилитися – це проблема шкідливості. З чим це пов'язано, насамперед з використанням сигналу 4G, 5G… За даними вчених оцінити безпеку сигналу 4G при існуючих методиках виміру практично неможливо: «Практичних досліджень досі немає, а оцінка їх шкідливості робиться, по суті, пальцем в небо…». Базові станції стільникового зв'язку за останні два роки принципово змінили електромагнітну обстановку в мегаполісах таким чином, що учені починають розглядати цю ситуацію як перспективну проблему для довкілля: «Якщо років 20 назад тільки 1% міського населення жило в умовах зміненого електромагнітного фону, то зараз ми говоримо вже про 90%. Він піднявся за рахунок збільшеної кількості базових станцій стільникового зв'язку». Учені вважають, що зміна фону для людей буде не безслідним, «але наскільки усе це небезпечно для здоров'я, потрібно ще вивчати, тому що довготривалих досліджень із цього приводу в науці поки немає».

Згідно з дослідженнями фахівців з проблеми електромагнітних випромінювань, в результаті дії електромагнітних полів на людину виникають вегето-судинні дистонії, гіпертонічні хвороби, атеросклеротичні

кардіосклерози, а з боку нервової системи можуть виникати астенічні, вегетативні дисфункції, церебральний склероз. Проте треба розуміти, що ці захворювання виникають у тих, хто постійно працює з полями.

Водночас, широкомасштабне використання технологій Інтернет речей призведе до виникнення та подальшої ідентифікації багатьох нових проблем, пов'язаних із захистом 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*). Буде складніше зберегти свою конфіденційність і приватне життя, тому що користувачі йтимуть на компроміси, іноді з небажанням, щоб отримати доступ до якої-небудь важливої інформації.

І насамкінець, найбільш вагому групу ризиків складуть правові проблеми, що будуть зумовлені виникненням принципово нової множини суспільних відносин, які базуються на використанні технологій ІР. Це буде пов'язано насамперед з виникненням та реалізацією правовідносин, що будуть виникати в процесі використання технологій ІР з елементами штучного інтелекту; правовими механізмами регулювання інфраструктурної безпеки впровадження та використання технологій ІР; забезпеченням кібербезпеки у разі транскордонного використання таких технологій; використанням радіочастотного ресурсу в умовах масового використання радіоприладів та ін.., забезпеченням конфіденційності, а також захисту персональних даних тощо.

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

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

ІНТЕРНЕТ РЕЧЕЙ І ПРАВО

До оцінки поняття «Інтернет речей» з точки зору еволюційного розвитку суспільства. На нашу думку, реальне впровадження «Інтернет речей» слід розглядати як:

- черговий етап побудові та розвитку інформаційного суспільства, одного з невід`ємних його складових;
- перехід від суцільної інформатизації до суцільної механізації, автоматизації та роботизації, природно, в рамках розумного;
- механізм, інструментарій переходу «інформаційного суспільства» до «суспільства знань»;
- реальне формування фундаментальних основ киберцивілізації.

***Взаємозв`язок інтернет речей з правом.*** «Інтернет речей» без сумніву здійснить дуже суттєвий вплив на трансформацію та, саме головне, створення нових суспільних відносин. Як відомо, право - система соціальних загальнообв`язкових норм, дотримання і виконання яких забезпечується державою. Саме держава відіграє особливу конститутивну роль щодо права, бо тільки вона здатна забезпечити загальнообов`язковість соціальних норм у масштабах усього суспільства. Право – один з головних засобів організованості й порядку в суспільстві, істотного впливу на характер суспільного розвитку. Саме тому, можна стверджувати про опосередкований зв`язок «інтернет речей» з правом.

У тій же час, як і все нове, «Інтернет речей» несе не лише нові бажані можливості, але й нові «клопоти» у вигляді нових, до цього часу невідомих або слабо відомих, ризиків та загроз для особистості, суспільства та держави в цілому.

У зв`язку з цим виникає досить логічне питання: наскільки людина, суспільство та держава підготовлені до суттєвої, практично докорінної, трансформації існуючих суспільних відносин та сприйняття нових.

На даний час, можна констатувати, що система правового регулювання суспільних відносин, яка склалася та функціонує в Україні, **є констатуючою** за фактом.

В часи стрімкого науково-технічного прогресу, наслідки якого «ламають», змінюють до докорінного існуючи суспільні відносини з одночасним породженням нових, наявність **констатуючої** системи їх правового регулювання є «недозволеною розкішшю» з наступними наслідками, які обов`язково рано чи пізно проявляться:

- система державного управління може поступово втрачати, аж до фактично повної втрати, контроль над суспільством та не зможе необхідною мірою забезпечувати його життєдіяльність;
- виникне суспільна напруга наслідки якої можуть бути непередбачуваними;
- держава однозначно «програє» у очах світової спільноти;

Як цього уникнути? **1.** Необхідно чітко усвідомлення на всіх рівнях, що сучасний науково-технічний прогрес є невід`ємною складовою еволюційного розвитку світу. Тобто, науково-технічний прогрес – **об`єктивний** процес, якій не можливо зупинити. Будь-який об`єктивний процес можна лише прискорити або пригальмувати, але зупинити неможливо.

Також об`єктивних є факт, а на даний час це – вже факт, що головним двигуном прогресу суспільства, його розвитку та благополуччя, а також інших благ є високі наукоємні технології.

Не усвідомлення цього гарантує Україні як державі та громадянам України не у настільки віддаленому часі залишитися поза «конкурсом» щодо попадання до «золотого мільярда».

2. Нарешті необхідно визначитися та довести до свідомості кожної людини: а) яку країни ми вже 26 років будуємо (аграрну, сировинну, промислову або високоінтелектуальну); б) зміст національної ідеї.

Лише за таких умов можна визначати пріоритети, розробляти концепції, стратегії та плани., а саме головне, консолідувати суспільство. Цього вимагає й об`єктивність науково-технічного прогресу бо все одне результати цього прогресу будуть «проникати» і до української держави, і до українського суспільства, і до кожного громадянина України, окрім їх волі або бажання. Питання лише глибині та спрямованості «проникаючих» результатів, а також ролі та місця України у процесах науково-технічного прогресу.

3. Коли це буде усвідомлене, то необхідно, не просто спостерігати за трансформацією або появою нових суспільних відносин, а приймати активну участь у їх формування з наступним правовим регулюванням. Проще кажучи, необхідно систему правового регулювання перетворити з **констатуючої** у **формуючу**.

На підтвердження цього можна навести такий приклад[1]: *«Міністерство транспорту США випустило нові правила для автоматизованих систем водіння - «Vision for Safety 2.0», які відображають важливість боротьби із зростанням смертності від дорожньо-транспортних подій в США внаслідок того, що 94% серйозних аварій на автотранспортних засобах в США відбуваються з вини людини.*

Нові правила призначені для уніфікації функцій автоматизації і включають як повністю автономне управління, так і просто розширені системи допомоги водієві. Це друга версія федеральної політики для безпілотних автомобілів, а в 2018 році планується випустити третю.

У правилах також роз'яснюється, що компаніям не треба чекати, щоб почати тестування і розгортання своїх автоматизованих систем водіння.

[1] Джерело інформації: http://news.eizvestia.com/news-auto/full/1309-v-ssha-poyavilis-novye-pravila-dlya-bespilotny

Очікується також, що правила спростять процес ліцензування для компаній-розробників.»

Наведеній приклад наочно показує відмінності між констатуючої та формуючими моделями правового регулювання суспільних відносин, переваги формуючої моделі правового регулювання суспільних відносин перед констатуючої, що особливо важливо у період стрімкого науково-технічного прогресу.

У контексті висловленого, головне не те, де та кім отримане результат (продукт) науково-технічного прогресу, головне – які наслідки він буде мати, особливо, якій вплив буде здійснено на конкретні суспільні відносини. Головне – у тому, що правовому регулюванню, в першу чергу, підлягають суспільні відносини у межах юрисдикції конкретної регуляторного органу – у нашому випадку, юрисдикції України.

Юрисдикція України не визначає ані напрямів, ані темпів науково-технічного прогресу, але вона визначає правовідносини на своїй території та несе відповідальність за повноту та своєчасність їх встановлення.

4. Перетворення констатуючої системи встановлення правовідносин в Україні на формуючу систему встановлення правовідносин – процес дуже складний та, у силу деяких суб`єктивних обставин, уявляється досить довготривалим, але іншого шляху немає. Коли не внутрішні чинники, так зовнішні все одне вимусять це робити.

Які чинники впливають на небажання або стримування перетворення констатуючої системи встановлення правовідносин на формуючу систему в Україні? На наш погляд, серед багатьох об`єктивних та, що найбільше впливових, суб`єктивних чинників, необхідно звернути особливу увагу на:

- відсутність чіткого та зрозумілого формулювання національної ідеї, а й відповідно розуміння спрямованості розбудови країни що, у свою чергу, не дає можливості відбудовування системи пріоритетів цій розбудови. На даний час, пересічний громадянин України бачить та відчуває лише один пріоритет

державної політики – безперервний ріст цін та тарифів на все без зрозумілого обґрунтування та стрімкого збільшення «доларових» і «гривневих» мільйонерів, які не мають офіційного відношення до бізнесу;

- повна зневага до науки, особливо, до правової науки, що в період стрімкого науково-технічного прогресу можна розцінювати, як відповідь на питання, які були наведені вище, по моделі держави, що будується, та пріоритетах цього будівництва. Ступень справедливості даного висловлення можна встановити з огляду, навіть не аналізу, законів України «Про Державний бюджет України на … рік», скажемо на 2015, 2016, 2017 роки та проекту Закону України «Про Державний бюджет України на 2018 рік». Цифри, які там були закладені та зараз закладаються, на фінансування правової науки, самі за себе говорять. Необхідно ще раз підкреслити, що встановлення коректних та своєчасних правовідносин є, в першу чергу, суто внутрішньою державною прерогативою, яку без відповідно розвинутої національної правової науки здійснити неможливо. Можна піти й іншим шляхом – шляхом імплементації правовідносин як за міжнародними нормативно-правовими актами, так й окремих країн. Саме шляхом імплементації, а не адаптації, бо для успішної адаптації знов-такі потрібна правова наука;

- консерватизм у підходах до законотворчої роботи, як науковців - теоретиків, так і юристів - практиків, якій виражається у збереженні радянських принципів та постулатів до визначення правовідносин «за фактом», не зважаючи на зміни які відбуваються у суспільстві;

- визначена «обособленість» різних галузей науки – технічних, філософських, соціологічних, медицинських, психологічних, політичних, правнічних та ін., які впливають на формування, трансформацію та регулювання суспільних відносин;

- дуже суттєвий кадровій «дефіцит» у сферах правотворення, правозастосування та правоохоронної на спеціалістів, які відповідають вимогам спрямованості та темпам сучасного науково-технічного прогресу.

Огірко І. В.,
д. фіз.-мат. н.,професор
Українська академія друкарства,Львів.

ТЕХНОЛОГІЇ МЕРЕЖ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (IP) — це мережа, що складається із взаємозв'язаних фізичних об'єктів (речей) або пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Крім давачів, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові і бездротові мережі. Ці взаємопов'язані об'єкти мають можливість зчитування та приводити в дію функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.

Сьогодні Інтернет речей став популярним терміном для опису сценаріїв, у яких Інтернет з'єднання і обчислювальна здатність поширюються на безліч об'єктів, пристроїв, давачів і повсякденних об'єктів. Основною концепцією IP є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть кросівки. Всі ці об'єкти (речі) повинні бути оснащені вбудованими давачами або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації.

Прикладом впровадження такої концепції є система «розумний будинок» або «розумна ферма». Ця система аналізує дані навколишнього середовища і в залежності від показників регулює температуру в приміщенні. У зимовий період регулюються інтенсивність опалення, а в разі спекотної погоди будинок має механізми відкривання і закривання вікон, завдяки чому провітрюється будинок, і все це відбувається без втручання людини.

Для об'єднання повсякденних речей у мережу потрібні декілька технологій. Для ідентифікації кожного об'єкту потрібна проста, компактна технологія. Тільки при наявності системи унікальної ідентифікації можна збирати та накопичувати інформацію про певний предмет. Такий функціонал можна забезпечити за допомогою мікросхем *RFID*. Вони здатні без власного джерела струму передавати інформацію приладам зчитування. Кожна мікросхема має індивідуальний номер. Як альтернатива до даної технології для ідентифікації об'єктів можуть використовуватись QR-коди. Для визначення точного місця знаходження речі підійде технологія *GPS*, яка ефективно використовується вже сьогодні у смартфонах та навігаторах. Для відслідковування змін у стані елементу чи оточуючого середовища об'єкти повинні оснащуватися сенсорами. Для обробки та накопичення даних з сенсорів повинен використовуватися вбудований комп'ютер. Для обміну інформацією між пристроями можуть бути використані технології бездротових мереж (*Wi-Fi, Bluetooth, ZigBee, 6LoWPAN*). Засоби передачі даних в мережі - інтеграція з Інтернетом має на увазі, що пристрої будуть використовувати IP-адресу як унікальний ідентифікатор.

Проте, через обмежені адресні простори в *IPv4*, об'єктам IP доведеться використовувати *IPv6*, який забезпечує унікальними адресами мережевого рівня не менше 300 млн пристроїв на одного жителя Землі. Об'єктами в IP будуть не тільки пристрої із сенсорними можливостями, але також пристрої, які виконують дії (наприклад, лампочки або замки, якими керують через Інтернет). Значною мірою, майбутнє Інтернету речей не буде можливим без підтримки *IPv6*, отже, глобальне впровадження *IPv6* у найближчі роки буде мати вирішальне значення для успішного розвитку IP в майбутньому.

Для бездротової передачі даних особливо важливу роль в побудові Інтернету речей відіграють такі характеристики, як ефективність, відмовостійкість, адаптивність, можливість самоорганізації.

Основне зацікавлення в цьому сенсі представляє стандарт *IEEE 802.15.4*, що управляє доступом для організації енергоефективних

персональних мереж, і є основою для таких протоколів, як *ZigBee, WiFi, Bluetoot, 6LoWPAN.ZigBee* — це комунікаційна технологія, заснована на протоколі *IEEE 802.15.4* для реалізації низькошвидкісних бездротових приватних мереж. *ZigBee* володіє такими характеристиками, як низьке енергоспоживання, низька швидкість передачі даних, низька вартість і висока пропускна здатність. В даний час *ZigBee* використовується, в основному, при передачі інформації між різними речами електронного обладнання, які знаходяться в межах короткої відстані і швидкості передачі даних не дуже висока. Це, в основному периферійні пристрої і побутова електроніка (*TV, DVD*), а також пристрої промислового управління. *WiFi* — це локальна бездротова технологія, яка використовує 2,4 ГГц надвисокої частоти або 5 ГГц супер-високочастотної радіохвилі. Ця технологія дуже добре підходить для передавання великих обсягів даних по бездротовій мережі між пристроями, але це також вимагає багато енергії для роботи і має невеликий рівень пропускної здатності даних. При використанні цієї технології потрібно буде замінювати батареї у всіх пристроях на регулярній основі. *Bluetooth* — це бездротова технологія, яка використовується для передачі даних в персональних мережах. Він передає дані по смузі частот від 2,4 до 2,485 ГГц і працює на коротших відстанях, ніж *Wi-Fi*. Ви можете синхронізувати пару пристроїв, таких як телефони, навушники, колонки, комп'ютери і багато іншого. З розвитком *Bluetooth v 4.0* з'явилася можливість реалізувати функцію низького енергоспоживання і збільшений радіус дії до декількох десятків метрів. Серед провідних технологій важливу роль у розповсюдженні інтернету речей відіграють рішення *PLC* — технології побудови мереж передачі даних по лініях електропередач, оскільки у багатьох додатках присутній доступ до електромереж (наприклад, торгові автомати, банкомати, інтелектуальні лічильники, контролери освітлення спочатку підключені до мережі електропостачання). *6LoWPAN*, який реалізує шар *IPv6* як над *IEEE 802.15.4*, так і над *PLC*, будучи відкритим протоколом, стандартизованих *IETF*, відзначається як особливо важливий для розвитку інтернету речей.

Так на виставці CES 2014 у Лас-Вегасі була представлена велика кількість побутової техніки (холодильники, телевізори, пральні машини) з можливістю підключення до Інтернет. Лідерами у розробці та впровадженні Інтернету речей є країни, в який розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів — це США, Китай, Південна Корея. Також значний прогрес у цій галузі демонструють європейські країни та Японія. Інтернет речей може викликати величезні зміни у повсякденному житті, надавши звичайним користувачам абсолютно новий рівень комфорту. Але якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, за допомогою надійного криптографічного алгоритму, замість користі вони принесуть шкоду, надавши кіберзлочинцям лазівку для підриву інформаційної безпеки. Оскільки речі із вбудованими комп'ютерами зберігають дуже багато інформації про свого власника (зокрема, можуть знати його точне місцезнаходження) доступ до такої інформації може допомогти зловмисникам вчинити злочин[7]. Відсутність на даний час стандартів для захисту таких автономних мереж дещо сповільнює впровадження Інтернету речей у повсякденне життя.

У вересні 2016 року після публікації статті про угрупування, які продають послуги ботнетів для здійснення DDoS-атак, веб сайт журналіста Брайана Кребса (англ. *Brian Krebs*) сам став жертвою DDoS-атаки, трафік якої на піку досягав 665 Гб/с, що робить її однією з найпотужніших відомих DDoS-атак. Оскільки хостер сайту відмовився надалі безоплатно надавати свої послуги, сайт довелось на деякий час закрити поки не був знайдений новий хостер. Атака була здійснена ботнетом з інфікованих «розумних» відео-камер. Ботнет Mirai став можливим завдяки реалізації вразливості, яка полягала у використанні однакового, незмінного, встановленого виробником пароля для доступу до облікового запису адміністратора на «розумних» пристроях. Всього мав відомості про 61 різних комбінацій логін-пароль для отримання доступу до облікового запису методом перебирання. Дослідження показали, що значна частина вразливих пристроїв була виготовлена з

використанням складових виробництва фірми XiongMai Technologies з офісом в Ханчжоу, та фірми Dahua, Китай. Інтернет Речей, – сфера, яка дозволяє реалізовувати такі концепти як «розумний будинок» чи «розумне місто» і поєднує програмування та пристрої.

Modum.io - проект, котрий поєднує сенсорні датчики і технологію блокчейн. Передбачається, що такий продукт повинен бути затребуваний при зберіганні і перевезенні товарів, що вимагають спеціальних умов зберігання. Датчики реєструють умови оточуючого середовища при транспортуванні або зберіганні товарів, а при зміні власника зібрані дані перевіряються через смарт-контракт Ethereum. Контракт підтверджує, що дані з датчиків відповідає всім стандартам, встановленим клієнтом або регулятором, а так само дозволяє перейти до функцій, такі як повідомлення відправника і одержувача, оплата та ін. Все управління процесом буде відбуватися через додаток в мобільному телефоні, а самі датчики і сенсори не вимагають спеціальної упаковки, захищені від несанкціонованого доступу, водонепроникні. У whitepaper досить докладно докладно описаний процес використання датчиків, реєстрації їх у системі, зняття показань. Так само наведені приклади використання датчиків вологості для перевезення сировини, датчиків руху для перевезення тендітних товарів і датчиків світла для доказу того, що посилка не розкривалася. В цілому, якщо говорити про сам продукт, то мені він здається затребуваним, а для деяких організацій просто обов'язковим. Використання такої технології може дати серйозну конкурентну перевагу компаніям, які займаються логістикою. Я хочу знати, що ліки і продукти, які я купую, правильно зберігалися. Техніка, яку я замовляю в інтернет - магазині не падала під час доставки, а конверт з документами не відкривався. Запуск першої лінійки продукції націлений на перший квартал 2018 року. Так само як впровадження підтримки одного з наступних блокчейнов: IOTA, NEO, Fabric, ETC або Rootstock. Інтернет речей (Internet of Things – IoT) перетворює звичні для нас речі у нові пристрої, створюючи як розумні годинники, так і розумні міста. Він

під’єднує далекі від Інтернету засоби до мережі та надає їм нові функції. Таким чином, всі пристрої в будинках, в автомобілях, на користувачеві виконують обробку інформації, її аналіз та обмін між собою та, залежно від результатів, приймають рішення і виконують певні дії. Сфера IoT – один із головних світових трендів. Експерт IoT – людина, яка творить майбутнє. Старі пристрої стають частиною Інтернет мережі і виконують нові функції. Недарма цю галузь вважають рушієм 4-ї індустріальної революції, яка зараз триває у світі. «Modum.io» поєднує в собі сенсори IoT з технологією блокчейнів для забезпечення цілісності даних для транзакцій фізичних продуктів, оптимізації процесів постачання в багатьох секторах. Модумні датчики визначають умови навколишнього середовища під час транспортування. Коли товари змінюють власність, зібрані дані перевіряються відповідно до конкретного розумного контракту в блок-схемі Ethereum. Контракт підтверджує, що транзакція відповідає всім стандартам, встановленим замовником, їх клієнтами або регулятором, і запускає різні дії: сповіщення відправнику та одержувачу, оплату або випуск товарів. Малопотужні, з широким охопленням мережі починають «робити круги» в світі IoT. Мережі (LPWA - Low-Power, Wide-Area) з широким охопленням та низьким енергоспоживанням є новим улюбленцем бездротової спільноти.

Розглянемо деякі з технологій і компаній, які активні в цьому просторі. Головною рушійною силою технології LPWA є бажання підключити сенсори IoT до Інтернету без оплати за стільниковий зв'язок (але майте на увазі цю думку), без додаткового живлення або розгортання складних Wi-Fi мереж та без обмеження дальності, як в Bluetooth. Незважаючи на те, що деякі люди думають, що технології LPWA не є істинно «малої потужності» в тому сенсі, що передача в них більш ефективна, ніж в інших. Дійсно, передавачі LPWA використовують в 10 разів і навіть більшу потужність для передачі, ніж Bluetooth. Назва «низька потужність» насправді походить від архітектури системи, яка дозволяє пристроям спати понад 99% часу. У режимі очікування (режим сну) струм становить всього кілька мікроампер, тому можлива

автономна робота протягом багатьох років. Частину «широке охоплення» в назві можна більш точно охарактеризувати як «вищий бюджет зв'язку». Проте, «малий струм режиму сну, вищий бюджет зв'язку» не зв'язані одне з одним. Широке покриття зв'язком для пристроїв LPWA, як правило, є результатом поліпшення чутливості приймачів на обох кінцях каналу зв'язку. Це продукт дуже низьких швидкостей передачі даних і творчого поліпшення обробки. Остаточним впровадженням інновацій в технології LPWA є множинний доступ.

SIGFOX

Sigfox вже в похилому віці, йому близько 7 років, і він є прадідом простору LPWA. Технологія була піонером в створенні ринку. Сьогодні є мережі провайдера і постачальники технологій для операторів на інших ринках. Раніше вже багато розглядалась технологія Sigfox, але як огляд:

- Sigfox використовує велику базову станцію з формуванням каналів за допомогою FPGA для виявлення передач ДФМ з низьким бітрейтом через сотні потенційних каналів.
- Кінцеві вузли наосліп передають те ж саме повідомлення 3 рази, на 3-х різних частотах, щоб підвищити ймовірність того, що повідомлення буде отримане.
- Низхідний сигнал теоретично можливий, але це дуже обмежено, тому що всякий раз, коли передає базова станція, то через атмосферу і, таким чином, збільшується ризик того, що буде пропущений трафік.

Ця проста технологія дозволяє використовувати безліч різних радіо трансиверів, тому клієнти мають кілька джерел постачання.Випадки використання повинні бути в числі найпростіших для IoT, оскільки доступні лише 12 байт корисного навантаження при передачі.Такі речі, як оновлення вбудованого програмного забезпечення або додатків управ- ління не є можливим з Sigfox.

Оскільки час FCC в прямому ефірі обмежений (400 мс), Sigfox має близько на 9 дБ гірший бюджету зв'язку в США, а це в поєднанні з більш

високим рівнем перешкод в смузі частот 900 МГц означає, що продуктивність мережі в США не така хороша для Sigfox, як в Європі.

WAVIOT

- WAVIOT є компанією, яка використовує технологію, яка практично ідентична Sigfox.
- Одна відмінність полягає в тому, що пропонуються не мережі, а тільки технологія.
- На відміну від Sigfox, будь-який бажаючий може купити обладнання WAVIOT для створення власного рішення.
- WAVIOT має стрибаючий сигнал, що дозволяє їх бюджету зв'язку перевищити для додатків на основі Sigfox для FCC/США.
- Обладнання базової станції WAVIOT є дорогим через велику FPGA, необхідну для реалізації всіх ДФМ (DPSK) каналів.

LoRaWAN

- Як і Link Labs, LoRaWAN заснована на технології LoRa фізичного рівня, однак протокол Symphony Link від Link Labs дуже відрізняється і пропонує безліч додаткових функцій, які LoRaWAN не робить.
- LoRa пропонує набагато кращу чутливість приймача на кінцевих пристроях, ніж Sigfox, і, таким чином, бюджет зв’язку є більш збалансованим.
- Як і Sigfox, LoRaWAN асинхронна, доступ в стилі Aloha, тому застосовуються одні й ті ж обмеження для низхідної лінії як для LoRaWAN, так і для Sigfox.
- Бізнес-модель LoRaWAN ускладнюється тим, що LoRa продається Semtech, але протокол розроблений Lora Alliance, і відомо також кілька пілотних мереж мережевих операторів на основі LoRa.
- Операторські мережі і приватні розгортання LoRaWAN заважають один одному.

LTE-M1

- Ця категорія LTE дозволяє отримати для пристроїв енергоефективність, як LoRaWAN або Sigfox, але може мати вишуканість і швидкість даних LTE.
- Очевидно, що якщо ви використовуєте LTE - M, то повинні платити оператору мережі.
- Сертифікація пристроїв на операторських мережах може бути дорогою.
- Мережі LTE-M1 не будуть розгорнуті в США до 2017 року.
- Ціни на LTE-M будуть конкурентоспроможними з пропонованими Sigfox.
- NB-IOT (або LTE-M2) є ще однією технологією 3GPP, яка була недавно завершена.
- Оскільки вона не є технічною частиною протоколу LTE, то може бути розгорнута в маскованих LTE блоках ресурсів або в захисних полосах.
- Була розроблена, щоб поміститься в старих блоках GSM спектру 200 кГц, і багато операторів в Європі і Азії, швидше за все, розгорнуть дану технологію для пристроїв IoT.
- У якомусь сенсі Sigfox створив NB-IOT показуючи операторам, що є хороший бізнес, який можна використати для пристроїв IoT.
- NB-IOT відстає близько року від LTE-M1, тому не буде готової мережі, ймовірно, до кінця 2017року, або вже в 2018 році.
- Застосовуються ті ж міркування про оплату мережевого оператора і сертифікацію пристроїв.
- Ingenu є ребрендингом Onramp Wireless. У них є свої власні технології DSSS 2,4 ГГц і розгорнуті на основі неї мережі.
- Має великий бюджети зв'язку, але DSSS-модем на кінцевій точці досить ненажерливий в порівнянні з LoRa.
- Мережі будуть розміщені тільки в декількох містах.
- Буде цікаво подивитися, чи зможуть вони вижити в умовах LTE-M від ATT і Verizon.

На закінчення, є багато варіантів для різних LPWA. Це доступна сама передова технологія LPWA.

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

Шахбазян К. С.,
к.ю.н., с.н.с Центру досліджень інтелектуальної власності та передачі технологій НАН України.

ІНТЕРНЕТ РЕЧЕЙ: РИЗИКИ ПОРУШЕНЬ У СФЕРІ ПРАВ ЛЮДИНИ

Визначення терміну "Інтернет речей" було надано в п. 3.2.2 Рекомендації Міжнародного союзу електрозв'язку Y.2060 (06/2012). Згідно з ним Інтернет речей (далі - "IP") - це "глобальна інфраструктура для інформаційного суспільства, яка забезпечує можливість надання більш складних послуг шляхом з'єднання одне з одним (фізичних і віртуальних) речей на основі існуючих і таких, що розвиваються, функціонально сумісних інформаційно-комунікаційних технологій". Автори Рекомендації Міжнаро- дного союзу електрозв'язку відзначають, що "в широкому сенсі Інтернет речей можна сприймати як концепцію, що має технологічні та соціальні наслідки". Більш того, з урахуванням масштабу очікуваних технологічних і соціальних наслідків[2], особливої актуальності набувають правові аспекти регулювання IP, зокрема ті, що пов’язані з дотриманням прав людини.

IP ще більше трансформує поняття конфіденційності (privacy) в Мережі. Дебати навколо права на приватне життя, закріпленого в ряді інструментів міжнародного права (Стаття 12 Загальної декларації прав людини ООН, Стаття 8 Європейської конвенції з прав людини, Стаття 17 Міжнародного пакту про громадянські і політичні права), вийшли на якісно новий рівень. Персональні та комунікаційні дані сьогодні все більше доповнюються геолокаційними, біометричними та іншими показниками людської активності – це дозволяє скласти більш повний портрет окремо взятої людини з усіма подробицями її життєдіяльності. А це відкриває нові горизонти для всіх зацікавлених осіб, які бажають отримати максимально

[2]Відповідно до звіту аналітичної компанії JuniperResearch, в 2020 році кількість пристроїв, підключених до IP, складе 38,5 мільярда одиниць

докладну інформацію про конкретну людину (або групу людей) для легітимних або нелегітимних цілей.

Таким чином, розвиток IP істотно ускладнює проблему захисту приватності, причому ставлення до неї, як і підходи до її вирішення, варіюватимуться в залежності від прийнятого в даному середовищі (країні, регіоні) ставлення до масового збору даних.

Відповідно, доцільно розробити принципи регулювання сфери IP в галузі прав людини, з їх подальшим втіленням в законодавство на національному рівні та на рівні міжнародного права. **Можливо запропонувати наступні принципи такого регулювання:**

1. Інформованість. Користувачі сервісів IP повинні мати інформацію щодо того, збір яких даних здійснюється тим чи іншим пристроєм, якими способами, в якому обсязі, де і яким чином такі дані зберігаються.Можливо, необхідно розглянути питання про створення відкритого реєстру пристроїв і рішень IP. Реєстр може містити інформацію про можливості пристроїв зі збору інформації та автоматизованої взаємодії з іншими пристроями. В якості альтернативи, на думку окремих представників індустрії, можна розглядати формування системи принципів, які виробники не повинні порушувати, і які будуть засновані на балансі інтересів сторін.

2. Вільна участь в IP. Незважаючи на те що IP - об'єктивна тенденція розвитку інформаційного суспільства, громадяни та організації не можуть бути дискриміновані в тому випадку, якщо вони не бажають бути повністю залученими до системи IP. Звісно ж, що, крім інформованості, суб'єктам повинна забезпечуватись можливість реального вибору - участі або неучасті в інформаційній взаємодії при використанні пристроїв IP. Крім традиційних рішень, пов'язаних з дією відповідного обладнання та програмного забезпечення, даний принцип може також реалізовуватися за допомогою інноваційних рішень IP, що перешкоджатимуть на легальній і анонімній основі збору інформації або даватимуть можливість гнучкого, безпечного і простого управління їх функціоналом.

3. Захист персональних даних і приватного життя. Будь-який пристрій може прив'язуватися доінтернет-профілю свого власника; навіть якщо декларується анонімізація даних, за наявними накопиченими відомостями в істотній кількості випадків можливо ідентифікувати суб'єкта.

По-друге, виникає необхідність вироблення нових принципів щодо отримання розробником (продавцем) пристроїв (програмного забезпечення) згоди суб'єкта персональних даних на використання (обробку) персональних даних, в тому числі всіма учасниками IP.Виникає необхідність нової оцінки існуючих підходів до можливості виробників пристроїв IP здійснювати збір та перехоплення інформації в мережах зв'язку, а також дистанційного керування пристроями IP.

4. Захист персональних даних на ринку «Bigdata». Формується ринок Великих даних, які фактично виступають предметом угод. Крім питання про правовий режим інформації як об'єкта правовідносин, необхідно визначити, в якому обсязі в принципі Великі дані можуть бути об'єктом торгівлі.

Законодавство про персональні дані встановлює ряд вимог до обробки персональних даних, включаючи необхідність отримання згоди суб'єкта персональних даних, а також покладає на операторів ряд обов'язків щодо захисту персональних даних. Проблеми IP в даному випадку перетинаються з проблемами обробки Великих даних - «Bigdatamining».

Проблеми IP в даному випадку перетинаються з проблемами Великих даних. Обґрунтованими є сумніви в тому, що в таких умовах можна дотриматися принципів обробки персональних даних на основі конкретних і заздалегідь визначених цілей, і далеко не завжди об'єктивно можливо отримати згоду на це суб'єкта персональних даних.

Знижується можливість задекларованого знеособлення персональних даних в ситуації, коли статистично можливо отримувати інші "допоміжні" дані з багатьох додаткових джерел, число яких зростає.

В цьому випадку можливо запропонувати наступне: по-перше, запровадження на офіційному рівні підходу, заснованого на балансі захисту

персональних даних і технологічного розвитку. Такий підхід повинен ґрунтуватися на принципі формальної визначеності правових норм і розумного обмеження поняття персональних даних так, щоб воно дозволяло застосовувати норми послідовно і передбачувано, захищаючи при цьому "мінімум недоторканності приватного життя".

По-друге, в умовах функціонування Інтернету речей і Великих даних питання ставиться вже не про те, чи передавати дані певному оператору (інтернет - ресурсу) чи ні, а про те, чи передавати дані в Інтернет в цілому чи ні - після такої передачі дані починають накопичуватися і оброблятися невизначеним колом пристроїв і систем. Згода суб'єкта може бути виражена на факт такої передачі в цілому. У той же час додаткового опрацювання потребує питання про те, як бути з даними про конкретного суб`єкта, які можуть збиратися незалежно від його волі.

По-третє, в частині додаткових можливостей доступу правоохоронних органів і виробників до пристроїв користувачів з метою збору інформації - єдиного підходу серед фахівців немає. В такій ситуації будь-які варіанти рішень потребують пошуку компромісу між різними групами тиску.

Як висновок можливо зазначити, що існування Інтернету речей створює нові і принципово складні "правила гри" для правової системи. Класичні правові проблеми Інтернету (включаючи ідентифікацію користувачів, правовий статус інформаційних посередників і проблеми визначення юрисдикції), рішення яких ще не знайдено, модифікуються і інтенсифікуються на даному етапі розвитку інформаційного суспільства.

Відтак, виходячи з актуальності зазначених вище юридичних питань, для таких принципів необхідна розробка специфічної нормативно-правової бази, як на державному рівні, так і на міжнародному - з урахуванням транснаціонального характеру питання. В такому аспекті цікавим є досвід міжнародних організацій, наддержавних утворень та їх органів.

Так, Європейська комісія вже давно визначила Інтернет речей як одну з важливих сфер розвитку. У 2009 році в комюніке Європейської комісії від 18

червня 2009 року «Інтернет речей: план дій для Європи» підкреслюється, що розвиток IP не може бути залишено для регулювання лише приватному сектору - з огляду на важливість соціальних змін, які він несе з собою.[3] Цей план відобразив важливі напрямки роботи в сфері IP.

Важливість забезпечення безпеки, конфіденційності інформації та інших прав людини, пов'язаних з розвитком IP, не повинна, однак, привести до надмірної регламентації цієї сфери, що перешкоджатиме її подальшому розвитку.

Коли в рамках прийнятого раніше плану Європейська комісія у 2013 році проводила консультації з питання IP з приватним сектором, були висловлені різноманітні думки про те, наскільки в дійсності необхідна спеціальна регламентація Інтернету речей. Опоненти ставили під сумнів заходи держави щодо такого регулювання в силу того, що (1) Інтернет речей з'явився недавно і все ще бурхливо розвивається, а тому передбачити всі випадки необхідності регламентації неможливо, (2) велику роль у розвитку галузі відіграють приватні гравці, тому належна ступінь свободи і саморегулювання необхідні; (3) встановлені правила можуть, навіть, перешкоджати подальшому розвитку.

Розгляд проблем IP в США. Аналогічно висновкам в Європі, в Звіті Федеральної торгової комісії США для Сенату відзначається, що запровадження спеціального законодавства щодо Інтернету речей є передчасним. При цьому Комісія звертає увагу на необхідність

[3]На думку фахівців, виробники зацікавлені в засиллі подібних смарт-пристроїв, так як вони дозволяють їм збирати аналітику. Наприклад, постачальники домашньої техніки зможуть не тільки дізнаватися, як часто їхні прилади виходять з ладу, а й за допомогою даних про місце проживання клієнтів підлаштовувати свою рекламу і таким чином збільшувати продажі. Причому сам користувач може навіть не підозрювати про це, оскільки пристрої будуть з'єднуватися з Інтернетом не через домашню Wi-Fi-мережу, а за допомогою свого власного 5G-підключення. Вже сьогодні відбувається чимало інцидентів, які наочно демонструють, скільки нових небезпек здатний принести з собою Інтернет Речей, особливо, коли виробники керуються лише міркуваннями прибутку і мало дбають про кібербезпеку.
У 2015 році аналітики HewlettPackard досліджували захищеність IP-пристроїв і з'ясували, що 70% IP-пристроїв мали вразливості в безпеці облікових даних, а шифрування даних майже не застосовувалося, спостерігалися також проблеми з дозволом доступу. У 2016 році майже три чверті опитаних компанією Accenture користувачів заявили, що знали про можливості злому IP-девайсів. Питання безпеки в цій галузі вкрай критичне.

вдосконалення саморегулювання різних галузей IT-промисловості з метою поліпшення методів забезпечення конфіденційності і безпеки даних.

Проте, існуючі небезпеки беруться до уваги різними відомствами: наприклад, Федеральне бюро розслідувань випустило керівництво по боротьби із ризиками з точки зору кіберзлочинності, що виникають з поширенням IP.

Правове регулювання на рівні ЄС. На даний момент для розумних пристроїв не прийнято ніякого визначення базового рівня безпеки та дотримання конфіденційності приватного життя. Не існує також міцних юридичних підстав для довіри до IP-пристроїв і IP-послуг. Однак, Єврокомісія планує ввести обов'язкову сертифікацію або іншу аналогічну процедуру для пристроїв, що підключаються до IP. Запропонована ініціатива "Building a Europeandataeconomy"[4] так само вносить вклад у створення єдиного європейського ринку для Інтернету речей. Дана ініціатива передбачає розробку політики і правові рішення, що стосуються вільного потоку даних через національні кордони, а також питання відповідальності в таких середовищах як Інтернет речей.

Нова рамкова система захисту персональних даних в ЄС була прийнята 8 квітня 2016 року у формі Загального регламенту щодо захисту персональних даних, GeneralDataProtectionRegulation (GDPR). GDPR замінить чинну Директиву про захист персональних даних і буде безпосередньо застосовуватися в усіх країнах-учасницях Євросоюзу без необхідності в розробці імплементації національного законодавства. Регламент буде введений в дію 25 травня 2018 року.

Розширення територіальної юрисдикції. GDPR поширюється на організації за межами ЄС, чия діяльність з обробки персональних даних пов'язана з пропозицією товарів і послуг (навіть безоплатними) суб'єктам даних в ЄС або з моніторингом їх поведінки на території ЄС.

[4]Building a European data economy as a part of the Digital Single Market strategy (Materials of the European Commission): https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

Закладена конструктивна конфіденційність. GDPR накладає на контролерів даних обов'язки вести певну документацію, виконувати оцінку впливу обробки персональних даних на права суб'єктів даних, запровадити захист даних на конструкційному рівні і за замовчуванням, наприклад, використовуючи підхід мінімізації даних.

Інспектори із захисту даних. У певних обставинах обробники і контролери даних будуть зобов'язані призначити інспектора по захисту даних (DataProtectionOfficer, DPO) в рамках своєї програми звітності.

Роль обробника даних. Одним з найважливіших нововведень GDPR є те, що у розробників даних вперше з'явилися прямі обов'язки: вести письмовий реєстр операцій з обробки персональних даних, виконаних від імені та за дорученням кожного контролера; призначити, якщо потрібно, інспектора із захисту даних; призначити при певних обставинах представника в ЄС (якщо у обробника немає представництва в ЄС); повідомляти контролера про виявлені витоки персональних даних без необґрунтованої затримки.

Згода суб'єкта персональних даних на обробку. Згода має бути надана вільно, має бути чітко висловлена і однозначна. Згоду на обробку персональних даних можливо настільки ж легко відкликати як і надати. Контролер даних зобов'язаний бути в змозі надати докази отримання згоди.

Інформація про добросовісну обробку даних. Контролери даних як і раніше зобов'язані надавати суб'єктам даних прозору інформацію про обробку даних, причому в момент збору персональних даних. Існуючі форми повідомлень про обробку повинні бути переглянуті, оскільки вимоги GDPR набагато більш деталізовані в порівнянні з діючою Директивою. Наприклад, за новими правилами повідомлення повинно містити більш широку інформацію, а також доводити до відома суб'єкта даних його права (таких як право на відкликання згоди) і про термін зберігання даних.

Повідомлення про витік даних. Контролери даних зобов'язані повідомляти DPA про витік даних, без невиправданої затримки - по можливості протягом 72 годин після виявлення витоку.

Запровадження системи штрафів. GDPR встановлює багаторівневі санкції за порушення законодавства про захист даних, що дозволяють DPA призначати штрафи за деякі порушення в розмірі, що досягає найбільшої з двох цифр: 4% річного світового обороту організації або 20 мільйонів євро (зокрема, за порушення вимог до міжнародної передачі даних або основних принципів їх обробки - як умов для отримання згоди).

Нова Європейська рада із захисту даних. Незалежна Європейська рада із захисту даних (EuropeanDataProtectionBoard, EDPB) буде складатись з керівника Європейської служби із захисту даних і старших представників національних DPA Євросоюзу. Призначення Ради - публікація висновків та керівних принципів, забезпечення однакового застосування GDPR і звітності перед Єврокомісією.

Права суб'єктів даних. Однією з головних цілей Європейської Комісії при розробці нової рамкової системи захисту даних було підвищення захисту прав громадян. Цей мотив чітко простежується в посиленні прав суб'єктів даних. Зокрема, це право особи вимагати інформацію щодо обробки його персональних даних, право доступу до даних за певних обставин і право виправлення неправильних даних. Також є право обмежити певну обробку даних і право заперечувати проти обробки своїх персональних даних для цілей прямого маркетингу.

Громадяни можуть також вимагати повернення своїх персональних даних в структурованому вигляді для полегшення їх передачі іншому контролеру (так звана портативність даних).

Величезну популярність, особливо після рішення Європейського суду за позовом «Google проти Іспанії», отримало так зване “право на забуття”, або право на видалення даних. У певних ситуаціях, таких як відкликання згоди, за відсутності інших законних підстав для обробки, суб'єкт даних може

вимагати від контролера негайно видалити свої персональні дані. Також передбачено обов'язок прийняти розумні заходи щодо інформування третіх сторін про те, що суб'єкт даних вимагав видалення будь-яких посилань на такі дані та будь-які їх копії. На практиці це буде часто досить складно здійснити.

Відзначимо, що контролер даних зобов'язаний реагувати на такі інформаційні запити протягом місяця, з можливістю продовження цього терміну для особливо складних запитів. Контролерам даних потрібно ввести чіткі процедури для виконання цих зобов'язань. Інформація повинна бути надана безкоштовно, за винятком випадків, коли запит є "явно необґрунтованим або надмірним".

Регламент 2016/679 набув чинності 25 травня 2016 року і буде введений в дію 25 травня 2018 року. З цього моменту Директива 95/46 / ЕС втрачає чинність.

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

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

ІНТЕРНЕТ РЕЧЕЙ ТА ІНФОРМАЦІЙНА БЕЗПЕКА: ДЕЯКІ ПРАВОВІ ПРОБЛЕМИ

У зв'язку зі швидким розвитком ІТ-відносин все частіше виникають нові об’єкти цивільного обігу, правова природа яких не завжди є чітко зрозумілою. Це породжує невизначеність, неврегульованість певних відносин, оскільки законодавець не встигає настільки швидко реагувати на постійні зміни сфері інформаційних технологій. Деякі об’єкти цивільного обігу існують на межі правових норм щодо власності та інтелектуальної власності, оскільки поєднують в собі властивості предметів матеріального світу та інформаційні технології. Найбільш яскравим прикладом таких комплексних об'єктів на сьогодні є так званий Інтернет речей (Internet of Things – IoT).

Сьогодні Інтернет речей визначається як концепція комунікаційної мережі фізичних або віртуальних об'єктів («речей»), які мають технології для взаємодії між собою та з навколишнім середовищем, а також можуть виконувати певні дії без втручання людини. Сутність цієї концепції полягає в тому, щоб всі предмети побуту, товари, вузли технологічних процесів тощо, були оснащені вбудованими комп'ютерами та сенсорами, мали змогу обробляти інформацію, що надходить із навколишнього середовища, обмінюватися нею та виконувати різні дії в залежності від отриманої інформації [1]. Також Інтернет речей може бути визначено як «речі», такі як пристрої та датчики, відмінні від комп’ютерів, смартфонів або планшетів, які поєднуються, взаємодіють або передають інформацію один з одним або один від одного завдяки Інтернету [2].

До основних компонентів Інтернету речей відносяться:

1. фізичні об’єкти, оснащені датчиками та механізмами для прийому та обробки сигналів;
2. Інтернет-доступ: стандарти і протоколи зв'язку для підключення датчиків до єдиної мережі;
3. Мережа (зв'язок): доступ в Інтернет: бездротовий/дротовий доступ, Wi-Fi, Bluetooth, ZigBee, VPN, мережі покоління 2G/3G/4G;
4. хмарні сервери: корпоративні і хмарні обчислювальні системи/ платформи, здатні обробляти дані і виконувати інші аналітичні операції в режимі реального часу, зберігання і доставка контенту, хостинг додатків;
5. додатки і взаємодія з користувачами: взаємодія людей, додатків і бізнес-процесів [3].

Останнім часом кількість пристроїв, підключених до Інтернету невпинно зростає. Так, у 2003 р. до Інтернету було підключено 500 мільйонів пристроїв, а вже у 2010 р. їх кількість зросла до 12,5 мільярдів. Прогнози щодо Інтернету речей вражають – компанії прогнозують до 2020 року підключення до Інтернету від 26 до 50 мільярдів пристроїв [4]. Тобто практично всі речі навколо нас можуть стати вузлами Інтернету речей.

Звісно ж, поширення Інтернету речей потребує його детального правового регулювання. Перед спеціалістами вже сьогодні постає низка проблем, пов’язаних із Інтернетом речей: правовий режим інформації, персональні дані й приватне життя, інформаційна безпека, розробка понятійного апарату, проблема ідентифікації осіб, відповідальність учасників цих відносин, проблема збору доказів тощо.

Сьогодні у світі активно робляться спроби визначити, які саме проблеми можуть виникнути у зв'язку із поширенням такого явища як Інтернет речей та врегулювати відносини, пов’язані із його існуванням. Так, у 2014 році Європейська комісія опублікувала позицію з даного питання, детально розглянувши натільні пристрої і пристрої системи «розумний будинок». Серед викладених Комісією рекомендацій є вимога про надання користувачам повного контролю над своїми даними. Вищезгадана позиція також передбачає операції, які організаціям необхідно взяти до уваги для забезпечення відповідності вимогам законодавства Європейського союзу про захист даних. На початку 2015 року члени Конгресу США Сьюзан Дельбене і Даррелл Ісса оголосили про формування фракції Конгресу з питань технологій IoT. Метою фракції є підвищення обізнаності членів Конгресу про можливості і проблеми, які створює упровадження рішень IoT в сферах охорони здоров'я і транспорту, удома і на роботі, а також надалі пошук балансу між збором даних, що генеруються за допомогою IoT, і захистом персональних даних споживачів. Приблизно в той же час Федеральна торгова комісія опублікувала звіт, що містить рекомендації по мінімізації даних і розробці програм саморегуляції в цілях підвищення рівня конфіденційності і безпеки .

Пізніше, у 2016 році, міжнародна юридична фірма Dentons спільно з Некомерційним Партнерством «RUSSOFT» розробили відкриту концепцію правового регулювання Інтернету речей. Основною метою створення концепції є формування юридичної термінології та єдиного бачення проблем правового регулювання у сфері Інтернету речей. У концепції поставлено питання про можливі спільні принципи регулювання, серед яких можуть

бути принципи інформованості користувачів та вільної участі у системі Інтернету речей, визначено основні проблемні питання, що виникатимуть у сфері Інтернету речей, серед яких підкреслюються проблеми ідентифікації користувачів, захисту персональних даних, визначення юрисдикції, відповідальність інформаційних посередників тощо [2].

За даними дослідників, на сьогодні вже існують деякі прецеденти вирішення проблем, що виникають у сфері Інтернету речей, але ще багато питань залишаються без відповідей, зокрема, йдеться про відповідальність за несправність підключених пристроїв та нещасні випадки, викликані цим, відповідальність за втрату інформації, доля відповідальності компаній та споживачів тощо. Ще одним важливим питанням, яке потребує відповіді, є питання про те, хто є володільцем інформації: компанія-виробник датчика, компанія-виробник пристрою або особа, чиї дані вимірюються та збираються. Представники законодавчих органів ЄС підкреслюють, що права на персональні дані належать громадянам, але так відбувається не завжди. Навіть у тих випадках, коли право на інформацію не викликає сумнівів, залишається відкритим питання про строк дії прав на зібрані дані [3].

Отже, чи не найважливішим проблемним питанням у сфері Інтернету речей на сьогодні є питання інформаційної безпеки та захисту персональних даних. В Інтернеті речей кожна річ крім фізичного втілення існує онлайн. Використання бездротових методів передачі даних відкриває багато можливостей, у тому числі, і неправомірного використання, для захисту від якого потрібні методи криптографії та фізичного захисту. У випадку взаємодії речей ситуація ускладнюється тим, що необхідною є згода суб'єкта на те, щоб збирати, обробляти, зберігати та передавати інформацію про нього. Така ситуація дає деяким дослідникам підстави вести мову навіть про правосуб'єктність речей, що входять до IoT [5].

Очевидно, що з розвитком Інтернету речей виникнуть і інші питання, пов'язані з правовим регулюванням відносин щодо речей, які крім своїх основних функцій, будуть виконувати ще й низку технологічних завдань, а

також стануть носіями інформації. Постануть і питання правової охорони нових об'єктів інтелектуальної власності. Всі ці проблеми поки що лише окреслюються, але вже потребують активного пошуку шляхів їх вирішення.

Література:

1. Інтернет речей [Електронний ресурс]. – Режим доступу: http://glossary.starbasic.net/index.php?title=%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9

2. Открытая концепция «Интернет верей: правовые аспекты (Российская Федерация)» [Електронний ресурс]. – Режим доступу: http://www.dentons.com/ru/whats-different-about-dentons/connecting-you-to-talented-lawyers-around-the-globe/news/2016/june/dentons-develops-russias-first-ever-whitepaper-on-the-legal-aspects-of-the-internet-of-things

3. Интернет вещей. Безграничные возможности взаимодействия человека и машины. Медиасектор и индустрия развлечений. – [Електронний ресурс]. – Режим доступу: http://www.ey.com/Publication/vwLUAssets/EY-mne-internet-of-things-rus/$File/EY-mne-internet-of-things-rus.pdf

4. Храмцов П. Всеобъемлющий интернет: прогнозы и реальность / П. Храмцов // Открытые системы. – 2013. - № 4 [Електронний ресурс]. – Режим доступу: http://www.osp.ru/os/2013/04/13035552/

5. Исаков В.Б., Сарьян В.А., Фокина А.А. Правовые аспекты внедрения Интернета вещей // ИТ-Стандарт. – 2015. - № 4-1 (5). – С. 9-16. – [Електронний ресурс]. – Режим доступу: https://elibrary.ru/item.asp?id=25208816

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

Кушнір М. О.,
к. н. з держ. упр., доцент, Заслужений юрист України, докторант кафедри публічного управління та публічної служби Національної академії державного управління при Президентові України

ДО ПИТАННЯ ІНСТИТУЦІЙНО-ПРАВОВОЇ МОДЕЛІ ПІДГОТОВКИ МАЙБУТНЬОГО ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ РОБОТОТЕХНІКИ

«Майбутнє приходить раніше, ніж ми його очікуємо»
Р.Саракко, 2017

Людство завжди намагалося полегшити свою працю за рахунок використання спроможностей як біологічних, так і фізичних створінь. Нині ми стоїмо на порозі високих технологій, вагому частку в яких займають

високотехнологічні, людиноподібні роботи. В основу цих пристроїв покладено штучний інтелект і вони, по суті, створюють новий ринок та уособлюють початок нової промислової революції, яка, вочевидь, зачепить все людство. Тому надзвичайно важливим завданням для держави є спрямувати свої зусилля на підготовку суспільства до технологічних змін, убезпечення його від можливих загроз з боку означених пристроїв та встановлення своєчасних і адекватних правил поведінки на новостворюваному ринку.

Закони щодо роботів обговорюються в усьому світі. Відомий американський футуролог Р. Курцвел на початку 2017 року виступив з прогнозом, що такі закони будуть прийняті у всьому світі до 2022 року [8]. Чому ж такий інтерес у суспільстві викликає це питання?

Як вбачається, причина криється у тому, що стрімкий розвиток інформаційних технологій загалом і робототехніки зокрема об'єктивує проблему меж розвитку та продуктивності людини: людська істота через біологічні обмеження не може подолати ці межі на відміну від машини, яка, при наявності у неї відповідних можливостей (ресурсів), таких меж не має. У світі вже є прецеденти використання роботів у різних сферах, зокрема, для виконання важких, працевмісних робіт; залучення їх для охорони громадського спокою і т.д. При цьому, людство вже зараз є свідком окремих випадків так званого «повстання» машин: наприклад, у 2016 році в Китаї на виставці China Hi-Tech Fair робот Little Chubby, якого залишили без нагляду на деякий час, несподівано «врізався» у скляний намет і травмував відвідувача [1]. Окрім того, однією із найбільших загроз, які стоять перед людством у зв'язку із впровадженням роботів, є масове безробіття. Так, за висновками PwC (однієї із найвідоміших аудиторських фірм світу) автоматизація може знищити в найближчі п'ятнадцять років третину робочих місць в Великобританії [6].

Отже, можливості штучного інтелекту, разом з його великими проривними спроможностями, виявляють об'єктивні загрози для людини, в

першу чергу, через здатність до самовдосконалення, самоосвіти. Напевно, зважаючи на це, відомий інженер і підприємець І.Маск стверджує, що штучний інтелект є основною загрозою, з якою людство зіштовхується як цивілізація, у зв'язку з чим у цій сфері необхідне державне регулювання, яке б стримувало виробників роботів [3].Тому у всьому світі триває робота щодо унормування питань, пов'язаних з використанням роботів.

Так, закони робототехніки сформульовані у художніх працях А.Азімова і вони можуть виступати правовою парадигмою унормування проблем, пов'язаних із роботизацією.

Зокрема, ці закони враховані у тривалій роботі європейських експертів над проблематикою щодо питань, пов'язаних з використанням роботів, що призвело до прийняття 16 лютого 2017 року Європейським парламентом Резолюції для Комісії ЄС «Норми цивільного права про робототехніку» (P8_NA-PROV(2017)0051) [9]. У цьому документі Комісії ЄС запропоновано розглянути низку питань у означеному контексті, зокрема, щодо:

- можливості створення Агентства ЄС щодо робототехніки та штучного інтелекту, яке б в інституційному плані було спеціалізованим органом, що володіє компетенцією в технічних, етичних та регуляторних питаннях (пункт 16);
- законодавчого урегулювання юридичних питань, пов'язаних з розробкою та використанням штучного інтелекту та робототехніки у наступні 10-15 років (пункт 51);
- вимог до майбутніх нормативно-правових актів (пункти 52-55).

Прикметним є додання до вказаної вище Резолюції Хартії Робототехніки, що складається з:

1. Кодексу етичних норм розробників у сфері робототехніки;
2. Кодексу для комітетів щодо етики наукових досліджень;
3. ліцензій (вимог) для розробників та для користувачів.

Південна Корея є однією із перших держав світу, яка закріпила правовий статус роботів у своєму законодавстві. Ще у 2008 році цією

державою був прийнятий Закон про сприяння розвитку і поширенню розумних роботів [2]. Відповідно до статті 1 вказаного Закону, метою вказаного акту є сприяння поліпшенню якості життя громадян і розвитку економіки країни шляхом розробки і просування стратегії сталого розвитку індустрії розумних роботів, а також створення необхідної основи для розвитку і поширення цих роботів.

Французькі ініціативи у сфері робототехніки ще у 2013 році порушили питання щодо наявності етичних питань у ній (сфері) і висновували, що необхідно здійснювати партнерство в контексті:

- соціальної і етичної прийнятності, зокрема, у сферах оборони і безпеки;
- відповідних ролей людей і «розумних» машин (пошук рівноваги, інструментів, що має бути відображено в основному законі про етику або професійну етику [4, с. 26].

Бізнес Росії вже розпочав розробку кіберкодексу – зводу законів, який введе роботів у правове поле держави. Початком у цій роботі є законопроект Д.Грішина щодо внесення змін до Цивільного кодексу РФ в частині удосконалення правового регулювання відносин у сфері робототехніки [5]. В цьому законопроекті передбачається, зокрема, розробка федерального законодавства про робототехніку (пропонується провести реєстрацію всіх видів моделей роботів-агентів у єдиному державному реєстрі роботів-агентів, порядок ведення якого і має визначатися вказаним законодавством).

У контексті вкладеного матеріалу розглянемо ситуацію з інституційно-правовим забезпеченням використання робототехніки в Україні. На жаль, аналіз правового поля держави, законодавчих ініціатив, зареєстрованих у Верховній Раді України, відповідного наукового доробку, свідчить про те, що вітчизняні управлінці та правники поки що не усвідомлюють небезпеки, яка криється у повсюдному використанні штучного інтелекту, та реальні перспективи його бурхливого розвитку. У дослідженнях вітчизняної науки «публічне управління та адміністрування» також відсутні ґрунтовні дослідження, присвячені проблематиці забезпечення сфери робототехніки.

Як вбачається, невелика частка використання в Україні новітніх технологій не виправдовує відсутність належної уваги як усього суспільства, так і держави до питання інституційно-правового забезпечення цієї сфери суспільних відносин.

Чинне українське законодавство згадує про розвиток робототехніки лише у контексті переліку стратегічних пріоритетних напрямів інноваційної діяльності на 2011-2021 роки, визначених у ст. 4 Закону України «Про пріоритетні напрями інноваційної діяльності в Україні» [7].

На основі досліджених актів формального законодавства та їх проектів, що діють або розроблені у окремих країнах, а також науково-практичних підходів у вказаній сфері нами пропонується *інституційно-правова модель підготовки майбутнього законодавства України у сфері робототехніки*, згідно з якою:

1) оптимальним управлінським підходом у цій сфері є «м'яке» законодавство - виражене у загальних термінах і обмежене суттєвими елементами, що враховують основні права і обов'язки суб'єктів сфери робототехніки;

2) визначається «скринька» інструментів, до якої включається тріада факторів, що мають бути враховані:

- науково-дослідні передумови до формування штучного інтелекту;
- морально-етичні принципи, що лежать у основі підготовки законодавства у сфері робототехніки та
- убезпечення можливих ризиків.

Література:

1. Епоха роботів – як нам мирно уживатися із «залізячками», що раптово порозумнішали. [Електронний ресурс]. – Режим доступу : http://nv.ua/techno/lectures/epoha-robotov-kak-nam-mirno-uzhivatsja-s-vnezapno-poumnevshimi-zhelezkami-585481.html. – Назва з екрану.

2. Закон о содействии развитию и распространению умных роботов № 9014 от 28.03.2008, с последующими изменениями и дополнениями. Южная Корея. [Електронний ресурс]. – Режим доступу : http://robopravo.ru/zakon_iuzhnoi_koriei_2008. – Назва з екрану.

3. Илон Маск назвал основную угрозу для человечества. [Електронний ресурс]. – Режим доступу : https://comments.ua/world/588974-ilon-mask-nazval-osnovnuyu-ugrozu.html. – Назва з екрану.

4. Инициативы Франции в сфере робототехники, 2013 год. [Електронний ресурс]. – Режим доступу : http://robopravo.ru/initsiativy_frantsii_v_sfierie_robototiekhniki_2013. – Назва з екрану.

5. О внесении изменений в Гражданский кодекс Российской Федерации в части совершенствования правового регулирования отношений в сфере робототехники : проект Гришина Д.С. [Електронний ресурс]. – Режим доступу :https://www.dentons.com/ru/insights/alerts/2017/january/27/dentons-develops-first-robotics-draft-law-in-russia. – Назва з екрану.

6. PwC: автоматизация может уничтожить треть рабочих мест в Британии. [Електронний ресурс]. – Режим доступу : https://www.audit-it.ru/news/personnel/902149.html. – Назва з екрану.

7. Про пріоритетні напрями інноваційної діяльності в Україні : Закон України від 8 вер. 2011 р. № 3715-VI (зі змінами). [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3715-17. – Назва з екрану.

8. Технический директор Google расписал будущее мира: прогноз до 2099 года. [Електронний ресурс]. – Режим доступу : https://inforesist.org/texnicheskij-direktor-google-raspisal-budushhee-miraprognoz-do-2099-goda/. – Назва з екрану.

9. Civil Law Rules on Robotics (P8_TA(2017)0051) : European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). [Електронний ресурс]. – Режим доступу:http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML +TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN. – Назва з екрану.

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

Кравченко О. М.,
аспірант, Академії праці,
соціальних відносин і туризму.

ПРАВОВІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Звісно, що сучасна людина не може обійтись без технологій нового покоління, які стрімко розвиваються. Але виникає проблема правового характеру, щодо правового унормування термінології та інших правових відносин в цій сфері.

Як влучно зазначає з цього приводу у своїх працях О. Баранов, що в останні кілька років пошук шляхів вирішення правових проблем, що виникають у процесі розвитку і використання технологій IP, набуває все

більшу актуальність. Широко відомо, що правова наука вимагала і вимагає уважного ставлення до своєї термінологічної системи. Технологічні революції, а особливо 4-та технологічна революція, що стоїть на порозі, сприяли появі багатьох термінів, які згодом стали широко використовуватися в праві. Досвід застосування технократичних термінів у правовій науці свідчить про необхідність формулювання дефініцій цих термінів, перш за все, з позиції інтересів права, але з безсумнівним збереженням технологічної (технічної) сутності явища або об'єкта, що описується [1, с.96].

Про реальність втілення в життя нової технології можна судити, якщо проаналізувати, хто розвиває її сьогодні і наскільки багато фінансів вже вкладено в дослідження та впровадження [2].

Основні прихильники нової технології: Cisco (CiscoIoTServicesPortfolio – портфель сервісів для IoT), Intel (IntelIoTPlatform – платформа для IoT, лабораторія Інтернету речей IntelIgnitionLab), Microsoft (операційна система Windows 10 IoT, фреймворк AllJoyn, хмарний сервіс Azure), IBM (IBM Bluemix - понад 100 відкритих програмних інструментів і хмарних сервісів, IBMCloud) та багато інших не менш відомих фірм [2].

Потрібно зазначити, що «Інтернет речей» є сучасним етапом розвитку Інтернету в наш час, який значно розширює можливості людини для збору, аналізу і розподілу даних та ін.

На думку науковців, до основних проблем Інтернету речей можна віднести інформаційну безпеку і захист персональних даних. Технології IP значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркулювання і використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання таких даних та забезпечення їх захисту від несанкціонованого використання. Можна зазначити, що широке використання технологій Інтернету речей призводить до необхідності вирішення таких основних правових проблем:

- 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).
- Крім того, необхідність створення багаторівневої і багатооб’єктної системи захисту персональних даних потребує формування нової системи правового регулювання [3, с.90].

Підводячи підсумки потрібно відмітити, що на нашу думку, треба узагальнити практику застосування законодавства щодо вироблення єдиних підходів до технічного регулювання «Інтернету речей» та розробити пропозиції, на предмет вдосконалення законодавчих актів України у цій сфері.

Література:

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

2. Могильний С. Б. Технології «Інтернету речей» - підготовка фахівців актуально в часі // Збірник матеріалів МНК. – 2016 [Електронний ресурс]– Режим доступу: file:///C:/Users/Valentina%20Ivanovna/Downloads/73606-153907-1-SM.pdf

3. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей / О.А. Баранов, В.М. Брижко // Інформація і право. – 2016. – № 2(17). – С. 85-91.

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

Шпига П. С.,
к. т. н., професор кафедри інформаційної політики та цифрових технологій Національної академії державного управління при Президентові України

ПОНЯТТЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ В НОРМАТИВНО-ПРАВОВИХ ДОКУМЕНТАХ УКРАЇНИ

Нині держава, громадяни і бізнес є активними споживачами інформаційних ресурсів. Виникнення та становлення "Інтернету речей" є новим етапом розвитку глобальної мережі, що передбачає підключення великої кількості пристроїв та лавинним зростанням навантаження на мережу. Органи державної влади та місцевого самоврядування теж розвивають власний інформаційний простір, намагаються удосконалити взаємодію розрізнених компонентів інформаційно-телекомунікаційної інфраструктури. Ці інтеграційні процеси та новітні цифрові технології мають забезпечити створення якісно нових прозорих форм організації діяльності публічної адміністрації, її взаємодії з громадянами та бізнесом шляхом надання доступу до відкритих державних цифрових ресурсів та електронних послуг.

Для подальшого аналізу сутності та проблем формування інформаційно-телекомунікаційної інфраструктури публічного управління важливим є питання термінології. Єдина, точно визначена і всім зрозуміла термінологія необхідна як при обговоренні концептуальних чи теоретичних матеріалів, так і при визначенні умов роботи з конкретними комп'ютерними системами. Вона дозволяє виокремити, конкретизувати, прояснити найсуттєвіші проблеми, зробити дослідження більш компактним і раціональним, значно збільшити точність формулювань основних теоретичних і практичних висновків, створити можливості контролю виконання запланованих заходів. Змістовні визначення нових понять важливі також при формуванні сучасних ІТ-компетенцій публічних службовців, які працюють з системою, та одержувачів е-послуг. Необхідність наведення термінів у нормативно-правових доку-

ментах (НПД) також регламентована постановою КМ № 870 від 06.09.2005 щодо правил підготовки проектів актів Кабінету Міністрів України. Проте нині ми змушені констатувати нерозвиненість вітчизняної наукової та нормативно затвердженої термінології, відсутність важливих для розвитку цифрових технологій стандартів.

Історично так склалося, що комп'ютеризація органів влади України відбувалася без єдиного плану, чіткої стратегії та досконалих стандартів, які б уніфікували вимоги до програмного, технічного, організаційного забезпечення інформаційно-телекомунікаційних систем органів влади. В установах держави впроваджувалися різні за складністю, завданнями, інтерфейсами, програмним та технічним забезпеченням комп'ютерні системи (інформаційно-аналітичні системи, бази даних, гео- інформаційні системи, ситуаційні центри тощо). Нині це програмно-технологічне різноманіття породжує серйозні проблеми реінжирінгу "успадкованих систем" (legacysystems) та забезпечення інтеропрабельності при наданні електронних послуг. Подальше використання цих систем у незмінному вигляді стає обтяжливим і навіть неможливим.

Протягом останніх десяти років органами влади України прийнято ряд нормативно-правових документів спрямованих на удосконалення інформаційно-телекомунікаційних систем, усунення розрізненості і покращення їхньої взаємодії, зменшення невиправданих витрат на обслуговування. У цих НПД в тій чи іншій формі наявні проблеми, програми чи окремі заходи щодо формування, модернізації чи підвищення ефективності телекомунікаційних об'єктів. Проте задовільного трактування понять "інформаційна інфраструктура", "телекомунікаційна мережа", "інформаційно-телекомунікаційна інфраструктура" ні в науці, ні у вітчизняних нормативно-правових документах нами не виявлено.

Серед термінів, які використовуються при обговорені інформаційно-телекомунікаційної інфраструктури публічного управління, на нашу думку, першочергового обговорення потребують терміни, які визначають основні

проблеми та завдання, найчастіше зустрічаються у відповідних нормативно-правових документах і викликають сумніви щодо однозначності їхнього тлумачення. Останнім документом, що стосується інформаційно-телекомунікаційної інфраструктури публічного управління і який визначає основні засади реалізації державної політики у відповідній сфері, нині є "Концепція розвитку системи електронних послуг в Україні" схвалена розпорядження Кабінету Міністрів України від 16.11.2016. Мета концепції полягає у визначенні "напрямів, механізму і строків формування ефективної системи електронних послуг в Україні для задоволення інтересів фізичних та юридичних осіб через розвиток і підтримку доступних та прозорих, безпечних та не корупційних, найменш затратних, швидких та зручних електронних послуг". Важливою складовою цієї системи є інформаційно-телекомунікаційна інфраструктура (ІТКС), що має забезпечувати надання електронних послуг на основі встановлених вимог. В Концепції є частина, що стосується термінології. На жаль, визначення чи опис всієї системи чи її компонент відсутні як в основному документі, так і в двох законах ("Про адміністративні послуги" і "Про електронні документи та електронний документообіг"), на які посилається Концепція. Серед першочергових проблем у Концепції названо відсутність єдиної інформаційно-телекомунікаційної інфраструктури, яку заплановано сформувати на першому етапі (2016-2017 роки). В концепції говориться, що формування ІТКС повинно здійснюватися за концептуальною моделлю системи електронних послуг, яка використовує сервіс-орієнтований підхід, модульний принцип з метою поєднання та повторного використання її компонентів під час запровадження нових електронних послуг та є достатньо універсальною для застосування як на місцевому, так і на національному рівні. Визначення ІТКС, програмно-технічні складові, вимоги та відповідальні за розробку відповідної архітектури у цьому та інших НПД не наводяться. Хоча для розуміння можливостей цієї інфраструктури, як елемента системи електронних послуг, та визначення усіх компонентів

системи є вкрай важливим. На нашу думку названа в Концепції ІТКС є засобом інформатизації і тому при її розвитку чи формуванні слід керуватися чинною постановою Кабінету Міністрів України "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації" № 121 від 04.02.1998 (із змінами), яка серед іншого вимагає "розроблення технічного завдання на створення або модернізацію засобів інформатизації" та дотримання державних стандартів.

У законі України "Про захист інформації в автоматизованих системах" наводяться два визначення: інформаційно-телекомунікаційна система — сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле; інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

В стратегії розвитку інформаційного суспільства в Україні від 15.05.2013 наводиться визначення інформаційної інфраструктури – це сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування.

В текстах перелічених вище нормативно-правових документів також зустрічаються такі терміни: інформаційна інфраструктура електронного урядування, інформаційна система електронної взаємодії державних електронних інформаційних ресурсів, відомча інформаційна система, засоби телекомунікаційного зв’язку тощо. Більшість із наведених термінів не мають чітких означень, пояснень особливостей застосування, програмно-технічних характеристик. Це унеможливлює встановлення новизни, можливостей, завдань, відповідальності, ступеню готовності, відповідності стандартам вказаних об'єктів, створює умови для корупційних зловживань.

Наведене у законі "Про телекомунікації" визначення телекомунікаційної мережі, як "комплексу технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь - якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням", говориться тільки про комплекс технічних засобів телекомунікацій та споруд. Відсутність у цьому визначенні програмного та інших видів забезпечення необґрунтовано звужує поняття телекомунікаційної мережі до апаратної та дротової компонент, тим самим зводячи його до наведеного в цьому ж законі визначення технічні засоби телекомунікацій - обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж.

Узагальнюючи наведені вище терміни ми пропонуємо таке визначення: інформаційно-телекомунікаційна інфраструктура публічного управління є програмно - технічним комплексом спрямованим на технологічне забезпечення інформаційної діяльності органів державної влади та органів місцевого самоврядування щодо надання управлінських послуг, покращення їх взаємодії з громадянами та суб'єктами господарювання шляхом використання локальних комп'ютерних мереж, інтернет та інтранет технологій. З технічної точки зору вона включає: територіально розподілені локальні та глобальні телекомунікаційні мережі спеціального призначення і загального користування, робочі станції, сервери, сховища та бази даних, засоби електронної комунікації та управління інформаційними потоками, автоматизовані робочі місця з відповідним програмним забезпеченням. З системної точки зору цей об'єкт є складною територіально розподіленою системою, яка складається з великої кількості підсистем, кожна з яких сама має елементи стохастики та взаємодіє із стохастичним оточенням. Елементи підсистем теж є складними об'єктами, вони періодично змінюються, удосконалюються, доповнюються та оновлюються.

Таким чином, поряд із позитивними тенденціями у формуванні інформаційно-телекомунікаційної інфраструктури органів влади існує і низка недоліків. Головним із них є проблема підвищення якості термінології, певна несистемність нормативно-правових документів, які стосуються телекомунікаційних об'єктів. Значну кількість НПД ухвалюють для вирішення певних тактичних завдань, без урахування вітчизняного та зарубіжного досвіду, що негативно впливає на процеси реалізації комп'ютерних систем та допускає корупційну складову.

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

[1] ***Білощицький А. О.***
д.т.н., професор, професор кафедри, мережевих та Інтернет технологій.
[2] ***Білощицька С. В.***
к.т.н., доцент, доцент кафедри інформаційних технологій проектування і прикладної математики.
[3] ***Вацкель В. Ю.***
начальник сектору Інформаційно-обчислювального центру.
[4] ***Вацкель І. Ю.***
аспірант кафедри технологій управління.
[5] ***Кучанський О. Ю.***
к.т.н.,доцент кафедри кібернетичної безпеки та комп'ютерної інженерії Київський національний університет імені Тараса Шевченка Київський національний університет будівництва і архітектури.

ПРОБЛЕМИ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ІНТЕРНЕТ РЕЧЕЙ «РОЗУМНИЙ БУДИНОК» НА ПРИКЛАДІ IT LYNX SMARTHOUSE

Для автоматизації завдання управління будинком з використанням технології Інтернет речей була розроблена концепція «Розумний будинок» IT Lynx SmartHouse. Інформаційна технологія IT Lynx SmartHouse - це програмно-апаратне рішення (IoT), яке пропонує використання концепції

«Розумний будинок» не тільки для окремих житлових квартир або приватних будинків, а для всього житлового комплексу в цілому, і дозволяє здійснювати контроль і управління різними параметрами на конкретному об'єкті цілий рік в режимі реального часу з будь-якої точки земної кулі.

Було побудовано концепцію «Розумний будинок» не тільки для окремих житлових квартир, а для всього житлового комплексу в цілому, а саме:

1. Автоматичне управління поливом території житлового комплексу. Відзначимо, що розроблений комплекс IT Lynx SmartHouse, дозволяє управляти поливом як використовуючи налаштування диспетчера (садівника), так і повністю в автоматичному режимі, ґрунтуючись на даних, отриманих з датчиків температури і вологості ґрунту (рис. 1).

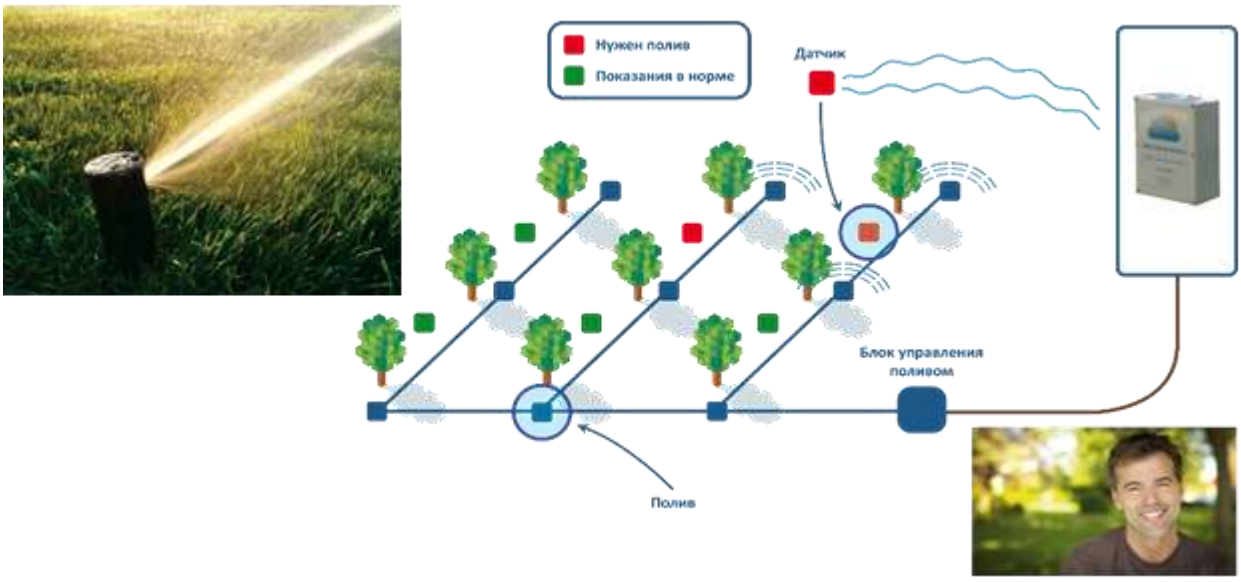

Рис. 1. – Схема автоматичного управління поливом

2. Автоматичне управління освітленням у житловому комплексі.

Розроблена технологія «Розумний будинок» IT Lynx SmartHouse дозволяє здійснювати управління освітленням на вулиці, в під'їздах житлових будинків, ілюмінацією і підсвічуванням дерев за заданими параметрами або повністю в автоматичному режимі за допомогою датчиків світла (рис. 2).

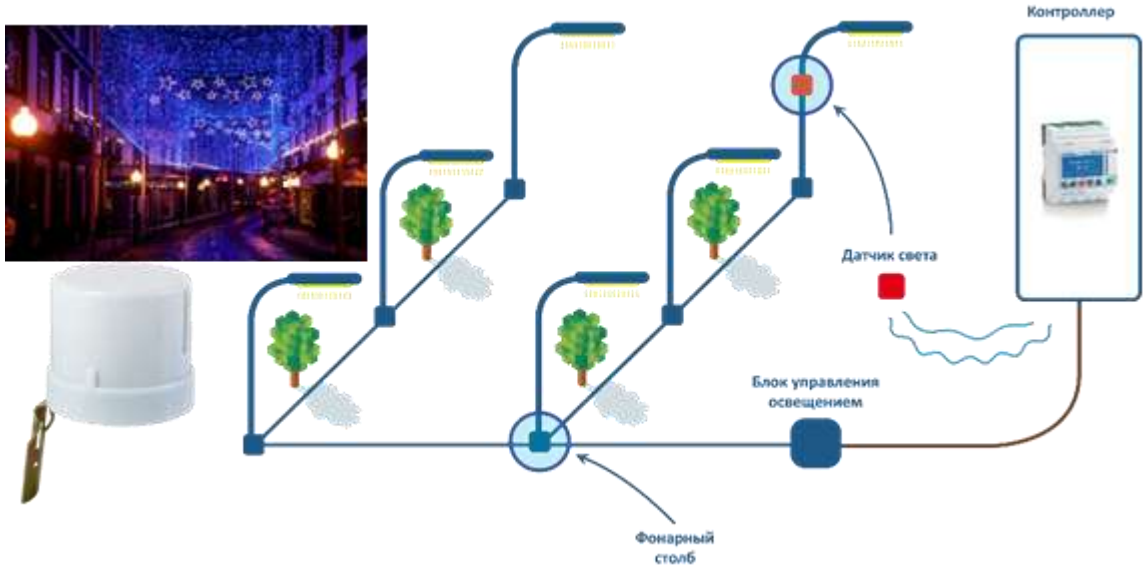

Рис. 2. – Схема автоматичного управління освітленням

3. Автоматизація роботи житлово-експлуатаційних підприємств та ОСББ.

Розроблена технологія «Розумний будинок» IT Lynx SmartHouse дозволяє автоматизувати зчитування показників лічильників газу, електроенергії, води тощо. Також технологія дозволяє виконувати моніторинг, фіксацію і сповіщення про різного роду несправності, помилки в роботі та багато іншого.

4. Автоматичне управління обладнанням в комерційних і житлових приміщеннях.

Технологія IT Lynx SmartHouse дозволяє здійснювати управління опаленням, теплими підлогами, світлом, охоронною сигналізацією та іншим побутовим обладнанням. Для цього використовується розроблений та

запрограмований контролер Lynx SmartController з відповідним програмним забезпеченням IT Lynx SmartHouse (рис. 3).

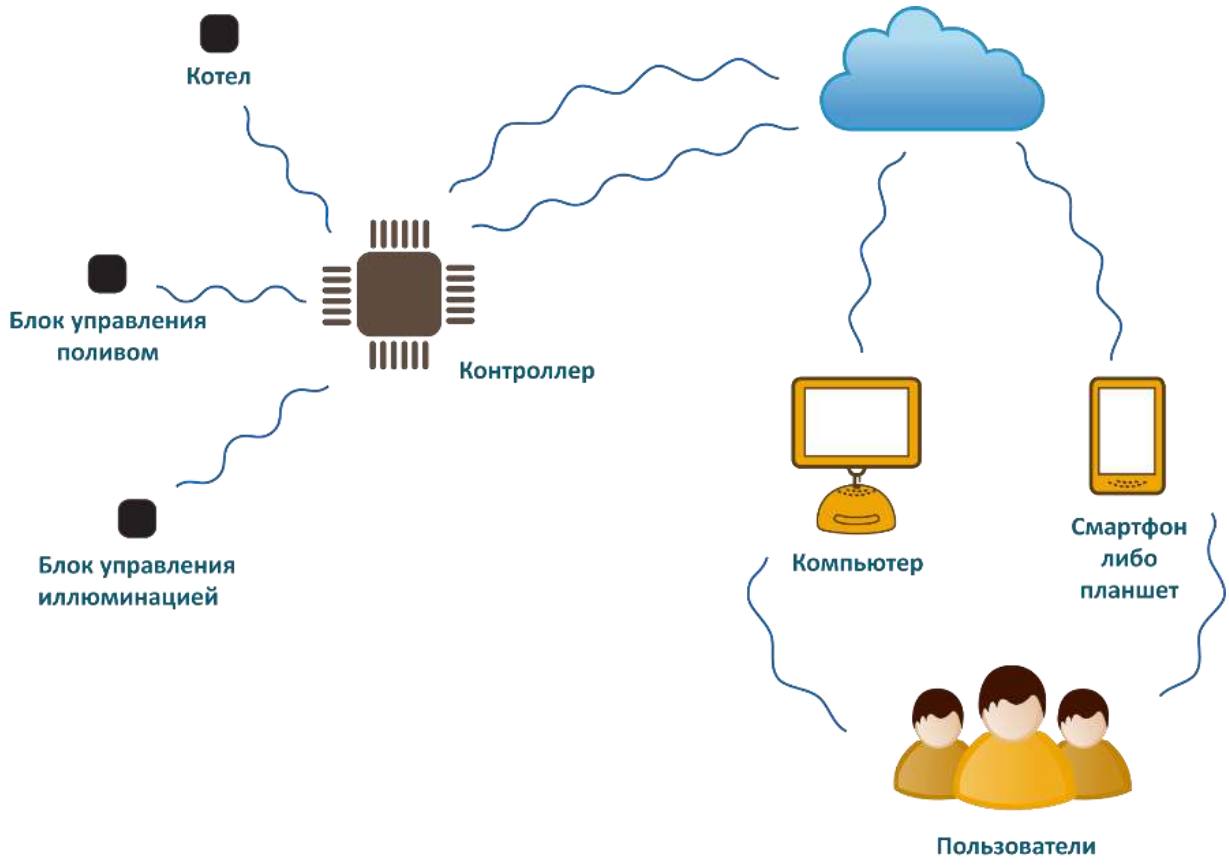

Рис. 3. – Елементи концепції «Розумного будинку»

Запропонована технологія IT Lynx SmartHouse забезпечує безпеку, ресурсозбереження та комфорт для всіх користувачів з можливістю віддаленого управління та моніторингу. Також технологія здатна розпізнавати виключні ситуації, що відбуваються в будівлі або у житловому комплексі, і відповідним чином на них реагувати: одна з систем може здійснювати управління поведінкою інших систем за заздалегідь виробленим алгоритмом. Крім того, від автоматизації декількох підсистем забезпечується синергетичний ефект для всього комплексу.

У випадку використання технології для житлових та комерційних приміщень забезпечується злагоджена робота системи опалення та кондиціонування, а також контроль факторів, що впливають на необхідність включення або відключення зазначених систем. Іншими словами, в

автоматичному режимі відповідно до зовнішніх і внутрішніх умов задаються та відслідковуються режими роботи всіх інженерних систем і електроприладів. У цьому випадку виключається необхідність користуватися кількома пультами при перегляді ТБ, десятками вимикачів при управлінні освітленням, окремими блоками при управлінні вентиляційними і опалювальними системами, а також системами відеоспостереження та охоронної сигналізації.

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

Чукут С. А.,
д.держ.упр., проф.,
професор кафедри теорії
та практики управління,
КПІ ім. Ігоря Сікорського

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ SMARTCITY НА ПРИКЛАДІ «SMARTDUBAI 2021»

Протягом наступних кількох десятиліть триваюча урбанізація та загальне зростання населення планети додасть містам понад 2,5 мільярдів людей [1]. Очікується, що всі регіони світу будуть урбанізовуватися далі, особливо в Азії та Африці, де розташовані найшвидше зростаючі міста.

Світ стає все більш взаємозалежним, і міста повинні діяти спільно через кордони для вирішення аналогічних проблем: зростання населення, зміна клімату, заторів і забруднення повітря, відсутність адекватного та доступного житла, освіти та охорони здоров'я, інтеграція біженців та мігрантів у міські життя, а також багатьох інших актуальних питань.

Також сприяють активним змінам в розвитку міст і зростання застосування ІКТ в усі сфери людського життя, зокрема це стосується розвитку Інтернет речей. Розумні пристрої допомагають поліпшувати якість життя, але й водночас загострюють проблеми, пов’язані з безпекою персональних даних, втручанням в приватне життя, цифровою нерівністю тощо.

Міста є найближчим рівнем влади у ставленні до своїх людей . Вони мають кращі можливості відстежувати і реагувати на реальні потреби свого населення та вирішувати глобальні проблеми. Проте міста сьогодні потребують фінансової підтримки для збільшення необхідної інфраструктури та базових послуг з метою забезпечення більшої соціальної справедливості та стабільності для всіх громадян. Існує нагальна потреба в розширенні можливостей міст.

Сучасною тенденцією є те, що місцеві дії мають значний глобальний вплив. У містах відбуваються соціальні інновації, які дозволяють кожному користуватися можливостями цифрової трансформації та технологічними досягненнями. Модель міської інновації, орієнтованої на забезпечення більш потужної цифрової економіки, можлива лише на основі співпраці між державними адміністраціями, компаніями, науковою і дослідницькою спільнотою та громадянами. Смарт технології є важливою складовою демократизації міста. Цифрові технології можуть працювати як інструмент для участі громадськості, прозорості та близькості громадян. Соціальне залучення починається з громадян знизу вгору - підхід необхідний для розширення можливостей людей. Саме з цією метою розробляються і впроваджуються різноманітні стратегії розумних міст.

Найяскравішим прикладом стратегії розумного міста є Стратегія «Смарт-Дубаї» [2]. Згідно цієї стратегії місто має перетворитися на модель «розумного міста», революціонізуючи, зокрема державні послуги, які надаються людям, запустивши понад 100 розумних ініціатив та понад 1000 розумних сервісів двома десятками державних департаментів та партнерами приватного сектора за період менш ніж за три роки. Стратегія Smart Dubai 2021 - це відповідь міста на сучасні виклики і зміни. Урядом Дубаї була розроблена амбіційна дорожня карта для підготовки міста до майбутнього, де визначено пріоритет людського щастя як найважливіший показник успіху. Згідно цієї стратегії, Дубаї має стати провідним світовим містом до 2021

року, відзначаючи золотий ювілей країни, сприяючи розвитку технологій, що приносять користь людям, завдяки зростанню економіки та ресурсів.

Смарт Дубаї – це місто, де всі його ресурси оптимізовані для максимальної ефективності, де послуги інтегровані в повсякденне життя, де захищені як самі мешканці, так й інформація, при цьому забезпечується найбільш збагачене повноцінне життя та обмін досвідом для всіх.

Smart Dubai 2021 - стратегічна дорожня карта для міста, метою якої є досягнення цілей цифрового перетворення до 2021 року. Дорожня карта визначає амбітні цілі у трьох напрямках впливу: щастя клієнта, економічне зростання та стійкість до ресурсів та інфраструктури. Вплив клієнта полягає в тому, що служби міста стануть більш ефективними та бездоганними, заощаджуватимуть час та гроші, використовуючи кращий досвід. Фінансовий вплив проявляється в тому, що ефективні міські служби дозволять заощаджувати витрати у всіх галузях промисловості, тоді як розуміння інновацій та керування даними стимулюватимуть економічне зростання. Вплив ресурсів та інфраструктури сприятиме підтримці чистого та здорового навколишнього середовища. Таким чином, Програма визначає загальноміський підхід до досягнення чотирьох цілей Smart Dubai: для ефективного, безперервного, безпечного та персоналізованого міста шляхом надання послуг та ініціатив по 6 стратегічних напрямах, які сприятимуть покращенню послуг та досвіду в масштабах усього міста, а саме:

1) розумне життя; 2) розумна економіка; 3) розумне управління;4) розумна мобільність; 5) розумне оточення; розумні люди.

Досягнення цих стратегічних завдань сприятиме трансформації способу життя громадян, роботи та взаємодії з містом.

Досвід «Смарт Дубаї 2012» може стати в нагоді в Україні, особливо з метою змінити підхід до формування та реалізації стратегії розумного міста. Не компанії-розробники, а громадяни та їх потреби мають бути орієнтиром на шляху реалізації цих стратегій, враховуючи специфіку кожного міста, його проблеми та переваги.

Література:

1. Smart City Expo World Congress 2017. Empower Cities. Empower People. . -Режимдоступу: http://www.smartcityexpo.com
2. Smart Dubai 2021. -Режим доступу: https://2021.smartdubai.ae/

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

Дмитренко В. І.,
здобувач кафедри теорії
та практики управління
КПІ ім. Ігоря Сікорського

РОЗВИТОК SMARTCITY: ДОСВІД ФІНЛЯНДІЇ

Сучасною тенденцією впровадження електронного урядування на місцевому рівні є розробка та реалізація різноманітних стратегій смарт-сіті або розумних міст. Розумне місто - це місто, в якому використовуються сучасні технології для покращення якості життя, вирішення екологічних проблем, удосконалення надання послуг для громадян і бізнесу. Новітні технології використовуються, щоб підвищити якість надання послуг, зменшити вартість та споживання ресурсів та поліпшити комунікацію і порозуміння між мешканцями.

Цікавим є досвід Фінляндії щодо розвитку смарт міст. Зокрема, заслуговує на увагу, розроблена на 2014-2020 роки стратегія «Відкриті та розумні послуги – Six City» [1], до якої залучені найбільші міста - муніципалітети Фінляндії: Гельсінкі, Еспоо, Вантаа, Тампере, Турку і Оулу, де проживає близько 30% населення.

Основна мета Стратегії Six City - зміцнення конкурентоспроможності Фінляндії за допомогою шести найбільших міст країни, як осередків інноваційного розвитку, тестування інновацій, а також підвищення продуктивності.

Стратегія має три основних напрямки:

1. відкриті інноваційні платформи; 2. відкриті дані та інтерфейси;
3. відкрита участь в управлінні.

Інноваційні платформи використовуються для створення і тестування нових послуг і продуктів в реальних умовах. Водночас, відкриті дані, доступ до яких забезпечують міста, покладено в основу для розробки нових послуг і операцій. Третій напрямок передбачає залучення всієї громади міст до проектування та розробки інноваційної комунальної служби та обслуговування клієнтів. На додаток до цього, відкрита участь в управлінні сприятиме зайнятості та участі людей з низькими перспективами працевлаштування.

Слід відзначити, що фінансування проектів Six City передбачається в розмірі майже 80 мільйонів євро за рахунок Європейського фонду регіонального розвитку (ERDF). Окрім цього, проекти будуть фінансуватися з Європейського соціального фонду (ESF), а також за фінансової підтримки муніципалітетів та Міністерства зайнятості та економіки Фінляндії.

Активну підтримку здійснює платформа ІТ-підтримки європейських міст «Код для Європи» [2]. У 2015 році «Код для Європи» включав в себе 14 організацій-партнерів з шести країн: Фінляндія, Нідерланди, Німеччина, Іспанія, Італія та Великобританія. Програма фінансується за кошти Європейської Комісії. «Код для Європи» набирає талановитих веб-розробників, дизайнерів, кодерів для тимчасової роботи в організаціях державного сектора, для розробки конкретних рішень і передових технологій з відкритим вихідним кодом, щоб зробити уряд більш відкритим та ефективним, щоб принести користь громадянам. Окрім того, створено форум Virium Гельсінкі, який відповідає за національну координацію Six City, а також за активацію мережевих і комунікаційних завдань [3].

Прикладом ефективного впровадження технологій електронного урядування, зокрема розвитку смарт технологій – є Каласатама (новий район Гельсінкі), який став експериментальним майданчиком для інновацій у побудові смарт-інфраструктури і міських послуг (http://fiksukalasatama.fi/). Смарт Каласатама має концепцію побудови ресурсозберігаючого району, в якому жителі отримують додаткову годину вільного часу кожен день.

Платформа охоплює велику різноманітність різних галузей промисловості й рішень, починаючи від інтелектуальних мереж в сфері електронної охорони здоров'я і смарт-роздрібної торгівлі.

Житлова Лабораторія Каласатама є відкритою інноваційною платформою, що пропонує можливість спільного створення нових міських служб в реальних умовах для людей, які живуть в цьому районі. До початку 2030-х років, Каласатама планує забезпечити житлом приблизно 20000 мешканців та робочими місцями 8000 чоловік. Наразі в районі проживає 2 000 чоловік. Також Kalasatama запрошує всіх до клубу інноваторів [4]. Клуб інноваторів зустрічається чотири рази на рік, щоб зробити район ще розумнішим. Завдяки клубу, всі зацікавлені сторони зможуть регулярно обмінюватися новинами та отримати інформацію про майбутні події і майбутні зміни. Іншим завданням клубу є організація співпраці. Саме функціонуюча мережа співпраці забезпечує природний шлях для впровадження нових експериментів, які б покращили якість життя громадян.

Література:

1. Six City Strategy (6Aika). -Режимдоступу: http://6aika.fi/
2. Code for Europe. - Режимдоступу: http://codeforeurope.net/cities/helsinki/
3. The cooperation strategy of the six largest cities in Finland. - Режимдоступу: http: //forumvirium.fi/en/the-six-cities-strategy
4. Innovators club. - Режимдоступу: http://fiksukalasatama.fi/en/building-blocks/innovators-club/

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

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

ЗАГРОЗИ БЕЗПЕЦІ У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ: ПРОБЛЕМИ, ВИКЛИКИ ТА ДЕРЖАВНИЙ ВПЛИВ

Оскільки сама технологія, на основі якої виник Інтернет речей, передбачає можливість підключення до мереж різноманітних речей матеріального світу, а не тільки електронно-обчислювальних машин

різноманітної конфігурації, питання забезпечення безпеки (у широкому розумінні) у цій сфері набуває надзвичайної ваги.

Основні фактори небезпеки були визначені свого часу фахівцями з забезпечення національної безпеки і зводяться до наступного.

У мережі Інтернет перебувають різноманітні пристрої, значна частина яких зумовлює взаємодію на рівні «машина-машина» (*M2M*), хоча окремі з таких пристроїв і перебувають під контролем людини [1, p.68]. Зазначене зумовлює уразливість інформації, що перебуває у пристроях, які знаходяться у мережі Інтернет і пов'язані між собою. Цей стан речей викликаний тією обставиною, що спочатку взаємодія між приладами відбувалась у їх власних мережах, і лише потім розробники приладів звернулись до можливостей відкритих мереж. При цьому подальша розробка таких пристроїв відбувалася практично без уваги до необхідності забезпечення безпеки інформації. Наприклад, загроза пристроям Інтернету речей, що відома під назвою «Диявольський плющ» (*Devil's Ivy Problem*) не є наслідком дій зловмисників, а викликана недоліками в архітектурі побудови зберігачів інформації [2]. Загрози такого типу є суто технічними і викликають збої у роботі пристроїв або впливають на їх працездатність.

Іншим типом загроз є загрози втрати контролю над пристроями внаслідок збоїв управління на рівні M2M, на рівні конкретного пристрою або ж як прояв цілеспрямованих деструктивних дій. У цьому плані пристрої, що перебувають в мережі Інтернет, є мішенню для деструктивних дій. У засобах масової інформації наводяться досить численні факти хакерських дій в мережах GSM (*GSM sniffing*), перехоплення в GPRS та втручання через Bluetooth, Wi-Fi або інфрачервоні порти з різною метою. У такому разі пристрої або захоплюються під управління іншим суб'єктом, або виходять з-під контролю оператора. Унаслідок різноманітності пристроїв Інтернету речей зазначена небезпека є досить серйозною. Особливо якщо мова йде про медичні пристрої [3], безпілотні літальні апарати, транспортні засоби та об'єкти критичної інфраструктури [4].

Проблема збереження інформації на ранній стадії розвитку пристроїв Інтернету речей особливо не турбувала розробників, оскільки вважалось, що вони передають лише технічну інформацію. Але у подальшому, при зміні підходів до правових проблем «великих даних» та необхідності збереження персональних даних в Інтернеті, було звернуто увагу і на цю проблему для безпеки в епоху Інтернету речей [5].

Занепокоєння небезпекою розповсюдження зазначених загроз зумовило досить гостру реакцію у деяких країнах.

Зокрема, у своїй доповіді від 25.02.2016 для Комітету Конгресу США з питань розвідки директор Національної розвідки Дж. Клепер зазначив, що проблема забезпечення безпеки у сфері Інтернету речей належить до глобальних загроз, оскільки такі прилади розроблялися з мінімальними вимогами до безпеки, і тому їх розповсюдженість насамперед у діяльності державних органів та установ становить небезпеку.

Реагування на такі загрози уповноваженими державними органами США відбувалося відповідно до компетенції шляхом підготовки рекомендацій або інших актів реагування.

Зокрема, Міністерство внутрішньої безпеки США *(DNS)* визначило низку стратегічних принципів у забезпеченні безпеки в сфері Інтернету речей. Зазначені принципи повинні бути розповсюджені на діяльність розробників та виробників приладів, постачальників послуг, а також державних і комерційних споживачів. Система зазначених стратегічних принципів зумовлена необхідністю належного державного реагування на загрози, що виникають у сфері Інтернету речей, і визначена наступним чином:

- упровадження вимог безпеки на етапі розробки приладу;
- забезпечення своєчасного оновлення засобів безпеки та управління вразливістю;
- слідування визнаним практикам у сфері забезпечення безпеки;

- надання пріоритету вимогам безпеки відповідно до потенційного впливу;
- забезпечення поінформованості стосовно приладів у сфері Інтернету речей;
- обережне та обдумане під’єднання до мережі [6].

Під час впровадження зазначених стратегічних принципів потрібно уникати директивного державного впливу на бізнес-кола, а лише рекомендувати кращі практики забезпечення безпеки, які відомі на сьогодні, окрім сфер державного регулювання (телекомунікації, платіжні системи тощо).

Міністерство оборони США *(DOD*) розробило для службовців рекомендації, що визначають як загальні вимоги до використання приладів у сфері Інтернету речей в установах, організаціях, військових частинах, так і конкретні заходи безпеки для користувачів [7].

Пропозиції стосовно регулювання безпеки у сфері Інтернету речей у США знайшли своє відображення у законопроекті сенаторів М. Уарнера, К. Гарднера, Д. Фішера і Р. Уайдена – «Акт щодо впровадження кібербезпеки стосовно Інтернету речей» 2017 року. Проте зазначений законопроект викликав досить серйозну критику з боку захисників громадянських свобод та фахівців у сфері інформаційних технологій. Найбільш неоднозначними є такі пропозиції: запровадження ведення державними органами обліку приладів, що можуть під’єднуватися до мережі Інтернет; регламентація порядку продажу таких пристроїв у роздрібній мережі; обмеження придбання таких приладів державними установами.

Загрози у сфері Інтернету речей є предметом уваги Європейського агентства з мережевої та інформаційної безпеки (ENISA) та Європейської групи кібербезпеки. Зокрема, у доповіді для Європейської наради з питань кібербезпеки 2016 року зазначено, що значне розповсюдження Інтернету речей буде знижувати рівень безпеки попри застосування належних методів захисту та людський фактор, який негативно впливає на стан безпеки [8].

Слід зазначити, що напрями державної політики визначені в ЄС менш детально, аніж у США, і ще не стали значним трендом для державних органів або міждержавних агентств.

Разом із цим, заходи реагування передбачають інформування користувачів приладів Інтернету речей, обмін інформацією між державними органами та впровадження кращих практик. Слід також зазначити, що фахівці з кібербезпеки визначають за необхідне унормування відповідних технічних стандартів у цій сфері шляхом відкритої сертифікації [9], хоча відкрита сертифікація не є обов'язковою і не вирішує багатьох організаційних і правових проблем.

Ефективність державного реагування на загрози в Україні можна охарактеризувати як досить низьку, попри зафіксований різними спеціалістами стан небезпеки у сфері Інтернету речей.

Зокрема, документи стратегічного планування з питань забезпечення кібербезпеки, що ухвалені останнім часом в Україні, оминають проблематику забезпечення безпеки у сфері Інтернету речей, хоча деякі із визначених заходів державної політики мимохідь торкаються і проблематики Інтернету речей.

Таким чином, зазначене дозволяє прийти до таких висновків.

По-перше, з урахуванням кращих світових практик та відповідних звітів фахівців з питань кібербезпеки, необхідно узагальнити наявні загрози безпеці у сфері Інтернету речей та відпрацювати прогнозовані показники. З урахуванням існуючої в державі моделі забезпечення кібербезпеки,
зазначене скоріш за все належить до компетенції Національного координаційного центру з питань кібербезпеки.

По-друге, вітчизняні законодавчі та нормативно-правові новації у цій сфері мають ґрунтуватись на відповідних рекомендаціях, що мають бути підготовлені фахівцями (аналогічно до рекомендацій державних органів США) і повинні враховувати кращі зразки світової практики.

По-третє, слід підтримати пропозиції щодо стандартизації у сфері Інтернету речей на міждержавному рівні, попри існуючі складнощі, насамперед щодо участі у таких заходах КНР та деяких інших країн - активних виробників приладів Інтернету речей.

Література:

1. Abomhara Mohamed. Cyber Security and the Internet Of Things: Vulnerabilities, Threats, Intruders and Attacks/Mohamed Abomhara, Geir Koien// Journal Of Cyber Security. – 2015 - Vol. 4. – P. 65-88.

2. Experts in Lather Over ‘gSOAP’ Security Flaw. Published 17.07.2017/ Режим доступу: https://krebsonsecurity.com/2017/07/experts-in-lather-over-gsoap-security-flaw/ – Назва з екрана. Дата звернення : 20.09.2017 р.

3 . Medical Devices and the Internet of Things: Defending against cyber threats/ Режим доступу: https://www.helpnetsecurity.com/2017/08/16/medical-devices-iot/ – Назва з екрана. Дата звернення : 20.09.2017 р.

4. Simon Tobby. Critical Infrastructure and the Internet Of Things/ Tobby Simon// Global Commission on Internet Governance. – 2017. – No 46/ Режим доступу: https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf Назва з екрана. Дата звернення : 20.09.2017 р.

5. Ziegeldorf Jan Henrick. Privacy In The Internet of Things: Threats and Challenges/ Jan Henrick Ziegeldorf, Oscar Garcia Morchon, Klaus Wehrle //Режим доступу: https://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-ziegeldorf-scn-privacy-in-the-iot.pdf Назва з екрана. Дата звернення : 20.09.2017 р.

6. US Department of Homeland Security. Strategic Principles for Securing the Internet Of Things. Version 1.0. November, 15.2016. – 22 p.

7. US Department of Defence. Policy Recommendations for The Internet of Things (IoT). December 2016. – 24 p.

8. European Foresight Cyber Security Meeting 2016 //Режим доступу: https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf Назва з екрана. Дата звернення: 20.09.2017 р.

9. Spiegelmock M. IoT Security Through Open Certification/Misha Spiegelmock// Режим доступу: https://spiegelmock.com/2017/08/14/iot-security-through-open-certification/ Назва з екрана. Дата звернення: 20.09.2017 р.

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

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

ПРАВОВІ ПРОБЛЕМИ КІБЕРЗАХИСТУ НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

Високі темпи віртуалізації сучасного соціуму зумовлюють необхідність адекватної реакції держави на ці процеси за допомогою притаманних їй засобів. Поряд із безсумнівними перевагами, які виникають внаслідок інсталяції віртуальної реальності у суспільні процеси, з'являються певні проблеми, особливе значення серед яких має правове регулювання кібербезпеки. Виходячи із транскордонної природи цього явища, створення високоефективної національної нормативної бази в цій сфері можливе тільки за умови узгодженої міжнародної політики, вироблення єдиних принципів і стандартів в сфері правового регулювання кіберпростору.

На сьогодні теоретичні та практичні аспекти безпеки кіберпростору знаходяться в центрі уваги міжнародних організацій та державних органів, наукових установ та громадських організацій, суб'єктів підприємницької діяльності та приватних осіб. Проводиться значна нормотворча, управлінська, аналітична та просвітницька робота в цій сфері суспільних відносин. В той же час, розробка та реалізація міжнародних норм в кіберпросторі пов'язана із значними складнощами. Національне законодавство в цій сфері формується повільно і є недосконалим, що створює відповідні труднощі і для розвитку міжнародного права [1, с. 356]. При цьому, дослідниками підкреслюється недостатність суспільних знань в цій галузі та необхідність нормативного закріплення партнерства всіх соціальних суб'єктів з метою, зокрема, боротьби із кіберзлочинністю [2, с. 356].

У зв’язку з цим актуалізується теоретичний аналіз проблем правового регулювання процесів кіберзахисту окремих об’єктів, зокрема, критичної інфраструктури, що і є метою даної статті.

Вперше в політико-правовому лексиконі поняття «критичні інфраструктури» було застосовано в 1997 році в доповіді Президенту США під назвою «Критичні основи захисту інфраструктури Америки», яку підготували члени спеціальної комісії. У доповіді, зокрема, зазначалося, що національна оборона, економічне процвітання та якість життя залежать від складових критичної інфраструктури, яка функціонує на основі технологій інформаційної ери. Швидке розповсюдження та інтеграція телекомунікаційних та комп'ютерних систем, об'єднаних між собою в складну інфраструктуру, створюють новий вимір вразливості та ризиків, які є безпрецедентними за своєю сутністю [3]. Водночас, у США до складових критичної інфраструктури було віднесено вісім позицій: телекомунікації, електроенергетичні системи, природний газ і нафта, банківська справа, і фінанси, транспорт, системи водопостачання, урядові послуги та служби екстреної допомоги [4].

У Європейському Союзі створення правових та організаційних механізмів захисту критичної інфраструктури було ініційовано в 2004 р. у зверненні Європейської Ради до Європейської Комісії, в якому ЄК доручалося підготувати загальну стратегію захисту. В жовтні 2004 р. ЄК оприлюднила офіційне повідомлення, в якому містився як огляд дій ЄК в цій сфері, так і пропозиції щодо додаткових заходів задля вдосконалення європейської системи запобігання, готовності та реагування на терористичні атаки, спрямовані проти елементів критичної інфраструктури [5].

10 березня 2004 року Європейським Парламентом та Радою було створено Європейську агенцію мереж та інформаційної безпеки як консультативний орган, покликаний сприяти розробці національних стратегій кіберзахисту, здійснювати дослідження проблем безпеки кіберпростору, реалізовувати політику та законодавство Європейського Союзу з питань, що стосуються інформаційних систем [6]. В документах цієї організації зазначається, що

першим кроком у процесі забезпечення та захисту критичних активів є визначення поняття критичної інформаційної інфраструктури.

Згідно з Європейською Директивою 2008/114/ЕС «Про ідентифікацію та визначення європейських критичних інфраструктур та про оцінку необхідності вдосконалення їх захисту», критична інфраструктура означає актив, систему чи її частину, розташовану в державах-членах, яка є важливою для забезпечення життєво важливих суспільних функцій, охорони здоров'я, безпеки економічного та соціального благополуччя людей, а порушення чи руйнування яких матимуть значний вплив на державу-учасницю внаслідок нездатності зберегти їх функції [7].

Аналіз застосування цієї конвенції в країнах – членах ЄС свідчить про різний рівень уваги національних інституцій до цієї проблеми і дозволяє виділити чотири типи держав щодо захисту критичної інфраструктури:

1. Держави, які фактично не вживають заходів щодо захисту інфраструктури і визначили тільки два вразливих сектори: транспортний та енергетичний.

2. Держави, які визнали в якості найважливішого сектора критичної інфраструктури інформаційно-комунікаційні технології і здійснюють їх захист.

3. Держави, що розробили загальну методологічну базу для ідентифікації активів критичної інфраструктури та визначили їх захист як пріоритетний для функціонування життєво важливих суспільних інституцій.

4. Держави, що запровадили чіткі критерії для ідентифікації активів критичної інфраструктури і встановили високий рівень їх захисту [8].

Аналіз чинного законодавства дає підстави стверджувати, що в запропонованій класифікації Україна належить до держав першого типу з невисоким рівнем захисту критичної інфраструктури. В Україні на сьогодні відбуваються процеси теоретичного обґрунтування необхідності захисту критичної інфраструктури та спроби нормативного врегулювання відносин в цій сфері. Так науковцями в якості об’єктів критичної інформаційної

інфраструктури України пропонується розглядати інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, припинення або порушення функціонування яких може призвести до людських жертв, завдання шкоди здоров'ю людей або довкіллю, порушення умов життєдіяльності людей, порушення виробничих або транспортних процесів, значних матеріальних збитків, неспроможності держави виконувати свої функції [9].

Водночас, аналітики звертають увагу на відсутність терміну «критична інфраструктура» в законодавстві України, а також чіткого переліку об'єктів, які віднесені до такої категорії, що заважає ефективно виконувати завдання з забезпечення національної безпеки [10]. В Стратегії кібербезпеки України зазначається необхідність забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура). Таке формулювання відзначається високим рівнем загальності і неможливістю ідентифікації елементів критичної інфраструктури. Не усуває цю проблему і можливе прийняття Закону «Про основні засади забезпечення кібербезпеки України», який винесено на повторне друге читання і включено в порядок денний сьомої сесії Верховної Ради України восьмого скликання, що передбачено Постановою Верховної Ради України від 3 жовтня 2017 року № 2149–VIII. В проекті цього закону об'єкт критичної інформаційної інфраструктури розуміється як інформаційна (автоматизована), телекомунікаційна, інформаційно-телекомунікаційна система, порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України.

Виходячи з того, що об'єкти критичної інформаційної інфраструктури піддаються різноманітним загрозам, кібератаки серед яких є найбільш поширеними, але не виключним видом, доцільним є прийняття

системоутворюючого закону «Про захист критичної інфраструктури України». Ключову роль у цьому нормативно-правовому акті слід відвести регулюванню питань кіберзахисту.

Враховуючи, що значна частина об'єктів критичної інфраструктури знаходиться у приватній власності, необхідно передбачити механізми державного впливу та співпрацю з приватним сектором, що може бути предметом подальших досліджень в цьому напрямку.

Література:

1. Eichensehr K. Cyberwar & International Law Step Zero. Texas international law journal, Volume: 50, Symposium, Issue: 2, 2015. – Режим доступу: http://www.tilj.org/content/journal/50/PROOF.pdf с. 355 – 378.
2. Bossong R., Wagner B. A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union. Режим доступу: https:// europa.eu/rapid/press-release_SPEECH-03-185_en.pdf
3. Critical Foundations Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. October 1997. – Режим доступу: https://fas.org/sgp/library/pccip.pdf
4. Rinaldi, S. M., Peerenboom, J. P., Kelly, T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems, Volume: 21, Issue: 6, December 2001. – Режим доступу : http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf
5. Скалецький Ю. М. Європейський досвід розбудови системи захисту критичної інфраструктури: уроки для України. Аналітична записка [Електронний ресурс] / Ю. М. Скалецький, Д. С. Бірюков, С. І. Кондратов // Національний інститут стратегічних досліджень – Режим доступу: http://www.niss.gov.ua/articles/1371/.
6. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. – Режим доступу: http://data.europa.eu/eli/reg/2004/460/oj
7. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). Official Journal of the European Union. L 345. 23 December 2008. – Режим доступу: https://publications.europa.eu.
8. Methodologies for the identification of Critical Information Infrastructure assets and services. Guidelines for charting electronic data communication network. – Режим доступу: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis.
9. Шеломенцев В. П. Основні напрями і суб'єкти забезпечення кібернетичної безпеки України / В. П. Шеломенцев // Боротьба з

організованою злочинністю і корупцією (теорія і практика). − 2013. − № 1. − С. 348 - 355.

10. Бірюков Д. С. "Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні". Аналітична записка [Електронний ресурс] / Д. С. Бірюков // Національний інститут стратегічних досліджень – Режим доступу: http://www.niss.gov.ua/articles/1477/.

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

Ткачук Т. Ю.,
к. ю. н., доцент, заступник завідувача кафедри Навчально-наукового інституту інформаційної безпеки ГА СБ України.

ТІНЬОВИЙ ІНТЕРНЕТ: СПІВВІДНОШЕННЯ МОЖЛИВОСТЕЙ І ЗАГРОЗ

Мало хто знає, що тільки 15-20% Інтернету доступні. Інша частина таємна і називається глибинним Інтернетом. Сучасні технології дозволили створити Мережу задля дотримання абсолютної анонімності користувача в обхід стеження серверів провайдерів. Така мережа називається Deep Web – тіньова мережа. Специфіка роботи Deep Web - беззастережна анонімність, абсолютна незалежність від сервера провайдера, що виключає можливість визначити, якою інформацією обмінюються користувачі. Такий таємний обмін називається цибулева маршрутизація (Tor). Tor, як технологія, що дозволяє користувачам зберігати свою анонімність в Інтернеті, використовується при відвідуванні сайтів, веденні блогів, відправленні повідомлень тощо.

На території тіньового Інтернету знаходяться комерційні веб-сайти, де торгують зброєю, наркотиками, фальшивими документами. Тут безмежні «полігони» для підготовки проведення державних переворотів і вирішення різного роду військових питань. Такий невидимий Інтернет налічує більше 8000 терабайт інформації (600 мільярдів окремих документів), це величезний обсяг у порівнянні з 20 млрд. «поверхневого» Інтернету.

Tor, як зазначають його розробники, – це безпечний простір для політичних активістів, журналістів та інших людей, за якими потенційно можуть стежити. В його основі лежить принцип – не приховувати, а захищати. Адже особисті дані користувача і те, що він робить в мережі, – це не секрет, це просто не для очей сторонніх [1].

З вище висловленого можна зробити висновок, що в Tor існує тотальний анонімний вандалізм серед користувачів. Проте, як запевняють самі розробники технології, в Tor захищають «хороших» людей від «поганих», з тим же успіхом захищають «поганих» людей від «хороших». Ані розробники Tor, ані державні органи не можуть відстежити фізичне місце розташування користувача цієї мережі так само як і заблокувати їх контент.

Однак, не всі сайти темної павутини користуються цим методом. Деякі використовують схожі сервіси, такі як, наприклад, I2P, але принцип дії залишається таким же: користувач повинен використовувати такий же інструмент шифрування, як і сайт, і, що дуже важливо, знати, де знайти сайт, щоб відвідати його за допомогою введення конкретного URL. Одним з найбільш відомих прикладів сайту темної павутини залишається сайт Silk Road («*Шовковий шлях*»)[5]. Silk Road довгий час був анонімним торговельним майданчиком для купівлі-продажу наркотиків.

У той же час існують легальні випадки використання темної павутини: люди, що живуть в закритих, тоталітарних суспільствах можуть використовувати темну павутину для того, щоб спілкуватися із зовнішнім світом, виключаючи стеження спецслужб за собою.

---

[5] **Silk Road** (з англ. *шовковий шлях*) — анонімний Інтернет-магазин який перебував у доменній зоні .onion анонімної мережі Tor. Більшість товарів, виставлених на сайті, були наркотичними речовинами. Веб-сайт був запущений у лютому 2011 року, а робота над його створенням почалася 6 місяців до того. Спочатку, на веб-сайті була обмежена кількість доступних аккаунтів продавця, такі аккаунти продавались через аукціон. Пізніше обмеження було зняте, фіксована плата стягувалася за кожний новий аккаунт продавця. Станом на березень 2013 року, в онлайн-магазині було розміщено близько 10 тис. товарів для продажу, 70% з яких були наркотиками. Того ж року ФБР заблокувало веб-сайт, та заарештувало власника ресурсу, відомого під псевдонімом англ. *Dread Pirate Roberts*, ним виявився Росс Вільям Ульбрихт (*Ross William Ulbricht*).

Спеціалісти виокремлюють ряд загроз, які містять такі технології [2]:

1. За вами можуть стежити. На форумах часто радять заклеювати камеру і мікрофон ноутбука для того, щоб не стати об'єктом стеження.

2. Користуючись Tor, Ви можете мимоволі стати співучасником масштабних злочинів і діяльності хакерів через те, що ваш ПК стає частиною мережі, що використовується іншими користувачами.

3. Тор розроблявся військовими й спецслужбами, що не виключає його використання у своїх цілях, не дивлячись на розкручений бренд про 100% безпеку і анонімність використання.

4. Створює незручність при користуванні «білими» сервісами, наприклад, поштою. Суть у тому, що при роботі з Tor у вас постійно змінюється IP-адреса, що призводить до відімкнення сервісів, які сприймають це як спробу зовнішнього злому.

5. Google часто блокує пошукові запити через Tor, оскільки вважає, що це хакерська активність. Ці два сервіси не створені один для одного.

Раніше, коли листи були паперовими, а покупки здійснювалися в фізичних магазинах за готівку, ви могли контролювати свою приватну інформацію. Але сьогодні все відбувається онлайн, і навіть у себе вдома, з появою Інтернету, ви втрачаєте цей контроль. Ваші дані миттєво відлітають в мережу і ви більше не відповідаєте за те, куди вони потрапляють потім і як використовуються.

Мало хто усвідомлює, що коли він або вона відкриває веб-сторінку, то комунікує не тільки безпосередньо з веб-сервером. Коли ви відкриваєте веб-сторінку, ваш браузер відправляє десятки, сотні і тисячі запитів на найрізноманітніші сервери – для зняття статистики, для показу реклами тощо. Тобто, кожен з нас сьогодні знаходиться під наглядом з боку різних організацій, які хочуть отримувати дані про користувачів, виділяти якісь тренди, а потім монетизувати їх.

Важливо розуміти, що, коли ви даєте якійсь компанії доступ до ваших даних, ви також даєте цей доступ всім її співробітникам. Але ви не можете

знати, хто ці люди, і наскільки їхні помисли чисті. І, на жаль, ви мало що можете з цим вдіяти. Але є ще небезпечніші особи, які також мають доступ до наших даних, – це кіберзлочинці.

Використання Tor розширює список доступних можливостей Інтернету. Ця мережа має власні веб-сайти, на які звичайним браузером не потрапиш. Визначити такі можна на око: замість «www» вони починаються з «.onion». Такі веб-ресурси часто називають «темним інтернетом» і експерти припускають, що там міститься приблизно 300 тис. сайтів, з яких 16 тис. знаходяться в Інтернеті. Наприклад, серед них є «Темна Вікіпедія» [3].

Як можна бачити із цього короткого аналізу, темна частина Інтернету має як свої переваги, так і ряд досить принципово важливих загроз. Розуміння цього факту дає змогу як попередити ці загрози, так і навчитися ними керувати.

Література:

1. Сандвик Р. О «темной стороне интернета» / Ранда Сандвик [Електронний ресурс]. – Режим доступу: https://lenta.ru/articles/2014/06/27/tor/
2. Темна павутина: все, що необхідно знати про приховану Мережу/ Zillya від 20.11.2015 р. // [Електронний ресурс]. – Режим доступу: http://zillya.ua/temna-pavutina-vse-shcho-neobkhidno-znati-pro-prikhovanu-merezhu
3. TOR и его аналоги для обеспечения приватности в интернет / Cryptoworld // [Електронний ресурс]. – Режим доступу: https://cryptoworld.su/tor-i-ego-analogi-dlya-obespecheniya-privatnosti-v-internet/

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

Огородников Д. В.,
Студент магістратури
ФІОТ КПІ ім. Ігоря Сікорського

МЕТОДИ ЗОВНІШНЬОГО ВТРУЧАННЯ У ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ ІНТЕРНЕТ РЕЧЕЙ

Основною концепцією Інтернету речей є взаємодія фізичних об’єктів, приладів та пристроїв. Пристрої мають вбудовані датчики і програмне забезпечення, які дають змогу здійснювати обмін даними між приладом та комп’ютерною системою за допомогою стандартних протоколів зв’язку.

Прикладами підключення усіляких можливих пристроїв в загальну функціонуючу систему, яку людина може використовувати у повсякденному житті, є: датчики погоди, датчики руху, пожежні сигналізації, холодильники, кондиціонери, електронні перепустки, годинники, браслети, тощо. Усі ці прилади входять до єдиної системи; за допомогою різноманітних чипів, модулів та антен вони отримують інформацію з датчиків і відслідковують їх стан. Зацікавленість третіх осіб у доступі до цих датчиків для своїх цілей є очевидною проблемою даних приладів.

Найпримітивніша система Інтернету речей складається з датчику, який включає в себе апаратну частину, своє програмне забезпечення, технологію передачі даних між приладом і системою, та саму систему, котра отримує дані. Отримання й обмін інформацією здійснюється двома методами:

- Системою ідентифікації;
- Технологією передачі даних між датчиком і системою.

Система Ідентифікації.

Для ідентифікації кожного підключеного у мережу об’єкту потрібна проста і компактна технологія. Процедура ідентифікації виконується з використанням мікросхем, RFID (Radio frequency identification), QR-кодів, та GPS [1], [2].

Типи атак, які виконуються у технології RFID.

Радіочастотне розпізнавання здійснюється за допомогою закріплення за об'єктом спеціальних міток, що несуть ідентифікаційну та іншу інформацію. Цей метод вже став основою побудови сучасних безконтактних інформаційних систем і має стійку назву RFID-технології [3].

1. Dos-атака. RFID першого покоління схильні до Dos-атаки. Чипи цього покоління використовують діапазон 902-938 МГц, який розділений на канали. Сканер може перемикатися з одного каналу на інший, а чип, в силу своєї пасивності, не може змінити діапазон. Стверджується, що даний діапазон можна заглушити з відстані в 1 м. за допомогою нескладного радіопередавача.

2. RFID Zapper. RFID Zapper (RFID-стирач) – електронний пристрій, який може перманентно відключити пасивний RFID чип. На відміну від інших методів відключення, він не пошкоджує пристрій, до якого підключений.

3. Клонування. Джонатан Вестхьюз (Jonathan Westhues) – студент, який створив пристрій, що дозволяє клонувати мітки. Девайс – названий proxmark – легко вміщувався в кишеню і при досить близькій відстані міг непомітно клонувати мітку.

4. Підміна вмісту пам'яті RFID-міток. Німецький експерт інформаційної безпеки Лукас Грюнвальд (Lukas Grunwald) продемонстрував, як вміст електронного паспорта може бути легко перенесено на будь-яку іншу радіо позначку, використовуючи додаток RFDump. Першою версією додатку був простий perl-скрипт. Для його роботи потрібен RFID-рідер: ACG Multi-Tag Reader або йому подібний. Версія додатку у наш час інсує тільки на Linux платформі.

5. Атаки через RFID-мітки. Через редагування мітки можливо отримати доступ до комп'ютера і тим самим виконати різноманітні види атак.

Вразливі місця RFID-мітки – SQL-Injection, web-інтерфейси, де не виключена можливість впровадження шкідливого коду, а також перевантаження стеку.

Типи атак які виконуються у технології QR:

1) Підміна коду; 2) Злом технології QR.

Типи атак які виконуються у технології GPS:

1. GPS Spoofing. Spoofing атака на GPS – атака, яка намагається обдурити GPS-приймач, передаючи більш потужний сигнал, ніж отриманий від супутників GPS, який може бути схожий на ряд нормальних сигналів GPS.

2. GPS Jammer. Вимкнення чи придушення глобальної системи супутникової навігації GPS.

Технології передачі даних

Для бездротової передачі даних особливо важливу роль в побудові Інтернету речей відіграють такі характеристики, як:

1)ефективність; 2)відмовостійкість; 3)адаптивність; 4)можливість самоорганізації.

Основний інтерес у цьому сенсі представляють стандарти IEEE 802 [4], що управляють доступом до організації енергоефективних персональних мереж, і є основою для таких протоколів у Інтернеті речей, як: ZigBee, WiFi, Bluetooth, 6LoWPAN. Відповідно, кожна з цих технологій має вразливості, через які можна перехопити дані. [5]

Типи атак які виконуються у бездротовому інтерфейсі IEEE 802.11:

1. Імперсонація та Identity Theft.
2. Мережевий сніффинг.
3. IP-spoofing.
4. Mac-spoofing.
5. Парольні атаки.
6. Атаки типу Man-in-the-Middle.
7. Переадресація портів.
8. Віруси і додатки типу "троянський кінь".
9. Відмова в обслуговуванні (Denial of Service - DoS).
10. Атаки на рівні додатків.
11. Атаки з деаутентифікацією [6][7][8].

Системи захисту потрібно комбінувати між собою для більшої ефективності, бо стандарт IEEE 802.11 надає вкрай слабкі засоби забезпечення безпеки, схильні до численних мережевих атак.

Найефективнішими методами захисту від атак на Інтернет речей будуть:

1. Планова перевірка апаратного функціоналу пристроїв.
2. Перевірка і використання систем захисту і антивірусів.
3. Шифрування даних найсучаснішими стандартами і технологіями.

4. Резервне копіювання.

Запобігти атакам на інформаційні технології в наш час неможливо, бо всі галузі і дані взаємодії людства перенесені у мережу, відповідно, до цих даних виникає інтерес третіх сторін.

Література:

1. Клаус Финкенцеллер. Довідник по RFID. — М.: Видавничий дім «Додэка-XXI», 2008. — 496 с.

2. Сандип Лахіри. RFID. Вказівки по впровадженню RFID Sourcebook / Дудников С . - М .: Кудиц-Пресс, 2007. - 312 с.

3. Максим Власов. RFID: 1 технологія - 1000 рішень: Практичні приклади використання RFID в різних областях. - М.: Альпина Паблішер, 2014. - 218 с.

4. Intercepting Mobile Communications: The Insecurity of 802.11 - Режим доступу: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

5. IEEE 802.22TM-2011 Standard for Wireless Regional Area Networks in TV Whitespaces Completed. - Режим доступу: http://www.businesswire.com/news/home/20110726007223/en/IEEE-802.22T

6. An Initial Security Analysis of the IEEE 802.1x Standard - Режим доступу: http://www.cs.umd.edu/~waa/1x.pdf

7. Official IEEE 802.11 Working Group Project Timelines - Режим доступу: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

8. Cisco Wireless LAN Security Web site - Режим доступу: http://www.cisco.com/go/aironet/security

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

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

ІНТЕРНЕТ РЕЧЕЙ: ВПЛИВ НА РОЗВИТОК ПРАВА ЄВРОПЕЙСЬКОГО СОЮЗУ (КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПИТАНЬ КІБЕРБЕЗПЕКИ)

Сучасний період розвитку правового регулювання інформаційної безпеки Європейського Союзу є послідовним продовженням попередніх чотирьох періодів (зокрема 1980–1998 рр., 1999–2004 рр., 2005–2008 рр. і 2009–2013 рр.). Він є логічним продовженням і європейської політики в

галузі впровадження, і розвитку новітніх і перспективних інформаційно-комунікаційних технологій. Його розвиток, що розпочався з 2014 р., пов'язаний із кількома чинниками і характеризується наступним.

Період з 2014 р. до 2017 р. видрізняється від попередніх значними змінами, внесеними інформаційно-комунікаційними технологіями (далі – ІКТ), які вже стали невід'ємним елементом як європейської економіки, так і повсякденного життя. Реалізація інноваційних способів використання ІКТ стає сьогоденною реальністю і очікує на подальший масштабний розвиток.

Серед інших, що несуть зміни – Інтернет речей (Internet of Things) – є одним із різноманітних і масштабних. Початкове підключення, як очікується, більше мільярда пристроїв до електронних мереж в Європейському Союзі надає значні переваги і зручності. У той же час, це здійснює і значний негативний вплив – зростає кількість, обсяг, розмах і різноманітність кібернетичних загроз.

Враховуючи ситуацію, Європейська комісія у 2017 р. запропонувала своє бачення нової, викликаної часом, архітектури європейської кібербезпеки та її правового забезпечення.

Доволі значний запропонований проект спирається на існуючі правові засади і, разом з тим, запроваджує нові ініціативи, спрямовані на такі цілі, що вдосконалюють систему кібербезпеки Європейського Союзу:

- забезпечення стійкості Європейського Союзу до кібератак та посилення його загальної спроможності до забезпечення кіберзахисту;
- створення дієвої системи кримінальної відповідальності;
- зміцнення глобальної кібернетичної стабільності через міжнародне співробітництво.

Широке і загальне формулювання цілей знайшло доволі чіткі відображення положень щодо їх реалізації в сучасних умовах, а також у можливій перспективі.

Досягнення першої мети – забезпечення стійкості Європейського Союзу до кібератак та посилення його загальної спроможності до кіберзахисту передбачає наступні заходи.

a) *утворення Агенції Європейського Союзу з кібербезпеки*;

Утворення Агенції планується здійснити на базі чинної Європейської асоціації мереж та інформаційної безпеки (ENISA), мандат якої спливає у 2020 р.. Європейська комісія пропонує надати більших повноважень Агенства з кібербезпеки, забезпечивши його постійним мандатом, значними операційними ресурсами та стабільною фінансовою основою.

Головною метою діяльності Агентства буде надання допомоги державам-членам. Головними напрямами роботи визначені оперативна співпраця і сертифікація безпеки ІКТ. Мандат, повноваження та завдання нової Агенції підлягатимуть постійному перегляду і розширенню.

b) *запровадження загальноєвропейської системи сертифікації кібербезпеки для продуктів та послуг ІКТ*;

Європейська комісія пропонує створити систему, яка, як очікується, буде визначати і надавати численні індивідуальні європейські схеми сертифікації кібербезпеки ІКТ, зокрема, у формі чітко визначених описів вимог безпеки, яким повинні будуть відповідати продукція, системи чи послуги ІКТ. Отримані сертифікати безпеки ІКТ, що підтверджують відповідність цим вимогам, визнаватимуться в усіх державах-членах ЄС.

Використання схем сертифікації буде на добровільній основі для учасників ринку. Високі стандарти кібербезпеки ІКТ, підтверджені і засвідчені за допомогою такої схеми сертифікації, можуть перетворитися на конкурентні переваги для компаній, які бажають забезпечити споживачів продуктами та послугами, що мають певний рівень кіберзахисту.

Сертифікація безпеки ІКТ відіграватиме важливу роль у підвищенні довіри та безпеки до продуктів та послуг ІКТ, що є ключовими для безперешкодного функціонування єдиного ринку цифрових технологій.

c) *прийняття акту щодо співпраці у реагуванні на масштабні інциденти та кризові ситуації в галузі кібербезпеки ЄС;*

Запропоновано прийняти «Керівництво щодо реагування на масштабні інциденти та кризові ситуації в галузі кібербезпеки».

Акт визначає цілі та способи співпраці між державами-членами та інституціями ЄС у відповідь на масштабні інциденти та кризові ситуації та пояснює, як існуючі механізми врегулювання кризи можуть взаємодіяти з існуючими органами кібербезпеки на рівні ЄС. Також державам-членам та інституціям ЄС пропонується створити *Рамкову програму критичного реагування в галузі кібербезпеки в ЄС* задля дієвості цього проекту. Заплановано, що він буде регулярно проходити тестування в кібер- та інших програмах кризового менеджменту.

d) *створення мережі з кібербезпеки з центром досліджень у галузі кібербезпеки;*

На думку Європейської комісії, протидія кіберзагрозам з боку ЄС потребує масштабних інвестицій у технології кібербезпеки, продукти, процеси та експертизи для досягнення технологічної автономії кібербезпеки та захисту своєї цифрової економіки, суспільства та демократії. Ці можливості є також важливими для сприяння глобальним зусиллям, спрямованим на створення безпечного кіберпростору для всіх. На основі роботи держав-членів та державно-приватного партнерства, започаткованого в 2016 році, Комісія пропонує створення мережі з кібербезпеки з центром досліджень у галузі кібербезпеки в Європі.

Центр європейських досліджень та компетенції з кібербезпеки допоможе розробити та впровадити інструменти та технології, необхідні для усунення постійно змінюваних загроз. Він буде доповнювати зусилля з нарощування потенціалу в цій сфері на рівні ЄС та на національному рівні.

Досягнення другої мети – створення дієвої системи кримінальної відповідальності – пов’язується із вдосконаленням законодавства ЄС.

Одним із кроків на шляху до вдосконалення кримінального законодавства щодо реагування на порушення кібербезпеки було прийняття у 2013 році *Директиви про напади на інформаційні системи*, яка встановила мінімальні правила щодо визначення кримінальних злочинів та санкцій у сфері нападів на інформаційні системи та забезпечила оперативні заходи.

Разом з цим, Комісія пропонує додатково посилити кіберзахист шляхом прийняття нової *Директиви з боротьби з шахрайством та підробкою безготівкових засобів платежу*. Відповідно до Стратегії кібербезпеки ЄС, а також Стратегії єдиного цифрового ринку, нова Директива посилить здатність держав-членів проводити кримінальне переслідування за шахрайство з безготівковими платежами.

Досягнення третьої мети – зміцнення глобальної кібернетичної стабільності через міжнародне співробітництво пропонується шляхом створення та підтримки надійних альянсів та партнерських відносин з третіми країнами задля запобігання та стримування кібератак.

ЄС вже співпрацює з США, Японією, Індією, Південною Кореєю та Китаєм. Також діють тісні консультації з міжнародними організаціями, такими як: НАТО, регіональний форум АСЕАН, ОБСЄ, Рада Європи та ОЕСР.

У липні 2017 р. у ЄС визначені рамки для спільної дипломатичної протидії зловмисній кібер-активності («Toolbox» для кібер-дипломатії).

Вперше у 2017 та 2018 роках НАТО та ЄС проведуть паралельні та скоординовані навчання у відповідь на можливий гібридний сценарій.

В умовах розробки Україною національного законодавства у сфері кібербезпеки дієвими можуть виступити врахування досвіду ЄС, перспективних майбутніх планів, програм і проектів, а також участь у спільних європейських проектах із забезпечення кібербезпеки.

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

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

ІНТЕРНЕТ РЕЧІ: ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВПЛИВ

У сучасному інформаційному суспільстві з'явився більш могутній засіб реалізації прийомів і методів спеціальних впливів – інтернет як засіб перетворення одноосібної або мало розповсюдженої інформації у масову. Людина, що живе в штучному інформаційному полі, одержує найсвіжішу інформацію з усіх куточків планети, і не тільки ту, яка надається їй пресою, радіопередачами, з екранів телевізорів. У такому випадку, повсякденно знаходячись у світі відірваних від реальності символів, людина може йти навіть проти своїх власних інтересів. Реальність при цьому відходить на задній план і відіграє підлеглу роль. У цьому сенсі людина не є вільною.

Сучасні засоби масової комунікації формують «масову» людину даного часу. У той же час вони роз'єднують людей, витісняють традиційні безпосередні контакти, заміняючи їх соціальними мережами, телебаченням та різного роду інформаційними і інформаційно-пошуковими системами. У деяких дослідженнях наведені характерні риси такої «масової» людини. Там відзначається, що одночасне поширення суперечливих взаємовиключних суджень затрудняє адекватну орієнтацію, породжує байдужність і апатію, провокує некритичність, формує виникнення соціальної дезорієнтації: більше враження справляє не аргументований аналіз, а енергійне, упевнене, нехай і бездоказове, твердження. Сприйняття формується не книжковою, як раніше, а екранною культурою. На цьому тлі відзначається зниження здатності до концентрації уваги.

«Масову» людину роблять імпульсивною, мінливою, здатною лише до відносно короткострокових програм дії. Вона часто віддає перевагу ілюзіям перед дійсністю. «Масова» людина, спрощена, має підвищену здатність до

навіювання – стає тим бажаним об'єктом, свідомість якого виявляється наскрізь структуровано небагатьма, але наполегливо впроваджуваними в неї твердженнями. Ці формули впливу, нескінченно транслюючись засобами інформації, утворюють деяку мережу з керуючих думок, установлень, обмежень, що регламентує і визначає її реакції, оцінки і, у кінцевому рахунку, поведінку.[6]

Науковці виокремлюють вербальний та невербальний механізми інформаційного впливу[7]. Так, в основі вербального лежать закономірності усвідомленого сприйняття змісту інформації. Він відбиває загальні закономірності інформаційних процесів у соціальному середовищі. Спочатку у людини формуються певний спосіб мислення, світогляд, система цінностей та інтересів, тоді відбувається процес їхнього збагачення та розвиток у якийсь конкретний бік, у результаті утворюється певний морально-семантичний фільтр, і нарешті, після отримання уже нової інформації відбувається аналіз та абсорбація із допомогою вищезгаданого фільтру, і в результаті цього процесу формуються нові вчинки, поведінка індивіда відповідно до певної ситуації. Самі орієнтації та усталеність фільтру впливають на той чи інший кінцевий результат. Якісні та змістовні характеристики такого фільтру залежать від ідеологічної пропаганди, релігії, філософських учень, національно-етнічних показників, системи освіти, історичних факторів, а також засобів масової інформації[8].

Щоб протидіяти маніпуляціям, необхідно заборонити інтерпретувати та поширювати неперевірену та неправдиву інформацію, здійснювати активне поточне аналітичне коментування подій. Для цього слід об'єднати зусилля громадськості, сім'ї, освіти всіх рівнів і влади. Уряд повинен на законодавчому рівні обмежити ЗМІ показ сенсаційних кримінальних новин

---

[6] Сучасні методи психологічного впливу. Режим доступу: http://sd.net.ua/2012/03/05/suchasni-metodi-psixologichnogo-vplivu.html

[7] Архипова Є. О. Інформаційна безпека: соціально-філософський вимір : дис. … кандидата філософ. наук : 09.00.03 / Є. О. Архипова. – К.: Нац.Техн.Ун-тетУкраїни«Київський політехнічний інститут», 2012. – 199 с.

[8] Грачев Г. В. Манипулирование личностью: Организация, способы и технологии информационнопсихологического воздействия / Г. В Грачев, И. К. Мельник. Издание второе, исправленное и дополненное. – М.: Алгоритм, 2002. – 228 с.

та сцен насильства. Цілком можливо, що доведеться створювати громадські освітні та просвітницькі програми з питань медіа грамотності на державному чи громадському телебаченні, навчати учнів об'єктивно аналізувати переглянуту телевізійну програму, порівнювати запропоноване в телепрограмах з реальним життям[9]. А також, з урахуванням сучасних реалій, необхідно обов'язково:

- вжити термінових заходів із забезпечення доступу населення прифронтових, окупованих та прикордонних районів до українських ЗМІ (пересувні передавачі для аналогового телебачення, забезпечення поширення преси, де це можливо);
- реально обмежити доступ сепаратистських ЗМІ до територій, підконтрольних українському урядові;
- забезпечити інтенсивну і компетентну комунікацію уряду з громадянами (в першу чергу через взаємодію зі ЗМІ) для роз'яснення цілей державної політики, особливо у питаннях управління окупованими територіями; – національним і регіональним ЗМІ, громадським організаціям розробити спільну стратегію інформаційної роботи з населенням, спрямовану на руйнування негативних міфів та стереотипів, що їх створює російська пропаганда, а також на розвінчування фейків, що потрапляють до інформаційного простору України з російських ЗМІ;
- відновити довіру населення окупованих територій до національних ЗМІ. Для цього медіа мають бути максимально правдивими та об'єктивними, а також створювати інформаційний продукт, розрахований на задоволення інформаційних потреб населення окупованих територій;
- включити елемент аналізу у процес вироблення державної політики в інформаційній сфері. Цілі та завдання державної політики, а також зміст політичних рішень будувати на основі чітко сформульованих проблем та потреб. Відійти від практики орієнтації на політичну волю всупереч даним аналітики;

[9] Субота Є. В. Інформаційно-психологічний вплив / Є. В. субота // Вісник ХДАК. – 2016. №49. – С.120-130, с.127-128.

- у подальшій перспективі впровадити в життя реальні інструменти, спрямовані на підтримку національного інформаційного продукту (кіно, телепрограм, книг, преси тощо). Обсяг національного продукту, який виробляється, має бути одним з ключових індикаторів в оцінці державної інформаційної політики;

- на державному рівні – необхідно забезпечити підтримку кампанії з просування медіа грамотності та включення елементів медіа освіти до системи загальної шкільної освіти; – підвищити спроможність медіа протидіяти пропаганді, мові ненависті і ворожнечі, а також створювати інформаційні продукти, розраховані на цільові групи, які є вразливими до пропаганди. Доцільними видаються: вивчення закордонного досвіду участі ЗМІ у відновленні довіри та примиренні; освітні заходи для журналістів; моніторинг контенту ЗМІ[10].

На завершення необхідно відмітити, що, незважаючи на зовнішньо орієнтовну технічну сторону, інтернет речей, впровадження та розвиток даного напряму науково-технічного прогресу, без сумніву, відобразиться і на питаннях інформаційно-психологічного впливу на людину та суспільство в цілому. Ступінь та глибина цього відображення потребує додаткових наукових досліджень

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

Арістова І. В.,
д. ю. н.,професор, завідувач кафедри адміністративного та інформаційного права Сумського національного аграрного університету

ФЕНОМЕН ІНТЕРНЕТУ РЕЧЕЙ: МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Усвідомлюючи існування суттєвого впливу технологічних революцій на життя сучасного суспільства в умовах глобалізації, що зумовлює, серед іншого, появу нових термінів, водночас, на мою думку, виникає об’єктивна

[10] Шутов Р. Стратегія та можливості інформаційно-психологічного впливу Росії на територіях, підконтрольних урядові України / Р. Шутов // Агора. №15. – С.53-58, с.58

потреба у з'ясуванні передусім змісту таких термінів, наприклад, як «інтернет речей». Для отримання відповіді на поставлене питання, вважалося за необхідне проаналізувати існуючі доктринальні визначення зазначеного терміну. Дослідження показали, що таку ж саме мету було поставлено і у статті відомого фахівця у галузі інформаційного права О.А.Баранова [1]. Ознайомлення з позиціями різних дослідників (зокрема, А. Лучеса, С. Халлера, Д. Еванса, Р.Гласса, К. Еберсалда, Е. Бербі та ін.), які викладені у роботі [1], дозволило переконатися у відсутності загального, усталеного визначення терміну «інтернет речей».

На мою думку, усвідомленню феномену «інтернет речей» сприятиме конструктивне впровадження належної методології дослідження. Оскільки йдеться про активізацію ролі науковців у пізнанні зазначеного феномену, вважаємо за доцільне під методологією розуміти вчення про організацію наукової діяльності та наукових знань [2] щодо інтернету речей. Виходячи із важливості ролі та місця суб'єкта наукової діяльності у методології дослідження, вважаємо за необхідне акцентувати увагу на значенні формування якісних стандартів, які мають бути у будь-якого суб'єкта (дослідника). Відомо, що такі стандарти передусім виробляються наукознавством [3]. Зокрема, дослідник повинен достатньо чітко і свідомо знати структуру наукового знання, критерії науковості наукового знання, форми наукового знання, якими він користується і в яких він хоче відобразити результати свого наукового дослідження і т. ін.

Розуміючи значення перелічених вище складових стандарту дослідника, вважаємо за можливе передусім стисло висвітлити питання, пов'язані із формою організації наукових знань. Аналіз літератури дозволив встановити, що на сьогодні практично відсутнє систематичне викладення зазначеного питання. Водночас, автори роботи [4, с. 43–52], усвідомлюючи сучасний стан опрацювання зазначеної теми, а також існування тенденції щодо помилкового та безсистемного використання науковцями форм організації наукових знань, навели повний системний опис зазначених форм.

Вважаємо за доцільне конструктивно використати цей матеріал у нашому дослідженні. Передусім, слід зазначити, що аналіз багатьох наукових праць, зокрема, у сфері інформаційного права засвідчив, що науковці:

1) вводять у науковий обіг різноманітні поняття, категорії;

2) висувають гіпотези; 3) розробляють концепції, теорії; 4) формують ідеї; 5) порушують проблему і т. ін.

З одного боку, у роботі підтримується у цілому намагання дослідників щодо розбудови науки інформаційного права, з іншого боку, вважаємо, що науковий рівень цих досліджень не завжди «дотягує» до існуючих стандартів, зокрема, щодо правильного розуміння та коректного використання таких конструкцій.

Ґрунтуючись на положеннях дослідження [4, с. 43 – 52], пропонуємо формами організації наукових знань, зокрема, у сфері інформаційного права вважати наступні: факт, положення, поняття, категорія, принцип, закон, теорія, ідея, доктрина, парадигма, проблема, гіпотеза. Усвідомлюючи важливість розкриття усіх зазначених форм, а також враховуючи обмежений обсяг тез, у роботі вважалося за можливе передусім акцентувати увагу на дослідженні «поняття» як однієї із форм організації наукових знань. Такий вибір зумовлений наступними чинниками:

1) інші форми організації наукових знань (факти, положення, теорії і т. ін.) виражаються через слова-поняття та зв'язки між ними;

2) найвищою формою людського мислення є понятійне, словесно-логічне мислення.

У зв'язку з останнім, дуже слушною є думка, що «зрозуміти» означає виразити у формі таких понять, які породжують адекватні образи. У роботі використовується наступне розуміння терміну «поняття»: це «думка, яка відображає в узагальненій та абстрактній формі предмети, явища й зв'язки між ними через фіксацію загальних та специфічних ознак – властивостей предметів та явищ» [4, с. 43].

Вважаємо, що дослідник має враховувати, що у науці існує точка зору про існування так званих «понять, що розвиваються». На нашу думку, у процесі становлення, зокрема науки інформаційного права спостерігається тенденція до накопичення нових наукових даних та розвитку наукових теорій, що може спричинити появу нових ознак та властивостей, що, у свою чергу, коригує зміст поняття (наприклад, поняття «інформаційне суспільство», «інформаційна сфера», «інформаційні відносини», «інформаційні правовідносини»). Тобто, зазначені поняття є прикладами «понять, що розвиваються» [2]. У роботі пропонується здійснювати постійний моніторинг змін у змісті понять, зокрема, науки інформаційного права, оскільки це, серед іншого, дозволить оперативно повідомляти відповідні органи державної влади щодо необхідності врахування змін у інформаційному законодавстві. Водночас, слід зазначити, що з'являються і нові поняття, які потребують свого визначення, наприклад поняття «інтернет речей».

Виходячи із того, що процес утворення та розвитку понять вивчає логіка (формальна та діалектична), у роботі наголошується на необхідності активізації використання логіки для правильного конструювання визначення понять будь - якої науки, у тому числі і науки інформаційного права. Вважаємо за необхідне акцентувати увагу на існуванні різних класів понять (наприклад, індивідуальні, загальні, збірні, абстрактні, конкретні, відносні, абсолютні) [5, с. 7 – 12], що треба враховувати під час формування понятійної бази передусім інформаційного права, яке знаходиться на етапі свого становлення. Зважаючи на те, що у логіці розглядаються такі конструкції (які відносяться до структури понять) як зміст та обсяг, слід чітко їх розуміти, а також знати, у чому полягає різниця між ними. Отже, обсяг понять визначає таку сукупність елементів, до якої додається дане поняття, а зміст визначає такі ознаки, які притаманні тому чи іншому поняттю [5, с. 15]. Що стосується ознак понять, то з часів Аристотеля вони поділяються на п'ять класів: родова ознака, видова відмінність, вид, власна ознака, невласна

ознака [5, с. 13, 14]. Вважаємо, що спеціального дослідження потребує і проблема відношення між поняттями, що пов’язано із розглядом логічних відношень, наприклад, субординація понять, координація понять, рівнозначність понять, протилежність понять, практичність понять та ін.

Усвідомлюючи, що головна мета визначення поняття – розкрити зміст поняття, зробити зміст поняття таким, щоб він був точним, у роботі акцентується увага на двох способах визначення поняття: а) перерахування ознак, які притаманні даному поняттю; б) визначення здійснюється за допомогою найближчого роду та видової різниці; визначення відбувається за допомогою судження, яке містить підмет та присудок; правильне визначення зумовлено дотриманням чотирьох спеціальних правил [5, с. 26–28]. Слід визнати, що існують і інші способи, наприклад, вказівка, опис, характеристика, порівняння та ін.

Аналіз багатьох наукових досліджень, зокрема, у галузі інформаційного права (передусім дисертаційних досліджень) переконливо доводить, що використання логіко-семантичного методу для визначення понятійної бази лише анонсується, і насправді є суттєві підстави для активізації наукової дискусії щодо правильного мислення, яке має бути підпорядковано вимогам чотирьох його законів. Розуміючи важливість і одночасно складність порушеного питання, вважаємо за необхідне привернути увагу наукової спільноти до спільного вирішення зазначеного питання, у тому числі щодо визначення поняття «інтернет речей».

Зважаючи на те, що останнім часом науковцями (зокрема, у роботі [1]) обговорюються питання перспектив і особливості феномену інтернету речей в контексті правової науки слід, на нашу думку, акцентувати увагу ще на одному стандарті дослідника відповідного об’єкта – на критеріях науковості нового знання. Встановлено, що науковому знанню притаманне те, що не просто повідомляється про істинність того чи іншого змісту, але й наводяться підстави, відповідно до яких цей зміст істинний (наприклад, логічний висновок). Таким чином в якості ознаки, що характеризує істинність

наукового знання, вибирають вимогу його достатньої обґрунтованості. До речі, принцип достатньої підстави (у логіці він називається «законом достатньої підстави») постає фундаментом усієї науки [4, с. 38].

Вважаємо, що існує потреба у перевірці на дотримання передусім принципу достатньої підстави тих знань про об'єкт дослідження (інтернет речей), які засвідчують про існування суспільних відносин та необхідність їх правового регулювання. У зв'язку із зазначеним, на нашу думку, перспективним напрямом дослідження постає аналіз процесу перетворення соціально-технічних норм у техніко-юридичні [6, с. 286, 287], що дозволить «зняти» деякі питання стосовно «юридичної конотації» дефініції терміну «інтернет речей» [1, с. 101].

Література:

1. Баранов О. А. «Інтернет речей» як правовий термін / О. А. Баранов // Юридична Україна. – 2016. – № 5–6. – С. 96-103.
2. Арістова І. В. Становлення науки «інформаційне право»: питання методології (частина ІІ) / І. В. Арістова // Публічне право. – 2016 р. – №. 3. – С. 232 – 243.
3. Кочергин А. Н. Методы и формы познания/А. Н. Кочергин. – М.: Изд-во МГУ, 1990. – 76 с.
4. Новиков А. М., Новиков Д. А. Методология научного исследования / А. М. Новиков, Д. А. Новиков. – М.: Либроком, 2009. – 280 с.
5. Челпанов В. Г. Учебник логики / В. Г. Челпанов. – М.: Научная библиотека, 2010. – 128 с.
6. Скакун О. Ф. Теория государства и права: учебник/ О. Ф. Скакун. – Харьков: Консул; Ун-т внутр. дел, 2000.– 704 с

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

Харитонов Є. О.,
д. ю. н., професор,завідуючий кафедрою цивільного права Національного університету «Одеська юридична академія», член-кор. НАПрН України.
Харитонова О. І.,
д.р ю. н., професор,завідуюча кафедрою права інтелектуальної власності та корпоративного права Національного університету «Одеська юридична академія», член-кор. НАПрН України.

МЕТОДОЛОГІЧНІ ПРОБЛЕМИ ВПОРЯДКУВАННЯ ВІДНОСИН У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ

У інформаційному суспільстві ефекти нових технологій охоплюють усі сфери людської діяльності, що, на думку Мануеля Кастельса, є однією з головних рис інформаційно-технологічної парадигми [1]. Наразі чи не найбільш помітним проявом цього феномену є, так званий, «Інтернет речей», котрий у найбільш загальному вигляді характеризують як концепцію комунікації об'єктів («речей»), які використовують технології для взаємодії між собою та з навколишнім середовищем, припускаючи при цьому виконання пристроями певних дій без втручання людини [2].

У більш ґрунтовному варіанті Інтернет речей визначають як сукупність

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) [3, с. 101].

Оцінка Інтернету речей у більшості випадків є суто позитивною (особливо з боку розробників). Разом із тим, у зв'язку з поширенням цього явища виникає низка ризиків, що загострює проблему впорядкування відповідних суспільних відносин.

При цьому слід зазначити, що специфіка інформаційних технологій зумовлює існування різних підходів до впорядкування відносин у ІТ-сфері. Позначимо ці підходи як:

1. «технологічний» (впорядкування здійснюється за допомогою самих інформаційних технологій)

2. «соціальний» (провідним є соціальне, у тому числі, правове регулювання). Якщо у першому випадку ІТ є інструментом здійснення/функціонування соціальних процесів, тобто переважає «технологічна» складова), то у другому – вони є предметом правового регулювання (тобто, переважає «інформаційна» складова).

Наразі помітною є тенденція зростання впевненості певних прошарків суспільства, осіб, долучених до ІТ, у доцільності й можливості вирішення багатьох соціально-економічних проблем за допомогою саме «технологічної складової», котра, нібито здатна забезпечити справедливе і безпечне впорядкування. Причому, часом ІТ-засоби впорядкування протиставляються правовому регулюванню (іноді останнє взагалі розглядається як нездатне забезпечити належне функціонування системи).

У підсумку значна частина відносин у сфері ІТ опиняється або може опинитися за межами правового поля і питання про доцільність і можливість їхнього повернення у це поле, поки що виглядає досить проблематичним [4].

До об'єктивних чинників такої тенденції слід віднести потреби економіки, інфраструктури, культури, пересічних користувачів у інформаційних технологіях, а також захоплюючі увагу результати застосування ІТ у цих та інших сферах буття. Великі сподівання покладаються на Blockchain, як базову технологію для вирішення проблем, у тому числі, у сфері Інтернету речей [5].

Ці обставини стали «спусковим механізмом» суб'єктивного чинника, яким можна вважати переоцінку можливостей «упорядкування» відносин за допомогою ІТ та значення «айтішників» у цьому процесі [6, с. 70-73; 7]. Це призвело до ідеалізації «ІТ-схем» організації бізнесу, результатів

застосування технології Blockchain, реабілітації (намірах легалізації) криптовалют, укладення смарт-контрактів тощо.

У підсумку маємо ситуацію, коли долучена до створення і використання ІТ частина суспільства, сподівається за допомогою суто технологічних рішень, шляхом зростання ролі ІТ досягти успіхів у бізнесі та гармонії в суспільстві, що й зумовлює обстоювання ідеї «ІТ-впорядкування», як шляху, альтернативного соціальному управлінню / впорядкуванню (правовому регулюванню та адмініструванню).

Проте активізація кібератак свідчить про неспроможність ідеї самовпорядкування ІТ-сфери на сучасному етапі її розвитку. У будь-якому разі немає гарантій, що якийсь хакер не вирішить спробувати довести свою першість, помститися комусь за образи або поліпшити своє матеріальне становище. Навіть якщо його зусилля будуть незабаром нейтралізовані, завдання шкоди відбудеться. У кращому разі, отримавши свої зиски, хакер заспокоїться лише на певний час.

Отже, проблеми, що виникають у ІТ, очевидно не можуть бути подолані лише за допомогою технічних засобів, оскільки останні можуть впливати лише на технологічну складову ІТ-сфери, залишаючи поза увагою «соціальний елемент», яким є учасники відносин, що виникають у ІТ-сфері. Це не можна визнати виправданим, оскільки саме соціальний елемент має бути об’єктом впливу. Хоча інформаційне поле дехто вважає не унікальною особливістю лише біологічних організмів, а загальною властивістю Всесвіту [8], виходимо з того, що при сучасному рівні знань вплив на це поле з метою його впорядкування реально можливий лише у частині його біологічного (людського) субстрату. Саме тому маємо підстави вести мову про впорядкування відносин у інформаційному суспільстві як про соціальне управління, котре є предметом свідомої діяльності людей, що ґрунтується на існуючих об’єктивних законах та разом із тим враховує їхні бажання. Одним з видів соціального управління є правове регулювання, котре слугує

основним засобом державного впливу на суспільні відносини з метою їхнього упорядкування в інтересах людини, суспільства і держави.

Проблеми правового регулювання у сфері Інтернету речей вже почали обговорюватися дослідниками і практиками, хоча методологічні підходи до їх вирішення ще не сформовані. Зокрема, авторами публікацій про Інтернет речей зверталося увагу на такі правові проблеми у цій галузі як збереження конфіденційності даних, захист права інтелектуальної власності, забезпечення кібербезпеки нових об'єктів, щодо яких зростають загрози хакерських атак, відсутність стандартів підключення у галузі технологій IoT, створення прецедентів тощо. При цьому відзначається прагнення представників законодавчих органів усіх країн світу заповнити прогалини у законодавстві, що виникають у зв'язку з появою технологій інтернету речей. У якості типового прикладу згадується, що у 2014 році Європейська комісія опублікувала думку з цього питання, детально розглянувши натільні пристрої та пристрої системи «розумний дім». Поміж рекомендацій Комісії є вимога про надання користувачам повного контролю над своїми даними. Також передбачені операції, які організаціям слід взяти до уваги для забезпечення відповідності вимогам законодавства ЄС про захист даних [10].

У запропонованому авторами підході, як на нашу думку, досить чітко проглядається орієнтація на цільове, «точкове» вирішення окремих, конкретних проблем, зокрема на основі прецедентів та видання нормативних актів, що стосуються конкретних випадків.

Проте більш правильною видається думка, автори якої, вважаючи, що розробка концепції правового регулювання ІТ має проводитися із врахуванням таких проблем (частина з яких тісно пов'язана з сучасними правовими проблемами регулювання Інтернету та інформаційних технологій як правовий режим інформації, персональні дані та приватне життя, нейтральність Інтернету речей, інформаційна безпека, сумісність та захист конкуренції, автоматизовані дії, децентралізовані мережі, при цьому слушно зазначають, що наведений перелік не є вичерпним, оскільки розвиток

технологій поставить нові проблеми, в тому числі й ті, котрі наразі передбачити неможливо).

Отже, маємо підстави для висновку про невиправданість орієнтації на «прецедентний» («кейсовий») підхід до вирішення проблем правового регулювання у ІТ-сфері, зокрема, у сфері Інтернету речей. Натомість, доцільним є створення концепту «ІТ-право», котре формується як симбіоз віртуальної та дійсної реальності, що відображає уявлення про цей феномен, спроби ввести у звичне правове поле традиційні цивільні відносини та ІТ-відносини, віртуальні за своєю сутністю.

Зараз до ІТ-сфери відносять широке коло відносин, які регулюються нормами цивільного, господарського, адміністративного законодавства. Зокрема, у сферу цивільно-правового регулювання попадають «ІТ-відносини» надання послуг програмного забезпечення або його розробки; правового захисту web-сторінок і контенту; правового забезпечення діяльності Інтернет-магазинів; ліцензійних угод; захисту прав інтелектуальної власності; захисту інформації тощо [11, с. 3]. Але оскільки розмаїття відносин, котрі вважаються «айтішними», створює на практиці істотні незручності при пошуку та застосуванні актів законодавства, які стосуються таких відносин, виникає необхідність визначення орієнтирів для встановлення кола норм, які можуть бути віднесені до сфери «ІТ-права».

При цьому враховуємо наступні засади визначення правового масиву у ІТ-сфері: 1) до сфери «ІТ-права» доцільно відносити лише регулятивні відносини, і відповідно, норми законодавства, що їх регулюють; 2) при систематизації та структуруванні «ІТ-права» має бути розрізнення цього поняття у широкому та вузькому сенсі; 3) під «ІТ-правом» у широкому сенсі розуміємо сукупність усіх норм і правил, що регулюють діяльність по використанню інформаційних технологій та інформаційної правомірної активності в Інтернеті; 4) структура «ІТ-права» у широкому сенсі виглядає як відносно інтегрована система багаторівневого порядку, котра містить приватно-правові та публічно-правові елементи, питома вага яких

визначається пріоритетністю приватних чи публічних інтересів. На цьому підґрунті визначаються особливості методів правого регулювання, що застосовуються у тих та інших випадках. Так, у відносинах інформаційної безпеки переважання публічних інтересів означає, що відповідні відносини регулюються лише нормами актів законодавства і не можуть бути змінені або припинені за домовленістю; 5) ІТ-відносини, що належать до приватно-правової сфери правового регулювання, переважно є регулятивними, тут діє принцип «Дозволено все, що не заборонено законом» (що дає можливість укладати будь-які договори). Саме за його допомогою складається основний масив норм ІТ-права – «ІТ-право» у вузькому сенсі, котре може розглядатися як регулятивні норми (переважно цивільно-правові), що забезпечують функціонування ІТ-відносин та відносин, пов'язаних з ними; 6) можливе також виокремлення «ІТ-права у спеціальному сенсі». До нього мають бути віднесені вже лише ті норми, що стосуються суто сфери ІТ-відносин: інформаційних відносин; програмного забезпечення; інтернету речей тощо.

У підсумку, враховуючи потенціал правового регулювання у ІТ-сфері та можливостей впорядкування ІТ-сфери за допомогою технологій, і можемо досягти бажаного балансу застосування соціальних та технологічних засобів впорядкування Інтернету речей.

Література:

1. Погляди Мануеля Кастельса на інформаційне суспільство. Режим доступу: http://osvita.ua/vnz/reports/econom_history/25179/

2. Що таке Інтернет речей. Режим доступу: http://iot.lviv.ua/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%80%D0%B5%D1%87%D0%B5%D0%B9/

3. Баранов О. «Інтернет речей» як правовий термін [Електронний ресурс] // Юридична Україна. – 2016. – № 5-6. – С. 96-103. – Режим доступу: http://nbuv.gov.ua/UJRN/urykr_2016_5-6_16. – С. 101

4. Павленко Д. Consensus и право 2017: регуляторные перспективы и вызовы блокчейна // http://forklog.com/consensus-i-pravo-2017-regulyatornye-perspektivy-i-vyzovy-blokchejna/

5. Yatskiv N.G., Yatskiv S.V. Перспективи використання технології блокчейн у мережі Інтернет речей. Режим доступу: http://nv.nltu.edu.ua/index.php/journal/article/view/451

6. Иванова Э. Короли жизни. – Новое время страны. – 2017. – № 12. – С. 70-73

7. Іщеряков С. Дуальна освіта: як втримати ІТ-мізки в Україні // https://dou.ua/lenta/columns/dual-education-in-ukraine/

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

9. Необходима осторожность: риски IoT. Режим доступу: http://www.ey.com/Publication/vwLUAssets/EY-mne-internet-of-things-rus/$File/EY-mne-internet-of-things-rus.pdf

10. Открытая концепция «Интернет вещей»: Правовые аспекты (Российская Федерация). Версия 1.0 для обсуждения.. Санкт-Петербург. 26.05.2016 года Режим доступу: http://www.dentons.com/ru/global-presence/russia-and-cis/russia/st-petersburg.aspx)

11. Бачинський Т. Основи ІТ-права. Посібник. – Львів: Апріорі. 2016. – С.3.

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

Отрешко Н. Б.,
д.соц.н., доцент, провідний науковий співробітник Інституту культурології НАМ України

ІНТЕРНЕТ РЕЧЕЙ: КОНЦЕПЦІЯ ТА РЕАЛЬНІСТЬ

Сполучення реального та віртуального світів, доповнена реальність, розумні інтерактивні середовища породжують не тільки економічні, а й глибокі політичні та соціо-культурні наслідки. Ми знаходимося на порозі найважливішою технологічної революції, яка можливо кардинально змінить не лише наш життєвий світ, а й саму природу людини та соціального світу.

Проект Інтернету Речей (Internet of Things, IoT) прийнятий в якості офіційної державної стратегії технологічного розвитку в ЄС та Китаї, а також є пріоритетним у багатьох міжнародних корпорацій (IBM, Cisco, HP ...). З 2009 року за підтримки Єврокомісії в Брюсселі щорічно проводиться конференція «Internet of Things» З початку 2010-х років «інтернет речей» стає рушійною силою парадигми «туманних обчислень» (англ. fog computing), розповсюджує принципи хмарних обчислень від центрів обробки даних до

величезної кількості взаємодіючих географічно розподілених пристроїв, яка розглядається як платформа «інтернету речей».

Починаючи з 2011 року Gartner поміщає «інтернет речей» в загальний цикл зрілості нових технологій на етап «Технологічного тригера» із зазначенням терміну становлення більше 10 років, а в 2012 році випущений спеціальний цикл зрілості для технологій «інтернету речей».

IOT − концепція простору, в якому все з аналогового і цифрового світів може бути поєднане. Цей процес в подальшому призведе до перевизначення як самих людських відносин з об'єктами в навколишньому середовище, так і властивостей і суті об'єктів. IOT – це єдина мережа, яка об'єднує навколишні нас реальні і віртуальні об'єкти. Річ в такому просторі − це будь-який об'єкт реального або віртуального світу, який існує, переміщується в просторі і часі і може бути однозначно визначено. Складові простору IOT − це речі (як реальні, так і віртуальні), системи комунікації, системи пеленгації (локації), системи управління та моніторингу та люди (Користувачі).

Проблема полягає в тому що говорити про IOT так, як ніби цей простір вже існує неправильно, насправді його ще не існує, ні в якому з можливих значень визначень цього поняття.

Проблеми, які не дозволяють сформуватися IOT:

- немає віртуальних образів більшості реальних речей (загальний опис, їх властивості та органи управління, їх поточні параметри, положення в просторі);
- більшість речей пасивні (малоактивні, малосамостійно функціональні) в плані їх фізичної активності;
- речі не бачать (погано бачать) одна другу;
- речі погано розуміють одна одну;
- речі не вміють самоорганізовуватися: навіть дві речі не знають як і для чого взаємодіяти, складно самоорганізуються конфігурації речей, що складаються з багатьох елементів і утворюють складні системи – поки це не реальність, а фантастика;

- речей не видно людині і немає зручних інтерфейсів взаємодії людини з віртуальними образами речей і конструкторів, що дозволяють людині конфігурувати простір речей (організовувати їх взаємодію однієї з другою, а також взаємодію з користувачем);
- речі дуже енергозалежні;
- слабкі економічні стимули: подорожчання речей, необхідне для їх підключення до ІОТ не дає очевидного прибутку, а частіше призводить до невиправданого збитку.

Але головною проблемою є те, що не лише серед користувачів Інтернет, а й серед спеціалістів не існує ясного бачення концепції «Інтернету речей» (знання про те, що це за новий простір, які його можливості та ознаки).

Крім цього, якщо нинішні тенденції розвитку ІТ індустрії не зміняться, віртуалізація простору та речей у ньому опиниться у пастці централізованих Бункерів. Зрештою, компанії і постачальники софта об'єднають ці бункери, і відмінності в протоколах стануть просто неважливими. І так само далі почнуть вибудовуватися економічні стимули. Однак розділяти дані стане важче, ніж повинно бути, враховуючи необхідність продовжувати будувати нові зв'язки між бункерами Це може стати, предметом високої завантаженості концентраторів, сповільнюючи надання послуг. Централізація даних може знизити їх безпеку і конфіденційність.

Щодо висновків (що робити у такої ситуації):

- Орієнтуватися на глобальну мережу, але робити локально корисні речі;
- Бачити системи і процеси в цих системах − будувати ІОТ для оптимізації цих систем;
- Орієнтуватися на інтерфейси мозок-машина (побудова систем навколо людини, а не вбудовування його в побудовану середу);
- Накопичувати знання - перехід на новий рівень розуміння реальності.

Боклан С. Г.,
студент бакалавр ФСП КПІ ім. Ігоря Сікорського.
Науковий керівник:
Мельник Б. Б., *викладач ФСП КПІ ім. Ігоря Сікорського*

ІНТЕРНЕТ РЕЧЕЙ І «ХВИЛІ» ЦИВІЛІЗАЦІЙ ЗА Е. ТОФФЛЕРОМ

Світ стоїть на порозі великих змін, широкого застосування новітніх технологій і процесів. Як зазначає Касьян В.І., автор праці [1]: «Поява нової наукоємної технології, реорганізація виробництва на основі впровадження найновіших досягнень науки й техніки привели в рух "третю хвилю" розвитку цивілізації, яка руйнує всі принципи попередньої економіки та змінює її на протилежні.» На його думку, у класичній праці «Третя хвиля» [2] Е. Тоффлер, почесний доктор літератури, права, природничих наук і менеджменту, член Міжнародного інституту стратегічних досліджень і член Американської асоціації розвитку науки «прагне обґрунтувати тезу, що економіка не є найголовнішим чинником сучасного капіталізму. Нова цивілізація буде кардинально відрізнятися від капіталістичного періоду "індустріалізму", в якому основними регулятивними принципами є стандартизація, концентрація, максимізація, які не будуть спрацьовувати при переході до економіки самообслуговування.» Це веде за собою і зовсім інший характер виробництва. Як пише Е. Тоффлер: «Новий спосіб виробництва робить можливим повернення до домашнього виробництва на новій, вищій, електронній базі й акцентує увагу на домівці як центрі суспільства». Тобто замість виробництва товарів для ринку, яке побудовано на концентрації власне виробництва і обслуговування в одному місці з'являється можливість все робити вдома, а це отримує назву промисловості самообслуговування. Такому типу виробництва і споживання відповідає певна етика. «Замість ранжування людей згідно з тим, чим вони володіють, ця етика надає високу цінність тому, що люди роблять» [1].

У своїх основних працях Е. Тоффлер наводив думку про те, що людство на межі XX і XXI століть знаходилося на переході до Третьої технологічної хвилі, так званої постіндустріальної цивілізації, становлення якої завершиться до 2025 року. Їй передувала Друга хвиля – індустріальна цивілізація, а Першою хвилею була аграрна цивілізація. Хвилі за термінологією цього автора – це ривки у розвитку науки і техніки. Усвідомлення людством потреби переходу до нової хвилі є поступовим, еволюційним процесом, однак породжує глибокі потрясіння, що мають суттєвий вплив на суспільство [2].

На думку прибічників «хвилеподібного» розвитку суспільства, тобто поступової зміни стадій, за постіндустріальною цивілізацією, економікою послуг, приходить Четверта хвиля – настає час інформаційного сектора економіки. Капітал і праця як основа індустрії поступаються місцем інформації та знанням в інформаційному суспільстві. Під час Третьої хвилі відбулася цифрова революція, широкого розповсюдження набули інформаційно-комунікаційних технології, обчислювальна техніка, зокрема персональні комп'ютери, персональні портативні комунікаційні пристрої, широке проникнення в наше життя Інтернету, процеси автоматизації, глобалізації та виникнення постіндустріальної економіки з 1980-х років по перші десятиліття XXI століття.

А серед поширених термінів, пов’язаних із четвертою промисловою революцією, є «Інтернет речей». Як стверджують автори у праці [3]: «Переважна більшість експертів погоджуються, що Інтернет речей до 2025р. набуде широкого розповсюдження і принесе користь людству, але є й більш скептичні прогнози. Інтернет речей – це сукупність фізичних об’єктів, комплексно з’єднаних між собою за допомогою сучасних Інтернет технологій. Він дає можливість появи нових, більш ефективних методів виробництва та ведення бізнесу. Інтернет речей – річ більш еволюційна ніж революційна, тобто усі необхідні технології для нього вже існують, але він поки мало

розповсюджений з точки зору масового застосування. Тим не менш, динаміку його розвитку на сьогоднішній день не варто недооцінювати [3].»

Баранов О. визначає Інтернет речей як «сукупність 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)» [4].

Четверта хвиля наче усуває кордони між фізичним, цифровим і біологічним світами. Як стверджують автори [3], у 2008 р. число пристроїв, приєднаних до Інтернету перевищило число населення Землі, через п’ять років пристроїв було вже 13 мільярдів і їх число зростає невпинно. Згідно з даними компанії Cisco, наведеним у [3], в 2020 р. таких пристроїв буде 50 мільярдів, включаючи телефони, чіпи, сенсори, імплантати тощо. Способи взаємодії з технікою будуть покращуватись, особливо голосові команди та управління дотиком, є припущення, що у 2025 р. масового поширення набуде безпосередній зв'язок мозку з Інтернетом.

Технології, які дозволяють реалізувати Інтернет речей, вирішують чотири основні задачі: ідентифікацію, збирання даних, зберігання даних та обмін інформацією. Необхідно врахувати, що це викликає певні наслідки, зокрема [3, 5]:

- Безперервний моніторинг стає великою частиною життя пересічної людини;
- Отримання потрібної і достатньої інформації про речі, з якими люди взаємодіють, у будь-який час;
- Голосова подача команд створює цілу «армію кіберприслужників»;
- Комунікація пристроїв зі штучним інтелектом - «комп’ютикація» (Computication);

- Сенсори і спостереження за рухами і навіть поглядом людини, досконаліші алгоритми машинного навчання зроблять взаємодію з технікою зручнішою;
- На виробництві це може покращити швидкість та якість виготовлення товарів та послуг, змінити моделі бізнесу;
- Зростання взаємного рівня довіри у суспільстві;
- Зростання активності участі громадян у важливих суспільної політичних подіях та організаціях;
- Створення експертних мереж для розробки спеціалізованих проектів (державних замовлень), сприяючи в такий спосіб здійсненню реформ у різних сферах життєдіяльності суспільства (електронна освіта, електронна медицина, електронна комерція, тощо) на основі консолідації ресурсів представників усіх суспільних секторів, а також їх рівноправності.

Водночас скептики називають свої міркування про розвиток Інтернету речей [3]:

- Лише заможні люди зможуть «розважатися» повсякденними предметами, під’єднаними до Інтернету;
- Зниження розумових здібностей людства;
- Позбавлення недоторканості особистого життя і помешкання;
- Нові можливості завжди приносять нові виклики

Прикладами роботи Інтернету речей в сучасних умовах на підприємствах є:

1. високоточна система контролю пересування поїздів як під землею, так і на поверхні. Ця система забезпечує швидке та ефективне транспортне сполучення пасажирського та вантажного транспорту;

2. General Electric уже декілька років використовує концепцію Інтернету речей для спостереження за роботою їх реактивних двигунів. Величезна кількість різноманітних спеціалізованих сенсорів збирає понад 14 гігабайт оперативних даних за один політ. Ця інформація аналізується дослідницьким підрозділом компанії для того, щоб оптимізувати і

вдосконалити роботу двигунів. Така робота не тільки знижує вірогідність відмови двигуна, але й дозволяє подовжити його загальний термін служби і знизити витрати на ремонт та обслуговування;

3. Фахівці компанії Google вважають, що у недалекому майбутньому різноманітна техніка взаємодіятиме між собою, покращуючи якість повсякденного життя людей. Потенціал зазначеного ринку є дуже великим, а компанії, що працюють у даному напрямку, отримають величезні переваги порівняно з конкурентами.

Основна проблема переходу до практичного використання Інтернету речей у людей полягає у низці причин, серед яких: зміна ментальності, інше сприйняття речей та процесів реального світу; злам соціальних і культурних стереотипів; використання шаблонів відносно того, що нові інформаційні процеси – це винятково прерогатива молоді, або, що ІКТ є потенційно шкідливими для здоров'я; острах, що опанувати комп'ютерною грамотністю виявиться не до снаги; використання ІКТ здебільш у якості індустрії розваг, а не освітнього чи ділового ресурсу; недоступність інформаційних і комунікаційних послуг через їх високу вартість у багатьох країнах; незнання про можливості голосування електронним шляхом, заповнення офіційних документів та їх реєстрацію в режимі он-лайн, обмеження у поширенні купівлі та продаж товарів чи надання послуг через мережу Інтернет, отриманні освіти, консультацій, діагностики та лікування, юридичних послуг в електронному форматі тощо внаслідок особистих упереджень та стереотипів. Як стверджує автор: «Нині лише 10 % людства користується глобальною мережею Інтернет» [5].

Впровадження Інтернет-середовища у всі сфери життя людини потенційно може змінити багато навколишніх об'єктів, призвести до глобальних економічних, політичних і загальнолюдських трансформацій. Запровадження Інтернету речей в України у відповідних видах економічної діяльності дозволить значно скоротити відставання у економічному розвитку від передових індустріально розвинених країн світу.

Література:

1. Касьян В.І. Філософія. [Електронний ресурс] / В.І. Касьян. – 2008. - Режим доступу до ресурсу: http://pidruchniki.com/1584072014809/filosofiya /filosofiya
2. Тоффлер Е. Третья волна. [Електронний ресурс] / Е. Тоффлер // Москва: ООО «Фирма Издательство АСТ». - 2010. - Режим доступу до ресурсу: http://lib100.com/philosophy/tretya_volna/doc/
3. Геселева Н.В., Головач М.С. Інтернет речей як складова четвертої промислової революції / Н.В. Геселева, М.С. Головач // Ефективна економіка. - 2016. - Режим доступу до ресурсу: http://www.m.nayka.com.ua/?op=1&j=efektyvna-ekonomika&s=ua&z=5315
4. Баранов О. «Інтернет речей» як правовий термін / О. Баранов // Юридична Україна. - 2016. - № 5-6. - с. 96-103
5. Колодюк А. Проблематика переходу до інформаційного суспільства / А. Колодюк // Політичний менеджмент. - 2004. - № 6. - С. 129-137

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

Фещенко К. С.,
студент ФСП КПІ ім. І.Сікорського

«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 століття стало століттям якісних технологічних зсувів та значних наукових проривів.

Важко уявити, що мобільні телефони сучасного зразка з’явилися 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 опитування, 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. Окрім 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 сну, мотивацією та екологічним станом навколишнього середовища.

Отже, переваги Інтернету речей полягають в наступному:

- По-перше, це простота використання. Не потрібно бути комп'ютерним генієм, щоб вміти користуватися цими девайсами. Окрім того, ці речі полегшують життя людей з обмеженими можливостями та людей літнього віку.
- По-друге, Інтернет речей надає можливість керувати пристроями на відстані (якщо це бездротова мережа).
- По-третє, Інтернет речей провокує появу інноваційних методів виробництва та ведення бізнесу.

Проте, на нашу думку, важливо зазначити і негативні сторони швидкого розвитку такого явище, як Інтернет речей.

Кожна з таких «розумних» речей, які є складовими частинами, має датчики зчитування інформації, які підключено до Інтернету, а отже кожна

людина, яка використовує дані девайси може позбаватися недоторканості свого приватного життя.

Вагомим недоліком є також і вартість даних девайсів. За сучасної економічної ситуації, в Україні зокрема, такі пристрої будуть доступні лише меншості населення.

Комп'ютеризовані речі роблять наше життя простішим в будь-якій сфері використання. Овертон довів, що людей можна привчити до всього. І посилаючись на його дослід, можна людей привчити до всього [3].

Треба пройти лише декілька етапів: від заперечення до легалізації/впровадження.

Як би не намагалися бабусі сперечалися зі своїми онуками щодо розумної техніки, говорячи, що їхнє дитинство повинне промайнути на дитячому майданчику чи в бібліотеці, а не за цим залізним монстром, та все ж мережа Інтернет сьогодні є частиною нашого життя.

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 – Режим доступу до ресурсу:http://www.m.nayka.com.ua/?op=1&j=efektyvnaekonomika&s=ua&z=5315
3. Д. П. Овертон. Вікно Овертона: технологія знищення, або Як легалізувати що завгодно. Режим доступу до ресурсу: https://www.ar25.org/article/vikno-overtona-tehnologiya-znyshchennya-abo-yak-legalizuvaty-shcho-zavgodno.html

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

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

РОЗВИТОК ІНТЕРНЕТУ РЕЧЕЙ У СУЧАСНОМУ СВІТІ

В сучасну епоху Інтернет нерозривно пов'язаний з життям більшості людей. Ще в дев’яностих роках минулого століття в Україні ніхто не

замислювався над питанням: "Що ж таке Інтернет?". Помітно відрізняється ситуація в даний момент – кількість користувачів Інтернету зростає з кожним днем. З його допомогою виникло багато нових напрямів в економіці та соціальному житті людства. Одне з них – це Інтернет речей .

Інтернет речей - це провідна або бездротова мережа, що з'єднує пристрої, які мають автономне забезпечення, управляються інтелектуальними системами, забезпеченими високорівневою операційною системою, автономно підключені до Інтернету, можуть виконувати власні або хмарні додатки і аналізувати зібрані дані. Крім того, вони мають здатність отримувати, аналізувати і передавати дані від інших систем [1].

Термін "Інтернет речей" ("internet of things") вперше був сформульований ще у далекому 1999 році. Саме поняття являє собою цілу концепцію комунікаційної мережі об'єктів ("речей"), які мають технології для взаємодії між собою та з оточуючим середовищем. Крім того, вони покликані виконувати певні дії без втручання людини. Тобто всі пристрої у Вашому домі, в авто, на Вас самих обробляють інформацію, обмінюються нею та виконують різні дії в залежності від цієї інформації. Середовище роботи таких пристроїв не обмежується лише розумним будинком, воно може охоплювати навіть все місто. [2].

Експерти стверджують, що Інтернет речей є однією з найперспективніших технологій останніх років, що вже сьогодні фактично створює сотні нових продуктів і призводить до появи нових компаній на ринку, які диктують свої умови IT-гігантам. Ви можете не помічати, але Ви самі, ваші друзі чи колеги вже не перший рік користуються такими пристроями кожен день. Більше того, у чималій кількості українських домівок вже встановлені системи "розумного будинку", в які інтегровані десятки датчиків. [3].

Переваги інтернету речей, які вже доступні і які ще в процесі розробки можна краще продемонструвати на прикладах, тим паче, що сфер використання цієї технології чимало.

Українські споживачі знайомі приладами з концепції інтернету речей в першу чергу завдяки пристроям, які носять на тілі. Фітнес - браслети, смарт-годинники, "розумні окуляри", тощо. Для багатьох ці гаджети стали незамінними. Найбільш відомі - Jawbone і Fitbit, які слідкують за фазами вашого сну та активністю протягом дня, відстежують ритм серцебиття, Ваш раціон. Всі дані синхронізуються із власним додатком на смартфоні, плюс відмінно працюють зі сторонніми програмами.

Серія смарт-годинників Pebble та нещодавно представленні Apple Watch також мають своїх фанатів в Україні. Багато в чому вони повторюють функціонал фітнес-браслетів, однак мають більші можливості за рахунок операційної системи і більшому дисплею. Так чи інакше - пристрої, які ми носимо вже достатньо давно - не викликають подиву, а розвиток технологій, однозначно призведе до збільшення їх кількості безпосередньо на мешканцях нашої країни. [4].

Але, як відомо, існує дві сторони медалі. Інтернет речей несе в собі також негативні, небезпечні наслідки, а проникнення високих технологій в повсякденність приносить нові загрози. Якщо нещодавно активність зловмисників в мережі була аспектом інформаційної безпеки, то тепер під загрозою можуть перебувати життя і здоров'я людей. Поки це лише тривожні припущення, однак реальність вже зараз дає привід турбуватися про фізичну безпеку при взаємодії з такими пристроями.

Актуальний приклад — "розумні" автомобілі. Декілька років тому, автомобілі без водія були сюжетом письменників-фантастів, проте вже сьогодні автономні машини їздять по вулицях Гонконгу, Дубаї, ряду штатів США та деяких країн Європи. І ці автономні автомобілі іноді потрапляють в аварії: так, наприклад, широко обговорюваним стали випадки з летальним результатом в результаті збоїв у роботі автопілота Tesla. Хто в таких пригодах повинен брати на себе відповідальність - власник машини або виробник обладнання - невідомо. Навіть не беручи в розрахунок системи для автопілота, сучасний автомобіль буквально нашпигований різними

високотехнологічними модулями, датчиками і засобами управління, які мають дистанційне керування, в тому числі і через Інтернет. Все частіше з'являються новини про проблеми в автомобілях, не пов'язані безпосередньо з механізмами машини, а з програмним забезпеченням, безпека якого, як і у випадку з побутовими IoT-пристроями залишає бажати кращого. Причому стосується ця проблема самих різних виробників. Так, восени минулого року компанія General Motors була вимушена відкликати більше 3 мільйонів автомобілів у зв'язку з помилками в програмному забезпеченні.[5]

Наступним важливим питанням є приватність користувачів. Справа в тому, що «розумні» пристрої збирають величезну кількість інформації про своїх «господарів». Проконтролювати, що саме знають про власників пристрої і їх виробники, стає практично неможливо. В неприємному, але тим не менше все ще оптимістичному сценарії, ця інформація може продаватися рекламодавцям. Інша справа, що ця інформація може в якийсь момент стати здобиччю зловмисників. Дані, отримані з таких пристроїв, можуть надати максимально повний і докладний портрет користувача. [5]

Отже, Інтернет речей - це технологія, яка зазнає швидкого розвитку та у найближчому майбутньому здатна кардинально змінити світ. З розвитком 3G-мережі в Україні, кількість продуктів інтернету речей буде збільшуватись. Потенціал цієї сфери справді вражає, але вона несе в собі, як позитивні, так і негативні наслідки.

Література:

1. Леонід Черняк. Платформа Інтернету речей. Відкриті системи. СУБД, №7, 2012.

2. Дейв Еванс (Dave Evans) Інтернет речей: як зміниться все наша життя на черговому етапі розвитку мережі http://www.cisco.com/web/RU/ news/releases/txt/2011/062711d.html

3. Інтернет речей (Матеріал з Вікіпедії) – Режим доступу: URL-адреса: wikipedia.org/wiki

4. Інформаційна безпека Інтернету Речей – Режим доступу: URL:http://www.smileexpo.ru/public/upload/showsEvent/informational_security_in_iot_14266798614437_file.pdf

5. Електронний ресурс – Режим доступу:http://www.securitylab.ru/ blog/company/falcongaze/333687.php

Круц А. О.,
студентка бакалаврату.
Науковий керівник:
Мельник Б. Б.,

ОСОБЛИВОСТІ ЯВИЩА "ІНТЕРНЕТУ РЕЧЕЙ" В ОКРЕМИХ СФЕРАХ ЖИТТЄДІЯЛЬНОСТІ

На сьогоднішній день сучасне суспільство виглядає дуже прогресуючим. За допомогою багатьох технологій ми облегшуємо собі життя. Однією з цих технологій є «Інтернет речей». Цей термін бере початок з кінця 20 століття. Він був введений Кевіном Ештоном у 1999 році.

«Інтернет речей» («Internet of Things») – це мережа, в якій можуть взаємодіяти між собою усі прилади, якими ми користуємося щодня. [3] Обмінюючись даними, речі «спілкуються» один з одним. Це концепція комунікації об'єктів («речей»), які використовують технології для взаємодії між собою та з навколишнім середовищем. Також ця концепція передбачає виконання пристроями певних дій без втручання людини.

Інтернет речей може викликати величезні зміни у повсякденному житті, надавати звичайним користувачам абсолютно новий рівень комфорту. Але елементи такої системи мають бути захищеними, тому що замість користі вони можуть принести величезну шкоду. Тобто злочинці можуть отримати доступ до інформації про господаря, 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.[3] Це одне із найважливіших питань, що повинно турбувати нас стосовно прагнення використання цієї концепції.

Також, говорячи про Інтернет речей, ми не можемо залишити поза увагою сферу ІТ. Саме ця сфера займається виробленням технологій, завдяки яким Інтернет речей прогресує. Застарілі пристрої стають частиною Інтернет-мережі і виконують нові функції.[1] Програмісти займаються тим, щоб всі пристрої могли виконувати обробку інформації, її аналіз та обмін між собою та, залежно від результатів, приймати рішення і виконувати певні дії. Люди

сфери ІТ – люди, які творять майбутнє. Завдяки ним, світ навколо нас стає набагато зручнішим.

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.

Саме в 2008 році відбувся перехід від Інтернету людей до Інтернету речей. Кількість підключених до мережі предметів перевищила кількість осіб. З цих пір попит на цю концепцію не спадає, а навпаки - зростає. За прогнозами аналітиків, ринок Інтернету речей до 2019 року досягне більше 947 млрд.$.[4] Сама ж концепція припускає інтеграцію комунікаційного устаткування і різних пристроїв.

Зараз Інтернету речей приділяється високий ступінь уваги, тому через декілька років ми вже зможемо жити у комфортних умовах.

Лідерами у розробці та впровадженні Інтернету речей є країни, в яких розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів – це США, Китай та Південна Корея. Також значний прогрес у цій галузі демонструють європейські країни та Японія.[3] А в Україні кількість Інтернету речей збільшується з розвитком 3-G мережі. Запит на цю концепцію вже існує. Технології – на підході.[4]

Література:

1. НУЛП. Що таке Інтернет речей? [Електронний ресурс] / НУЛП // - Режим доступу до ресурсу: http://iot.lviv.ua/що-таке-інтернет-речей/
2. НТУУ КПІ. Що таке Інтернет речей і чому це важливо? [Електронний ресурс] /НТУУ КПІ// MikroTik. – 2016. – Режим доступу до ресурсу: http://mikrotik.kpi.ua/index.php/courses-list/iot/79-what-is-the-internet-of-things-and-why-is-it-important
3. Владимир Парамонов. Інтернет речей. [Електронний ресурс] /Парамонов В.// «Розумна» електроніка. – Режим доступу до ресурсу: https://www.turkaramamotoru.com/uk/Інтернет-речей-20010.html
4. Андрій Петруня. Інтернет речей. Новомодне захоплення чи технологія, що змінює світ? [Електронний ресурс] /Петруня А.// Економічна

правда – 2015. – Режим доступу до ресурсу: http://www.uipdp.com/articles/2015-06/03.html#top

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

Андрощук Г. О.,
завідувач лабораторії правового забезпечення розвитку науки і технологій НДІ інтелектуальної власності НАПрН України, к.е.н., доцент, консультант Комітету Верховної Ради України з питань науки і освіти

ІНТЕРНЕТ РЕЧЕЙ І ОХОРОНА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ: НОВІ ВИКЛИКИ

Термін "Інтернет речей" (IP) - (англ. Internet of Things, IoT), як відомо, був введений у 1999 р. Кевіном Ештоном з Массачусетського технологічного інституту (США). Концепція Інтернету речей полягала у використанні радіочастотних міток для оптимізації логістичних процесів, Офіційною появою IP вважають 2008—2009 р.р., коли кількість підключених до Інтернету пристроїв перевищила кількість населення нашої планети. Нині кількість підключених до Інтернету пристроїв (речей) у двічі перевищує кількість населення, а до 2020 року, згідно прогнозів, перевищуватиме в 10 разів [1]. Отже, Інтернет речей — це концепція підключення до Інтернету побутових пристроїв, які завдяки цьому можуть взаємодіяти один з одним або із зовнішнім середовищем, збирати корисні дані та на їх основі самостійно здійснювати дії та операції, без участі людини. Набуває поширення також термін всеохоплюючий, або всеосяжний інтернет (англ. Internet of Everything, IoE).

У січні 2017 року робочі групи Міністерства торгівлі США з питань Інтернет - політики і цифрової економіки заявили: ***«Як і в будь-якій технологічній галузі, можна очікувати, що патенти будуть відігравати ключову роль у розвитку IP, надаючи винахідникам стимул для розробки інноваційних пристроїв, виробничих процесів і інфраструктури. Більш***

того, деякі питання патентної політики можуть вплинути на розвиток IP - галузей», «Якість патентів» - ще одна критична проблема, особливо щодо судових розглядів, і середовище IP також може висунути проблеми при захисті патентів, оскільки її розподілений характер потенційно викликає питання про багатосторонню відповідальність за правопорушення [1].

Нещодавно, обговорюючи проблеми майбутнього інтелектуальної власності, Генеральний директор ВОІВ Френсіс Гарі зазначив: «Сьогодні, коли великі дані починають давати віддачу і коли ми переходимо до «Інтернету речей», генеруються колосальні масиви даних. Значна частина цих даних випадає за межі традиційних категорій системи інтелектуальної власності. Це - одна з причин, через яку дослідники все частіше вдаються до комерційної таємниці для охорони своєї передконкурентної лабораторної роботи» [2].

Патентні активи Інтернет речей. Масштаби і глобальне поширення IP в поєднанні з їх величезною ринковою вартістю і потенціалом означає, що нас чекає інтенсифікація патентування в середовищі IP. Вже зараз розглядаються патентні заявки, що стосуються IP - технологій, які зачіпають широке коло дисциплін: програмне забезпечення, пристрої і датчики, обладнання, мережеві з'єднання і протоколи зв'язку, безпеку і шифрування даних, управління енергетичними ресурсами, аналіз даних, призначені для користувача інтерфейси і додатки. Великі гравці галузі, такі як LG Electronics, Samsung, Qualcomm і IBM (які, до речі, володіють чотирма з перших п'яти патентів США, що містять у своїй назві фразу «Інтернет речей»), активно розширили свої портфелі IP-патентів. Згідно зі звітом LexInnova, розподіл IP - патентів не концентрується у жодного домінуючого гравця. Крім того, в звіті наголошується, що деякі відомі організації (патентні тролі), які не практикують в даній області - такі, як Interdigital і ETRI - також звертаються до IP - патентів, припускаючи, щов майбутньому тут з'являться великі шанси на подання патентних позовів [3]. IP-патенти зазвичай стосуються трьох сфер: 1) технічних характеристик кінцевих пристроїв для

збору даних або реагування на імпульси управління; 2) мережевих протоколів і комунікаційних систем; 3) додатків, що використовують зібрані дані. Кількість IP - патентів зростає в геометричній прогресії, що наочно проявилося в усе більш частому згадуванні словосполучення "Інтернет речей" в патентних заявках США, опублікованих в період з 2006 по 2015 роки. Серед виданих патентів США, тільки близько 350 включають в термін "Інтернет речей", причому близько 75% таких патентів припадає на 2015 рік. Проведене у Великобританії в ширшому масштабі дослідження показало, що з 2004 до 2013 роки майже 22 тис. опублікованих патентних заявок в усьому світі були орієнтовані на IP-технології та підключені до Інтернету "розумні" (smart) пристрої [3].

Роль держави у сприянні розвитку IP. Федеральна торгова палата (ФТП) США в січні 2015 р. опублікувала звіт про IP-простір, визначивши ризики для споживачів, які, зокрема, включають: 1)несанкціонований доступ і неправильне використання персональної інформації; 2)напади на інші системи; і 3) ризики для особистої безпеки. Опубліковані ФТП Принципи справедливої інформаційної практики (Fair Information Practice Principles (FIPPs) є керівними нормами, що представляють загальноприйняті уявлення про чесну інформаційну практику в електронному ринку. На запит «Переваги, проблеми і потенційна роль уряду в сприянні розвитку IP» Міністерством торгівлі США підготовлено відповідний документ, датований січнем 2017 року. У ньому визначаються ключові проблеми, що можуть вплинути на розгортання технологій IP, висвітлюються потенційні переваги і проблеми, а також роль, що відводиться Уряду США і, зокрема, Міністерству торгівлі, до складу якого входить Патентне відомство, у сприянні розвитку IP. Розглянуто проблеми охорони інтелектуальної власності у сфері IP взагалі і, зокрема, питання, що стосуються охорони авторських прав, патентів, комерційної таємниці і торгових марок [4]. Коротко охарактеризуємо їх основні положення з деякими коментарями.

Авторське право. Пов'язані з авторським правом питання IP стосуються володіння, доступу і використання даних, програмного забезпечення, а також кому належать дані в IP-середовищі і що з цим слід робити. Ставилось питання про те: а) як умови ліцензування можуть вплинути на характер взаємодії споживачів із захищеним авторським правом програмним забезпеченням, вбудованим в IP-пристрої; б) які рішення могли б дозволити споживачам користуватися копіями програмного забезпечення, вбудованого в куплені IP-пристрої. Відзначалася також важливість: а)недопущення ненавмисного підриву IP-політикою прав інтелектуальної власності; б) ослаблення встановлених методів ліцензування; в)дотримання відповідальної ролі авторського права в стримуванні контрафактних мобільних додатків за допомогою відмови від підроблених додатків, що можуть містити шкідливе програмне забезпечення.

Патенти (винаходи). У розвитку IP патенти відіграватимуть ключову роль. Забезпечуючи виключні права власності для творців технічних нововведень, винаходи стимулюють розробку нових IP-пристроїв, вдосконалення виробничої практики та інфраструктури. Деякі питання патентної політики можуть вплинути на розвиток IP-галузей в майбутньому. В процесі розробки в різних країнах IP-стандартів можуть виникати ті ж питання, пов'язані зі стандартизацією істотних патентів і ліцензуванням, що вже має місце в ІКТ- технологіях. Якість патентів - важлива проблема, яка привертає увагу зацікавлених сторін, особливо в зв'язку з судовими розглядами. Діючі в галузі конкуренти і представники громадськості повинні чітко розуміти, які функціональні можливості або дії охоплюються патентом, коли їм потрібно вдаватися до ліцензування або інших альтернативних заходів. Уряду рекомендовано активізувати протидію патентним тролям в цілях скорочення непривабливих патентних суперечок. Необхідне більш чітке формулювання вимог до патентоспроможності об'єктів у сфері IP. Патентним відомством США вже видано посібник для патентних експертів щодо того, як застосовувати відповідні рішення Верховного суду в процедурі

патентування. Розвиток IP загострює проблеми примусового застосування патентів. Наприклад, розподілений характер IP може викликати ряд питань, що стосуються відповідальності за «багатокористуватське правопорушення» (multi-party infringement liability). Іноді кілька осіб діють разом таким чином, що об'єднаний результат викликає патентні претензії. У таких ситуаціях у окремих патентовласників обмежуються можливості здійснення своїх прав - зокрема, оскільки Інтернет відкриває можливість невидимої ефективної взаємодії з декількома учасниками даного процесу.

Комерційна таємниця є конфіденційною, комерційно цінною інформацією, яка надає компанії конкурентні переваги, Вона може включати списки клієнтів, методи виробництва, маркетингові стратегії, інформацію про ціни і хімічні формули. В даному випадку мова йде про те, як розвиток IP впливає на захист комерційної таємниці. Секрети виробництва мають вирішальне значення для підприємств, що створюють і впроваджують інновації в IP-просторі. Поширення IP-пристроїв і з'єднань посилює вразливість комерційної таємниці. Значимість IP-продуктів буде оцінюватися не тільки їх великими даними, але і алгоритмами, які перетворюють ці дані в дії і, в кінцевому рахунку, впливають на споживача. Додаткові ризики виникають при спільному використанні даних в IP-середовищі без належного контролю за ненавмисним розкриттям конфіденційної інформації. Відповідно, захист комерційної таємниці є одним з ключових елементів стимулювання інновацій в IP-середовищі.

Торгові марки виконують кілька функцій для споживачів і власників торгових марок. Вони є індикаторами якості, а також сприяють встановленню відповідального за неякісний продукт. Використання відомих торгових марок (брендів) третіми особами, минаючи ліцензування, призводить до правових конфліктів, ймовірність яких істотно зростає в Інтернеті, де торгові марки стикаються з подібними знаками інших осіб, доменними іменами та іншими, ніде не зареєстрованими словесними позначеннями (посиланнями, фреймами, метатегами, а також з ключовими

словами в онлайновій рекламі). Згадані проблеми слід враховувати при прийнятті рішення про те, як найкращим чином використовувати бренди при поширенні нових IP - технологій.

В останні кілька років Міністерство торгівлі США опублікувало «Зелену книгу» (офіційний урядовий документ) Copyright Policy, Creativity, Innovation, and the Digital Economy. В ній представлено ретельний аналіз політики в галузі цифрового авторського права, що включає питання IP. Підготовлено також «Білу книгу» Remixes, First Sale, and Statutory Damages, яка зачіпає питання стандартів і функціональної сумісності в контексті онлайнової торгівлі. Надалі буде продовжена робота щодо сприяння позитивній еволюції системи інтелектуальної власності та її захисту в цифровій економіці. Україні необхідно використати досвід у цій сфері, накопичений іншими країнами.

Висновки. Основою Індустрії 4.0 є інформаційні засоби та технології в будь-якому їх прояві. В Україні інформаційні технології (IT) є провідним сектором економіки та суспільного життя, який забезпечує динамічний розвиток іншим галузям економіки. Це підтверджує той факт, що у світі IT – компанії є лідерами за кількістю патентів у Європі. Кількість IT-компаній в Україні складає понад 1000 одиниць та близько 100 науково-дослідних (Research & Development) центрів. За кількістю зайнятих спеціалістів у сфері IT (близько 100 тис.) та кількістю щорічних випускників з IT-спеціальностей (15 тис.) Україна є лідером серед країн Центральної та Східної Європи. За результатами 2016 р. ринок IT-послуг збільшився до 2,9 млрд доларів, що становить 4% ВВП країни. Україна продовжує займати лідируючі позиції по IT-фрілансу серед країн Східної Європи, контролюючи 33% ринку. За результатами 2016 р., 12 українських компаній потрапили в рейтинг 100 кращих постачальників послуг аутсорсингу. Галузь займає третє місце за рівнем експорту. У минулому році було надано послуг іноземним замовникам на 2,55 млрд доларів. З аналізу доповіді BOIB World Intellectual Property Report Breakthrough Innovation and Economic Growth [5] видно, що Україна входить

до 20 країн-лідерів за кількістю патентів у сфері революційних технологічних інновацій: 3-D друку (11 місце) і робототехніки (17 місце).

Інтернет речей IP є новою формою технологічного розвитку, яка трансформує зміст нашого життя і ведення підприємництва. Водночас, для повної реалізації потенціалу IP необхідно створити відповідну інфраструктуру, розробити політику і стратегію реагування на нові виклики. Ключовим завданням у всіх випадках стрімкого еволюційного розвитку є збереження справедливого балансу охорони інтересів трьох складових - фізичних осіб, бізнесу і держави. Слід зазначити, що в основі технологій, в сукупності складових IP, базується на програмному забезпеченні (ПЗ), правова охорона якого далека від досконалості. Можна зробити висновок, що за відсутності нормативно-правових основ функціонування інфраструктури IP найбільш важливим і складним завданням є визначення правового режиму інформації, що генерується в рамках IP, а також оцінка можливості поширення на неї прав ІВ. В результаті цього має з'явитися юридичний алгоритм розстановки пріоритетів в частині належності інформації таким суб'єктам, як користувачі, оператори IP, власники підключених пристроїв, власники виключних прав на програми для ЕОМ і треті особи (включаючи державних регуляторів). Ці питання мають стати предметом обговорення на парламентських слуханнях «Національна інноваційна система: стан та законодавче забезпечення розвитку», проведення яких заплановано на наступний рік.

Література:

1. Elena Holodny. Fourth Industrial Revolution great for lawyers // http:/// [Електронний ресурс]. — Режим доступу: - www.businessinsider.com/ **fourth-industrial-rev**....

2. Фрэнсис Гарри о будущем интеллектуальной собственности: возможности и проблемы [Електронний ресурс]. — Режим доступу: - http://www.wipo.int/wipo_magazine/ru/2017/05/article_0001.html

3. Special report: Will the Internet of Things need new patenting/licensing strategies? – *Dugie Standeford // Intellectual Property Watch, 3 April 2017* –[Електронний ресурс]. — Режим доступу: ip-watch.org› …special…internet-things…strategies/

4. Fostering the Development of the Internet of Things// THE DEPARTMENT OF COMMERCE, INTERNET POLICY TASK FORCE & DIGITAL ECONOMY LEADERSHIP TEAM [Електронний ресурс]. — Режим доступу: http:/ ntia.doc.gov›files/ntia…iot_green…01122017.pdf
5. World Intellectual Property Report Breakthrough Innovation and Economic Growth [Електронний ресурс]. — Режим доступу: http://www.wipo.int/edocs/pubdocs/en/wipo_pub_944_2015.pdf

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

Яшарова М. М.,
к. ю. н., доцент кафедри інформаційного права та права інтелектуальної власності КПІ ім. Ігоря Сікорського

НЕПРАВОМІРНЕ ВИКОРИСТАННЯ ЗАСОБІВ ІНДИВІДУАЛІЗАЦІЇ В УМОВАХ ІНТЕРНЕТ РЕЧЕЙ

Наразі в електронній торгівлі використовується засоби індивідуалізації в доменних іменах, що відіграють вагому роль у конкурентоспроможності товарів та послуг на ринку. Інформаційні технології сучасного світу дозволяють людству миттєво обмінюватися інформацією. Це означає, що суспільні відносини у цифровому середовищі гратимуть все більшу роль у житті людини.

Особливу увагу слід звернути на господарські відносини, які мають визначальний вплив на економіку. Знаки для товарів і послуг відіграють важливу роль у індивідуалізації та ідентифікації суб'єктів господарювання. Швидкість та легкість розповсюдження інформації у цифровому середовищі значно ускладнює захист від неправомірного використання таких об'єктів інтелектуальної власності.

Поширеним порушенням прав власників інтелектуальної власності є неправомірна реєстрація чи притримування назв доменів, тотожних чи подібних до існуючих знаків для товарів і послуг, з метою їх комерційного використання чи продажу законним власникам цих знаків. Така діяльність отримала назву «кіберсквотинг» — захоплення доменних імен. Використовуючи недосконаліть реєстраційної системи доменних імен,

кіберсквотери реєструють назви відомих знаків для товарів і послуг, фірмових найменувань, прізвища відомих людей без згоди їхніх власників. Оскільки реєстрація доменних імен є порівняно недорогою процедурою, кіберсквотери реєструють сотні доменних імен. Потім вони виставляють на продаж або пропонують ці імена безпосередньо компаніям-власникам знака або фірмового найменування за значні суми. Це прояв недобросовісної конкуренції у віртуальному світі. Власники цих позначень змушені для власного використання в Інтернеті купувати свої ж назви знаків для товарів і послуг[1] .

Отже, проблема порушення прав на засоби індивідуалізації розглядається, в основному, у контексті класичного кіберсквотингу, метою якого є продаж доменних імен власникам прав на торговельні марки. Слід зазначити, що протиправне використання знаків для товарів і послуг в Інтернет мережі має значно ширший характер, який проявляється також і в недобросовісній конкуренції. Існують наступні види кіберсквоттингу:

- «Брендовий кіберсквотинг» - реєстрація доменних імен, що містять товарні знаки, фірмові найменування.
- «Іменний кіберсквотинг» - аналог «брендового», реєстрація доменів популярних імен і прізвищ.
- «Галузевий кіберсквотинг» - реєстрація доменних імен, співзвучних або таких, що точно позначають галузі економіки, назви товарів або послуг. Володіння таким доменом дає ряд вагомих переваг, таких як прямий набір користувачем, брендовість і запам'ятовуваність. Саме галузева діяльність приносить кіберсквотерам найбільший прибуток.
- «Географічний кіберсквоттинг» - реєстрація доменів з територіальними назвами. У сфері туризму певний географічний домен може надати домінуюче положення у продажах туристичних путівок.

- «Тайпсквотинг» - реєстрація доменних імен, близьких за написанням з адресами популярних сайтів в розрахунку на помилку частини користувачів.
- «Захисний кіберсквотинг» - коли легальний власник популярного сайту (знака для товарів і послуг) реєструє всі доменні імена, близькі, співзвучні, схожі, пов'язані за змістом з його власним доменним ім'ям[2].

Порушення прав на засоби індивідуалізації можна поділити в залежності від суб’єктивної сторони такого правопорушення:

- використання торговельної марки у доменному імені з метою продажу домену власнику майнових прав на знак для товарів і послуг.
- використання торговельної марки у доменному імені в цілях недобросовісної конкуренції.

Перший випадок є найбільш розповсюдженим. Класичні кіберсквотери не ведуть жодної господарської діяльності, звинуватити їх у недобросовісній конкуренції складно, оскільки вони не використовують доменне ім’я для продажу товарів, або надання послуг. Суть у тому, щоб зайняти найвдаліші варіанти доменних імен, які б вказували на відповідну торгівельну марку та запропонувати продати їх власнику торгівельної марки. Така діяльність є досить прибутковою, оскільки не кожен правовласник ризикне витрачати час та кошти на судове вирішення спору. Дану ситуацію також ускладнює відсутність арбітражу за UDRP (Єдина політика виришення доменних спорів) стосовно національної зони .UA, та низька компетентність судів у питаннях інтелектуальної власності.

Недобросовісна конкуренція проявляється у перехопленні трафіку. Саме на це розрахований тайпсквоттинг. Перехоплений трафік може бути використаний для:

- продажу товарів з використанням торговельної макрки, яку очікує побачити користувач;

- продажу товарів аналогічних за призначенням (не використовуючи торговельну марку);
- завдання шкоди діловій репутації.

Останній випадок є найбільш небезпечним, оскільки метою є саме деструктивна діяльніть відносно гудвілу суб'єкта господарювання.

Слід також зазначити, що продаж товарів з використанням торговельної марки може здійснюватися і без використання знака для товарів і послуг у доменному імені. Така діяльність зустрічається у соціальних мережах, дошках оголошень, інтернет-магазинах.

Існують випадки, коли декілька компаній, які на законних підставах користуються однаковими торговими марками, але заявленими на різні класи товарів і послуг, не можуть зареєструвати їх у якості доменних імен, оскільки існування двох однакових доменних імен є технічно неможливим. У такому випадку тільки одна з компаній, яка звернулася із заявкою першою, може зареєструвати доменне ім'я, що відповідає її торговельній марки[3, с.77].

Проблема у тому, що кіберсквотер теж може зареєструвати торгівельну марку на інші класи товарів і послуг. Відповідно до Єдиної політики вирішення доменних спорів, сама собою реєстрація торговельної марки не створює законного інтересу. Яскравим прикладом є рішення Уповноваженого органу у справі Madonna Ciccone проти "Madonna.com", відповідач намагався довести наявність законного інтересу тим, що у нього була зареєстрована торговельна марка "MADONNA" в Тунісі. Однак Уповноважений орган всебічно дослідив усі подані докази та встановив, що відповідач не веде підприємницьку діяльність у Тунісі і реєстрація торгівельної марки не була здійснена з метою ведення бізнесу у цій країні[4, с.29].

Нестабільна фінансово-економічна ситуація в Україні також впливає на суспільні відносини у цій сфері, оскільки призводить до значного підвищення цін на доменні імена. Це завдає значного удару по кіберсквотерам, адже скуповувати доменні імена стає все складніше. З іншої

сторони, власники торгівельних марок втрачають можливість використовувати захисний кіберсквотинг.

У підсумку слід зауважити, що законодавча база України не встигає за рівнем становлення та розвитку технологій і реаліями життя, що актуалізує необхідність розробки відповідних нормативних актів для визначення порядку присвоєння доменних імен у мережі Інтернет. Наразі, важливою є профілактика таких правопорушень, оскільки кількість Інтернет речей до яких відносяться і засоби індивідуалізації, постійно зростає і відслідкувати неможливо, цим саме і користуються кіберсквотери тому, що зареєструвати доменне ім'я у мережі Інтернет простіше, ніж зареєструвати торговельну марку.

Література:

1. Максимова Н.Інтернет у законодавчому полі України// [Електронний ресурс] - Режим доступу:https://patent.km.ua/ukr/articles/i33
2. Энциклопедия кибersквоттинга // [Електронний ресурс] - Режим доступу: http://www.saferunet.org/adult/news/548/
3. Індивідуалізація учасників цивільного обороту, товарів та послуг у всесвітній мережі Інтернет /Т. Кузьменко//Юридичний вісник.-Одеса: Юридична література.-2012.-3 .-С. 79-82.
4. Доменні спори: міжнародний досвід та українські відмінності / А. Кравчук // Інтелектуальна власність. – 2012. – № 11. – С. 28─31 .
5. Закон України «Про захиствіднедобросовісноїконкуренції» від 07.06.1996 р. № 236/96-ВР. Режим доступу: http://zakon2.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80

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

Радейко Р. І.,
к.ю.н.,асистент кафедри адміністративного та інформаційного права Національного ніверситету «Львівська політехніка».

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ПРАВА НА ПРИВАТНІСТЬ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ «ІНТЕРНЕТ РЕЧЕЙ»

Сучасні інформаційні технології надають можливість користувачам керувати вимикачами, дверима, вікнами, жалюзями і температурою у житловому будинку чи офісному приміщенні. Ці технології називають

«Інтернет речей» (Internet of Things (IoT) [1, с. 96-103]. Їх застосування передбачає, що побутові прилади (будильник, кондиціонер), домашні системи (система садового поливу, охоронна система, система освітлення), датчики (теплові, датчики освітлення і руху) і «речі» (наприклад, деякі лікарські препарати) взаємодіють один з одним за допомогою комунікаційних мереж (інфрачервоних, безпровідникових) і забезпечують повністю автоматичне виконання процесів (вмикають кавоварку, змінюють освітленість, нагадують про прийом ліків, підтримують температуру, забезпечують полив саду, дозволяють зберігати енергію і контролювати її споживання) [8].

Однак існує небезпека порушення приватності життя людини через використання даних технологій. Так, у 2013 році, Федеральна торгова комісія США прийняла рішення у справі № 122-3090 про застосування санкцій до компанії TRENDnet Inc [10]. Ця компанія продавала IP-камери «SecurView», призначені для віддаленого контролю за житловими чи іншими приміщеннями. Через помилки в програмному забезпеченні, камери виявилися вразливими до хакерських атак, що дозволило зловмисникам перехопити відеопотоки з камер користувачів і опублікувати їх в Інтернеті. Загалом було опубліковано відео майже з 700 IP-камер. Коли в TRENDnet дізналися про цей недолік, то завантажили програмний патч на свій веб-сайт і спробували попередити своїх клієнтів про необхідність відвідування веб-сайту для оновлення програмного забезпечення своїх камер.

16 січня 2014 р. Федеральна торгова комісія США ухвалила рішення у справі № 122-3090, яким встановлено, що незадовільна практика діяльності компанії TRENDnet призвела до порушення приватного життя сотень споживачів при використанні IP-камер. Крім цього, у рішенні зазначалося, що «Компанія TRENDnet, її посадові особи, агенти, представники і співробітники, які діють безпосередньо або через будь-яку корпорацію, дочірню компанію, що належить або контролюється компанією TRENDnet, не повинні створювати прямих чи опосередкованих перешкод для

функціональної безпеки пристрою; безпеки, конфіденційності та цілісності інформації; права споживача на контроль будь-якої вхідної інформації, що зберігається, отримується чи передається за допомогою пристрою» [6].

Крім цього, компанію TRENDnet зобов'язали створити програму інформаційної безпеки для усунення загроз, які можуть призвести до несанкціонованого доступу до пристроїв або несанкціонованого використання пристроїв компанії, а також захисту конфіденційності та цілісності інформації, яка використовується, передається чи зберігається на пристроях. Компанія також повинна отримувати незалежну оцінку системи інформаційної безпеки кожні два роки протягом наступних 20 років.

Також компанія TRENDnet повинна повідомляти своїх клієнтів про проблеми забезпечення безпеки камер і про оновлення програмного забезпечення для виправлення неполадок і надання користувачам безкоштовної технічної підтримки у цих питаннях протягом двох наступних років [5].

У доповіді Федеральної торгової комісії США «Internet of things. Privacy&Security in a Connected World» (2015) [7] містяться рекомендації для розробників технологій «Інтерент речей», з метою забезпечення безпеки і ефективного захисту конфіденційності даних споживачів: формувати безпеку пристроїв на стадії проектування; інформувати співробітників щодо необхідності забезпечення безпеки на відповідному рівні в компанії; забезпечити безпеку пристроїв (деталей), отриманих від зовнішніх постачальників; коли виникають ризики для безпеки, застосовувати стратегію «поглибленого захисту», відповідно до якої кілька рівнів безпеки можуть використовуватися для захисту від конкретного ризику; розглянути заходи щодо недопущення доступу неавторизованих користувачів до пристрою, даних або особистої інформації споживача, що зберігається в мережі; слідкувати за підключенням пристрою протягом його терміну експлуатації, і де це можливо, надавати патчі для усунення можливих ризиків.

Укладачі доповіді також рекомендують компаніям розглядати мінімізацію даних, тобто обмежувати збір даних про користувачів і зберігати цю

інформацію лише протягом певного періоду часу, а не на невизначений термін. Мінімізація даних забезпечує два важливі аспекти конфіденційності: по-перше, зменшує ризик того, що компанія з великим сховищем даних може стати об'єктом хакерської атаки чи викрадення даних; по-друге, дані про споживачів можуть використовуватися способами, протилежними до очікувань їх власників.

Співробітники Федеральної торгової комісії США також рекомендують компаніям повідомляти споживачів та надавати їм відомості про те, як їх інформація буде використовуватися, особливо коли збір даних виходить за межі розумних очікувань споживачів технології «Інтернет речей». У той же час, представники американського регулятора закликають до подальшої співпраці у сфері саморегулювання в межах «Інтернету речей» з одночасним прийняттям системи забезпечення безпеки даних і застосування законодавства про конфіденційність.

Протягом 2015-2017 р. Європейська комісія як вищий орган виконавчої влади Європейського Союзу прийняла декілька важливих документів у сфері "Інтернету речей" «на благо європейських громадян і підприємств».

У травні 2015 р. ухвалено Стратегію єдиного цифрового ринку (Digital Single Market (DSM) Strategy [3]. У даному документів зокрема наголошується на необхідності уникнення фрагментації та сприяння забезпечення розвитку «Інтернету речей». Для реалізації положень цієї стратегії, Європейська комісія 19 квітня 2016 р. опублікувала робочий акт «Просування Інтернету речей у Європі» (Advancing the Internet of Things in Europe) [9], який є складовою частиною ініціативи «Оцифрування європейської промисловості» (Digitising European Industry (DEI) [4] та визначає основні засади розвитку «Інтернету речей».

У Європейській Комісії вважають, що головною проблемою для функціонування «Інтернету речей» залишається недовіра користувачів, не важливо для якого використавання: приватного, ділового чи урядового. У цьому аспекті безпека і захист персональних даних є першочерговим

завданням для успішного використання Інтернету речей. Незважаючи на те, що дана інформаційна технологія активно розвивається, випадки взлому об’єктів "Інтеренету речей" демонструють, що кількість атаках зростатиме експоненціально, якщо відомі вразливості будуть зберігатися.

Важлива проблема також пов’язана з безпекою аутентифікації. Мережеві пристрої, які обмінюються даними з іншими пристроями "Інтернету речей", повинні бути правильно автентифіковані для забезпечення безпеки даних. Це може зумовити використання зашифрованих каналів зв’язку. Крім цього, у Європейській Комісії вважають, що важливо сертифікувати мережеві пристрої, які б забезпечували мінімальний рівень безпечної аутентифікації, від апаратного рівня до цілісності мережі, для безпечної оброки даних і безпечного зв’язку пристроїв, якими передаються дані [2].

Слід враховувати, що "Інтернет речей" функціонує в реальному світі, тому збої в роботі, зумовлені відключенням або несправністю пристроїв, неминучі. Такі технічні неполадки створюють чимало юридичних ризиків. Правотворчим і правозастосовним органам різних країн необхідно вирішувати складні правові проблеми і визначити: хто є суб’єктом відповідальності за несправності підключеного пристрою або спричинені ним нещасні чи форс-мажорні випадки; хто відповідає за «витік» інформації за таких умов; яку відповідальність несуть компанії-розробники, посередники і споживачі?

В епоху стрімкого розвитку інформаційних технологій, традиційних правових засобів та інструментів вже недостатньо для вирішення проблем приватності. Однак, не варто відмовлятися від нових технологій, важливо вирішити питання регулювання, накопичення, зберігання, застосування і захисту даних про особу. Це дозволить використовувати потенціал і переваги інформаційних технологій для споживачів і одночасно мінімізувати ризики втрати безпеки та конфіденційності.

Література:

1. Баранов О. "Інтернет речей" як правовий термін / О. Баранов // Юридична Україна. - 2016. - № 5-6. - С. 96-103.
2. Advancing the Internet of Things in Europe Accompanying the document 19.4.2016 SWD(2016) 110 final [Electronic resource]. - Mode of access: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52016SC0110
3. Digital single market [Electronic resource]. - Mode of access: https://ec.europa.eu/commission/priorities/digital-single-market/.
4. Digitising European Industry [Electronic resource]. - Mode of access: https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry.
5. FTC Approves Final Order Settling Charges Against TRENDnet, Inc. [Electronic resource]. - Mode of access: https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.
6. In the Matter of TRENDNET, INC., a corporation. AGREEMENT CONTAINING CONSENT ORDER FILE NO. 122 3090 [Electronic resource]. - Mode of access: https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetorder.pdf
7. Interner of things. Privacy&Security in a Connected World (2015) [Electronic resource]. - Mode of access: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
8. Neil Gershenfeld, Raffi Krikorian, Danny Cohen. The Internet of Things. Scientific American, Oct, 2004 [Electronic resource]. - Mode of access: http://fab.cba.mit.edu/classes/S62.12/docs/Cohen_Internet.pdf
9. Staff Working Document: Advancing the Internet of Things in Europe [Electronic resource]. - Mode of access: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe
10. TRENDnet, Inc., In the Matter of. FTC MATTER/FILE NUMBER: 122 3090 [Electronic resource]. - Mode of access: https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter

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

Німко А. В.,
студент бакалаврату
Національного юридичного
університету ім. Ярослава Мудрого

ЗАХИСТ ПУБЛІЧНОЇ ІНФОРМАЦІЇ В УМОВАХ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ «ІНТЕРНЕТУ РЕЧЕЙ»

Вступивши в шостий технологічний уклад, людство відчуває, як кожного дня звичний стиль життя, побут поступово зазнають змін, які пов’язані з невпинною автоматизацією, скороченням потреб у прикладанні фізичних та

інтелектуальних зусиль для досягнення різноманітних цілей у сферах транспорту, освіти, промисловості, сільського господарства, інфраструктури тощо. Прогноз того, як швидко й у що саме технології перетворять світ навколо, може бути обмежений хіба-що тільки фантазією: складно уявити, що буде наприкінці цієї науково-технологічної революції, якщо при тому, що вона тільки розпочалась, ми вже бачимо кардинальну різницю між власним стилем життя 5- 10 років тому і тим, яким він є зараз.

За передбаченням авторитетного футуролога Реймонда Курцвела, вже в 2022 році найрозвинутіші країни Європи та Америки почнуть приймати нормативно-правові акти, що матимуть на меті регулювання відносин між людьми та роботами. Останні, в свою чергу, мають усунути потребу у створювені робочих місць для виконання важкої фізичної праці, оскільки вона буде повністю автоматизована[1; 377]. Такі задачі перед законодавцем України постануть, скоріш за все, трішки пізніше, через те, що науково-технологічні розробки на початку свого виходу на ринок є дуже дорогими продуктами, й, передбачувано, що в більшості українців буде недостатньо коштів для їхнього придбання. Тим не менш, не викликає сумніву, що швидкість розвитку цієї галузі прикладної науки невдовзі забезпечить доступність нових гаджетів для більшості людей планети, докорінно змінивши соціальні зв'язки і, відповідно, суспільні відносини. Для різних правових систем це стане справжнім викликом. Серед технологій, які привносять у життя людини, разом із комфортом, певні ризики, є «Інтернет речей» (Internet of things). Об'єднані в одну систему, електронні носії швидше збирають та обробляють різного роду інформацію, формуючи її в групи, щоби використовувати для спрощення людської життєдіяльності, а в випадку, коли один носій легко координує з іншим, створюється ситуація, коли є можливість витоку важливої інформації в небезпечне русло. Наприклад, вірус Petya.A, який нещодавно атакував комп'ютери світу, і завдав найбільшої шкоди саме Україні: за даними компанії ESET, у нас відбулося 75, 25% із усіх атак [2]. Як наслідок - знищені дані на 13 тисячах вітчизняних

ПК, порушене нормальне функціонування банківської системи: як вказав НБУ, 30 банків України зазнали безпосередньої шкоди від вірусу[3].

Якщо розглядати отриману гаджетами інформацію , які її самостійно збирають, обробляють і використовують у цілях конкретної ососби, як плід речі, то згенеровані дані є об'єктом права власності володаря певного технологічного продукту, і він самостійно несе ризик їхнього випадкового знищення чи пошкодження. У світлі цих аргументів, не виникає сумніву, що захистом від подібної ситуації повинні стати особиста технічна грамотність українців, що працюють за комп'ютерами та зацікавлені в збереженні своєї важливої інформації. Однак що робити у випадку, коли об'єктом хакерської атаки стає база даних НБУ чи іншої державної установи або організації, нормальне функціонування якої з тими даними, які акумулюють спеціальні служби, становлять публічний інтерес і їхня втрата може завдати непоправної шкоди? У даному випадку надзвичайно гостро постає необхідність створення ефективних механізмів захисту відповідних носіїв інформації – організаційних, правових та матеріально-технічних основ діяльності технологій «Інтернету речей» там, де їхнє безпечне функціонування становить суспільний інтерес. На мою думку, вирішення проблеми убезпечення надважливих даних від несанкціонованого доступу полягає не тільки в придбанні/створенні достатньо високотехнологічного устаткування, яке міститиме стійкі запрограмовані системи захисту - криптографічні алгоритми, - вони також повинні бути віднесені СБУ до відомостей, що становлять державну таємницю, задля попередження зламів цих систем. Як додатковий спосіб гарантування стабільності функціонування приладів у цій сфері, повинен бути нормативно введений механізм загальнообов'язкового страхування відповідних технологічних продуктів, що зменшуватимуть ризики їх пошкодження чи втрати.

Організаційна основа охорони даних повинна проявитися в високій компетентності щодо обережного поводження з інформацією, що становить суспільний інтерес, і приладами, які її збирають та обробляють. Тут важливе

місце належить не тільки Кіберполіції, роль якої, безсумнівно, все зростатиме, а й абсолютно всім працівникам публічних установ, чия діяльність є прямо й опосередковано пов'язаною з тими технологіями, які збирають та обробляють публічну інформацію. Такі люди повинні по-новому, відповідно до теперішніх матеріально-технічних умов праці і ризиків, пов'язаних із виконанням своїх службових обов'язків, усвідомити значення належного поводження з устаткуванням. Для цього я пропоную ввести на рівні відповідного галузевого законодавства вимогу обов'язкових спеціальних тренінгів для підвищення кваліфікації у сфері кібербезпеки, зміст яких повинен постійно оновлюватись із поточним розвитком технологій, для усіх працівників, які виконують роботу з підвищеною відповідальністю щодо публічних даних.

На перетині організаційної та матеріально-технічної основи забезпечення захисту публічної інформації в умовах використання «Інтернету речей», слід відвести важливе місце для стимулювання розробки інноваційних технологій українськими вченими. З метою створення сприятливого клімату для їхніх стартапів із можливістю подальшої комерціалізації, вважаю за потрібне внести пропозицію оновити законодавство України про інноваційну діяльність, ввівши особливий полегшений порядок оподаткування стартапів. У світлі початку шостого технологічного укладу, урядам країн, на мою думку, слід приділити значну увагу показнику Bloomberg, що відображає глобальний індекс інновацій. На жаль, він є невтішним стосовно України: вона на 42 місці з 50 можливих[4]. Це свідчить, що для нас важливо встановити належні умови для підтримання інноваційних починань українців, які часто через складність комерціалізувати свої розробки, шукають відповідні перспективи за кордоном. Таким чином, Україна втрачає інноваторів, які могли би забезпечувати вітчизняну як публічну, так і приватну сферу новими високотехнологічними розробками за відносно доступнішою ціною, ніж коли вони придбанні з-за кордону.

На моє переконання, для досягнення мети максимального зниження ризиків із використання сучасних технологій в управлінській сфері, повинні бути прийняті нові нормативно-правові акти, що міститимуть вимоги до технологічного рівня самого приладу, який використовується в системі з іншими, збираючи й обробляючи публічну інформацію, правила поводження з цими об'єктами працівників публічних установ та організацій, закріплений список професійних навиків, які потрібні для безпечного поводження з технологіями «Інтернету речей», особливий порядок добору кадрів, які обслуговуватимуть відповідні прилади .

Отже, законодавство з питань захисту публічних даних, в умовах використання «Інтернету речей», не можна буде прийняти остаточно і розраховувати на універсальність його положень для тривалого періоду часу, бо технології будуть модернізовуватись в експоненціальному типі розвитку, що обумовлене темпом науково-технологічної революції 21 століття. У даному випадку, потрібно налаштуватись на гнучке нормотворення, для якого буде властива велика кількість імперативних норм, покликаних вбезпечити від ризиків дані, що становитимуть публічний інтерес, і, що не менш важливо, з одночасним створенням сприятливого клімату для розробки українськими науковцями інноваційних продуктів, розповсюдження яких на світовому ринку товарів та послуг зможе влити в Державний бюджет України кошти й підняти її авторитет на міжнародному просторі співпраці найрозвинутіших країн.

Література:

1. Ray Kurzweil «The Singularity Is Near: A True Story about the Future» [Електронний ресурс] // Viking. – 2005. – С. 377 – Режим доступу до ресурсу: http://hfg-resources.googlecode.com/files/SingularityIsNear.pdf.

2. PETYA Ransomware Outbreak [Електронний ресурс] // ESET, spol. s r. o.. – 2017. – Режим доступу до ресурсу: https://www.eset.com/ us/about/ newsroom/corporate-blog/petya-ransomware-what-we-know-now/.

3. НБУ «Банки посилять власну інформаційну безпеку та співпрацю з протидії кіберзагрозам» [Електронний ресурс] // Офіційне інтернет представництво НБУ. – 2017. – Режим доступу до ресурсу:https://bank.gov.ua/ control/uk/publish/article?art_id=51479152&cat_id=55838.

4. Bloomberg «These Are the world's Most Innovative Economies» [Електронний ресурс] // Bloomberg Markets. – 2017. – Режим доступу до ресурсу: https://www.bloomberg.com/news/articles/2017-01-17/sweden-gains-south-korea-reigns-as-world-s-most-innovative-economies.

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

Головко М. Б.,
к.ю.н.,доцент кафедри кримінального права правосуддя ЧНТУ(ННІ права та соціальних технологій.
Юрченко Д. П.,
студентка юридичного факультету ЧНТУ (ННІ права та соціальних технологій).

ДО ДЕЯКИХ ПИТАНЬ ПРАВОВОГО РЕГУЛЮВАННЯ ІНТЕРНЕТУ РЕЧЕЙ

Сфера «розумних технологій» давно перестала бути перспективою майбутнього. Інтернет речей поступово проникає в наше життя, стаючи звичним, буденним явищем для людей. Відомий вчений Д. Еванс дав достатньо просте та якісне визначення: «Інтернет речей» (далі - IP) - це момент, коли до мережі Інтернет пристроїв і об'єктів підключено більше, ніж людей [1]. В огляді, зробленому під егідою Інтернет-співтовариства (The Internet Society, ISOC), дано таке визначення: Інтернет речей – це використання можливостей обчислювальної техніки та підключення до мережі Інтернет об'єктів, датчиків і побутових предметів (пристроїв), які не належать до звичайних комп'ютерів, що дозволяє цим пристроям забезпечувати генерацію, обмін і використання даних з мінімальним втручанням людини [2]. Таким чином, до IP відносяться технічні пристрої, які підключені до мережі Інтернет та самостійно обмінюються даними й інформацією з іншими подібними пристроями з метою виконання певних завдань.

Радою з архітектури Інтернету (Internet Architecture Board, IAB) в RFC 7452 було запропоновано свій варіант дефініції терміна «IP» - це тенденція, при якій велика кількість вбудованих пристроїв використовує комунікаційні послуги, основані на Інтернет-протоколах (IP – протокол). Багато з цих при-

строїв, які часто називають «розумні об’єкти», безпосередньо не керовані людьми, а функціонують як складові компоненти в будівлях або транспортних засобах або в інших об’єктах навколишнього середовища існування людини [3]. На думку, С. Халлера, IP пов’язаний з інтеграцією фізичного світу з віртуальним світом Інтернету. К. Еберсолд і Р. Гласс вважають, що основною філософією IP є бажання зробити об’єкти, які повсякденно оточують нас, повністю взаємопов’язаними для забезпечення ефективної взаємодії людини з людиною, людини з річчю, речі з річчю або машини з машиною [4].

Е. Бербрі досліджував поняття IP в юридичному аспекті, на його думку, «IP» - мережа мереж, яка дозволяє ідентифікувати цифрові юридичні особи та фізичні об’єкти, безпосередньо і однозначно, за допомогою стандартизованих і уніфікованих систем електронної ідентифікації і бездротових мобільних пристроїв, і, таким чином, робити можливим отримання, зберігання, передачу та обробку даних, які їх стосуються, без розриву між фізичними і віртуальними світами [5].

З огляду на вищезазначені доктринальні визначення, можна зробити висновок, що IP – це глобальна інфраструктура Інтернет, що надає можливість дистанційної взаємодії речей та людей, сукупність взаємодіючих технічних систем і комплексів, що складаються з мікропроцесорів, сенсорів, пристроїв передачі даних, локальних та/або розподілених обчислювальних ресурсів і програмних засобів, призначених для реалізації суспільних відносин, в 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). Тобто по суті IP – глобалізація всього суспільно-побутового життя людей, наділення речей «штучним інтелектом». Наприклад, «розумний будинок» завдяки вмонтованим сенсорам знає не лише, наскільки тепло в різних приміщеннях, а знає також в яких саме кімнатах знаходяться люди, як вони пересуваються, що роблять. А оскільки такі будинки оснащені приладами, які «самі навчаються» та веб-технологіями, вони можуть

«вирахувати» місцезнаходження своїх мешканців навіть за межами будинку – завдяки смартфонам. Чи приміром широко розповсюджуються додатки, за допомогою яких можливо управляти деякими речами побуту через смартфон, будучи віддаленими від них. На сьогодні список розумних речей швидкими темпами поповнюється: розумний годинник приймає та відправляє кореспонденцію, може слугувати в якості телефону й фітнес-тренера, аналізує вхідні повідомлення та пропонує, як на них відповісти; розумний плеєр – вміє підбирати музику в залежності від вподобань власника і періоду доби, пропонує ознайомитися зі схожими композиціями і робить це для окремого користувача, який до нього підключається; «розумний будинок» - система, що повністю аналізує та оптимізує процес управління житлом користувача; IP для медицини - для діагностики вже застосовуються методи теле-медицини, коли є зв'язок з лікарем, поліклінікою або лабораторією, що знаходиться в іншому районі [6, с. 140]. Розроблені протези кінцівок, керовані за допомогою сигналів мозку людини. Існують бездротові, які дозволяють паралізованим пацієнтам керувати телевізорами, комп'ютерами та інвалідними візками [7].

Але слід зазначити, що внаслідок такої інформаційно-технічної еволюції виникають досить проблемні питання. По-перше, людина стає вразливою: під загрозу потрапляє приватність, конфіденційність життя і здоров'я людей. По-друге, достатньо розвинута система правового регулювання IP-технологій сьогодні, на жаль, відсутня.

Проблема в тому, що в пам'яті пристроїв та засобів наявний значний масив персональних і особистих даних як фізичних осіб, так і окремих підприємств, установ та організацій. У наш час багато пристроїв вже мають датчики, що дозволяють збирати інформацію про фізичний світ і людину – камери, гіроскопи, акселерометри, термометри, пристрої розпізнавання мови. Активне використання гаджетів, що забезпечують інформаційну взаємодію, призводить до того, що за допомого Інтернет - технологій можна стежити практично за кожним куточком і за кожною подією в світі, збирати різні

персональні дані [8]. Це дозволить будь-якому кібер-злочинцю під'єднатися до мережі домашніх пристроїв особи і відслідкувати будь-які, в тому числі й приватні питання, що його цікавлять. Також зростає велика вірогідність постійного спостереження за життям громадян урядовими та неурядовими агенціями. Реальними також стають і злочини проти власності, життя та здоров'я особи з використанням ІР. Тепер, щоб вбити людину достатньо розігріти газовий котел опалення через Інтернет, до такої температури, щоб він міг вибухнути. Викрасти машину можна через додаток автозапуску, вимкнувши сигналізацію. Такі злочинні дії є наслідком використання ІР.

Варто погодитись з думкою Баранова О., що «інтернет речей» — це сукупність 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) [9, с. 101].

Важливого значення набуває розгляд ІР в юридичному та правовому аспекті, що передбачає здійснення правового регулювання всіх процесів пов'язаних з «розумними технологіями». На нашу думку, слід вже сьогодні приділити велику увагу вдосконаленню чинних правових норм та нормативно-правових актів, щодо регулювання суспільних відносин у сфері ІР, а також розробити систему організаційно-правових заходів для попередження правопорушень з використанням «розумних технологій».

Отже, ІР – це сукупність 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 (фізичних або юридичних осіб).

Безперечно сфера застосування мережі Інтернет та «розумних технологій» забезпечує реалізацію волевиявлення суб'єктів суспільства та у рамках техніко-технологічних можливостей задовольняються інформаційні, економі-

чні, суспільні та інші потреби. Поряд з тим, існування цієї мережі породжує проблеми, для вирішення яких необхідна сукупність технічних та організаційно-правових заходів, що здійснюються спеціально уповноваженими суб'єктами.

На нашу думку, слід розробити масштабну систему захисту пристроїв, які є носіями приватних та особистих даних фізичних та юридичних осіб. В аспекті правового регулювання важливо, на наш погляд, приділити увагу питанням кримінально-правової охорони життя, здоров'я, майна особи від злочинних посягань з використанням технологій «IP». З цією метою вбачається за необхідне розробити та прийняти відповідні зміни до Кримінального кодексу України та проект Закону України «Про основні засади забезпечення кібербезпеки України», який повинен стати регулятором забезпечення і гарантом безпеки використання «IP» та мережі Інтернет загалом у спільному житті людей.

Література:

1. Інтернет речей [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9.

2. Evans D. The Internet of Things. How The next Evolution of the Internet Is Changing Everything. CISCO white paper . – 2011. – P. 11 [Електронний ресурс]. – Режим доступу: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

3. Rose K., Eldridge S.,Chapin L. The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World. – The Internet Society (ISOC), October 2015. – 50 P. [Електронний ресурс] – Режим доступу: https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-2015.

4. Architectural Considerations in Smart Object Networking. – Internet Architecture. Category: Informational. – March 2015. [Електронний ресурс]. – Режим доступу: http://www.rfceditor.org/rfc/rfc7452.txt.1015%E2%80%936/ 2016%C3%92%C3%8E%C3%97%C3%8A%C3%80.

5. Haller, S. The Things in the Internet of Things. Poster paper presented at Internet of Things Conference. Tokyo, Japan. – 2010 [Електронний режим]. – Режим доступу: http://www.iot2010.org.4/.

6. Е-будущее и информационное право / В.Брыжко, А.Орехов, О.Гальченко; ред. ю.н., проф. Р.Калюжного и д.э.н, проф. Н.Швеца. – К.:Інтеграл, 2002. – 264с.

7. Как технологи будут выглядеть через пять лет [Електронний ресурс]. – Режим доступу: http://igate.com.ua.

8. Интернет вещей: чем угрожает будуще [Електронний ресурс]. – Режим доступу: http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee.

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

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

Костенко А. О.,
аспіран кафедри адміністративного права юридичного факультету Київського національного університету імені Тараса Шевченка

ПРАВО НА ДОСТУП ДО ІНТЕРНЕТУ І ПРАВА, ПОВ'ЯЗАНІ З ІНТЕРНЕТОМ РЕЧЕЙ: ПРОБЛЕМА СПІВВІДНОШЕННЯ

Окрім Інтернету, функціонування і розвиток якого зумовлює чисельні дискусії щодо меж прав і свобод приватних осіб в інтернет-сфері, а також щодо відповідальності цих осіб за свої дії в інтернет-просторі, відносно самостійним і не менш проблемним феноменом є Інтернет речей. Однією з ключових проблем правового регулювання та впровадження Інтернету речей є необхідність вирішити питання юридичного визначення, обґрунтування і закріплення відповідних прав приватних осіб щодо Інтернету речей. Важливість цього пояснюється тим, що введення Інтернету речей в полі правового регулювання потребуватиме оперативного визначення як заборонених, так і обов'язкових проявів поведінки у сфері його поширення і використання, зокрема з точки зору гарантування кібербезпеки [1]. Однак вважаємо, що цьому має передувати визначення змісту права приватних осіб щодо Інтернету речей, що має стати орієнтиром для наступного процесу - формулювання заборон і обов'язків. В якості аналогії, яка пояснює таку позицію, слід вказати, що заборона на вбивство людини, як і вимога до поваги чужого життя, випливає з права людини на життя, а не навпаки. Адже, як стверджується в науці, саме права людини є мірилом розвитку права в суспільстві і показником його цивілізованості, а також дають людині

можливість долучитися до матеріальних і духовних благ суспільства [2, с. 49].

Концепція «Інтернет речей» (англ. «Internet of Things») переживає своє становлення, зокрема в Україні. Інтернет речей, зараз, є більш новітнім і маловивченим феноменом, аніж сам Інтернет, та відноситься більшою мірою до галузі техніки, оскільки основою Інтернету речей є саме технічні пристрої, здатні обмінюватися інформацією. О. А. Баранов влучно стверджує, що є цілком необхідним формулювання дефініцій технократичних термінів з позицій права з одночасним збереженням технологічної сутності описуваних явищ [3, с. 96]. Відповідно, коректне юридичне розуміння Інтернету речей повинне охоплювати, з одного боку, ідею про те, що в основі користування Інтернетом речей лежить користування відповідними технічними системами (локально розміщеними комплексами взаємно пов'язаних пристроїв, датчиків, засобів зв'язку тощо) як об'єктами права власності, а з іншого боку – враховувати те, що таке користування потребує доступу до Інтернету.

В першу чергу необхідно обрати найбільш коректне формулювання ключового права приватних осіб у сфері використання Інтернету речей. В якості найближчої аналогії, на першу думку, спадає загальновідоме право на доступ до Інтернету. Однак побудоване за цією аналогією формулювання «право на доступ до Інтернету речей» вважаємо дещо некоректним через те, що категорії «Інтернет» та «Інтернет речей» позначають відмінні за своїм обсягом і характером феномени. Так, Інтернет за різними підходами може розумітися і як інформаційно-комунікаційна система, утворена сукупністю мереж різних рівнів (технічний підхід), і як інформаційний онлайновий простір, зумовлений функціонуванням відповідних комп'ютерних мереж (просторовий підхід). У зв'язку з цим у попередніх дослідженнях з цієї тематики нами вже зверталася увага на те, що формулювання «право на доступ до Інтернету» потребує трансформації у «право на доступ до Інтернету та перебування в ньому» [4, с. 432].

Що ж стосується Інтернету речей, то спільною ідеєю різних поглядів на його сутність є те, що вимагається залучення різноманітних технічних пристроїв, які взаємодіють між собою, з людьми чи з навколишнім середовищем, виконують конкретні завдання, а також при цьому підключені до Інтернету, за рахунок чого їх можливості та цінність значно зростають (наприклад, виклик негайної допомоги у випадку фіксування натільним датчиком факту падіння літньої людини [5]). Відповідно, формулювання «право на доступ до Інтернету речей» мало б означати, що приватна особа має право користуватися Інтернетом речей як чимось вже створеним і запущеним, як чимось зовнішнім і незалежним від неї. Однак користування Інтернетом речей на практиці означає не лише можливість доступу, а й розробки власних технологічних рішень (наприклад, власних «розумного кабінету», «розумної кухні», «розумного будинку» тощо) з їх наступним підключенням до Інтернету і налаштуванням. Тобто основу правовідносин, пов'язаних із взаємодією приватної особи з Інтернетом речей, нерідко складають саме правовідносини власності, і їм найбільше відповідає законодавчо закріплене право власника володіти, користуватися і розпоряджатися належним йому майном на власний розсуд і незалежно від місцезнаходження цього майна (статті 317, 319 Цивільного кодексу України) [6].

Тому пропонується розглядуване право розуміти як «право на впровадження Інтернету речей і взаємодію з ним», в якому слід розрізняти такі внутрішні складові (правомочності):

- право на впровадження Інтернету речей, тобто створення необхідних технічних систем (які водночас є майном), які будуть використовувати необхідні можливості Інтернету для виконання запланованих завдань (функцій);
- право на взаємодію з Інтернетом речей, яке складається з таких прав як володіти, користуватись і розпоряджатись створеними власноруч чи придбаними технічними системами, так і добросовісно користуватись чужими технічними системами;

- право на доступ до Інтернету та перебування в ньому, яке хоч і є самостійним суб'єктивним правом, але в даному контексті з логічною необхідністю виступає однією з правомочностей права на впровадження Інтернету речей і взаємодію з ним.

Відповідно, співвідношення права на доступ до Інтернету і права на впровадження Інтернету речей і взаємодію з ним пропонуємо розуміти як співвідношення частини і цілого. Це можна пояснити наступним чином. Право на доступ до Інтернету як мінімум передбачає можливість будь-яким чином взаємодіяти з елементами інфраструктури Інтернету, а саме: відвідувати веб-сайти, отримувати доступ до розміщених на серверах файлів, здійснювати інші можливі технічні дії в мережі тощо. В цей же час право на впровадження Інтернету речей і взаємодію з ним передбачає не лише можливість онлайн-взаємодії з елементами інфраструктури Інтернету, а й можливість налагоджувати цілий комплекс фізичних пристроїв, які будуть функціонувати в «матеріальному» світі (офлайн) та водночас будуть ідентифіковані як елементи інфраструктури Інтернету (онлайн). Тобто це право є значно ширшим і більш складним за своєю природою, ніж право на доступ до Інтернету, і його реалізація практично завжди вимагає реалізації у своєму складі права на доступ до Інтернету.

Вважаємо, що запропоноване розуміння права на впровадження Інтернету речей і взаємодію з ним як єдності трьох правомочностей якісним чином сприятиме визначеності відповідного суб'єктивного права приватних осіб, що має братися до уваги при розбудові системи правового регулювання Інтернету речей. Однак всі питання прав людини у сфері взаємодії з Інтернетом речей такою постановкою проблеми повністю не вирішуються. Так, залишаються недослідженими деякі проблеми захисту приватності та гарантування інших прав і законних інтересів приватних осіб, які виникають у зв'язку із залученням пристроїв у повсякденне життя (наприклад, розміщення у приватних помешканнях), частина з яких можуть збирати дані (аудіо-, фото- та відеоспостереження) та водночас є підключеними до Інтернету.

Література:

1. Інтернет речей: друг чи ворог? / Незалежна асоціація банків України. – [Електронний ресурс]. Режим доступу: http://anticyber.com.ua/article_detail.php?id=106
2. Загальна теорія права: Підручник / За заг. ред. М.І. Козюбри. – К.: Ваіте, 2015. – 392 с.
3. Баранов О.А. «Інтернет речей» як правовий термін / О.А. Баранов // Юридична Україна. – 2016. – № 5-6. – с. 96-103.
4. Костенко А.О. Право на доступ до Інтернету: необхідність належного юридичного закріплення / А.О. Костенко // Альманах права. Право і прогрес: складові забезпечення в сучасних умовах. – Випуск 7. – К.: Ін-т держави і права ім. В. М. Корецького НАН України, 2016. – с. 429-433.
5. Бондарев О. Лекторій. Що таке інтернет речей і навіщо він потрібен? [Електронний ресурс] Режим доступу: http://nv.ua/ukr/science/lectures/lektorij-shcho-take-internet-rechej-i-navishcho-vin-potriben-1326653.html
6. Цивільний кодекс України : від 16.01.2003 № 435-IV [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/435-15

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

Кравчук О.О.,
д.ю.н., доцент, зав. кафедри господарського та адміністративного права КПІ ім. Ігоря Сікорського

ІНТЕРНЕТ РЕЧЕЙ І СУЧАСНІ СИСТЕМИ АВТОМАТИЗОВАНОГО ПРИЙНЯТТЯ РІШЕНЬ У ПОДАТКОВИХ ПРАВОВІДНОСИНАХ

Концепція «Інтернет речей», як відомо, полягає в тому, що розвиток Інтернет-технологій відбувається в напрямі стрімкого збільшення кількості пристроїв, приєднаних до мережі, унаслідок чого мережа об’єднує по суті не людей, а речі – машини, які хоча і працюють за допомогою заданих людиною алгоритмів, але часто підключаються, відключаються та проводять певні операції в Інтернеті без відома людини, а отже користувачами Інтернету є також і речі, а не лише люди.

Не оминає процес розвитку технологій і сферу діяльності органів виконавчої влади, і зокрема сферу адміністрування податків і зборів. Цікавий приклад врегулювання порядку застосування машинного інтелекту можемо знайти в новітньому податковому праві України – при впровадженні в 2017 р. механізмів автоматичного блокування (зупинення реєстрації) податкових

накладних у Системі електронного адміністрування податку на додану вартість (далі – ПДВ).

Відповідно до п. 201.16 Податкового кодексу України (далі – ПКУ), реєстрація податкової накладної (розрахунку коригування) з податку на додану вартість (далі – ПН) в Єдиному реєстрі податкових накладних може бути зупинена у порядку, визначеному Кабміном, у разі відповідності такої ПН сукупності критеріїв оцінки ступеня ризиків, достатніх для зупинення реєстрації ПН в Єдиному реєстрі податкових накладних, встановлених відповідно до п. 74.2 ПКУ.

При цьому згідно з п. 74.2 ПКУ, в Єдиному реєстрі забезпечується проведення постійного автоматизованого моніторингу відповідності ПН критеріям оцінки ступеня ризиків, достатніх для зупинення їх реєстрації в Єдиному реєстрі податкових накладних.

Критерії оцінки ступеня ризиків, достатніх для зупинення реєстрації податкової накладної / розрахунку коригування в Єдиному реєстрі податкових накладних затверджено наказом Мінфіну від 13.06.2017 № 567.

Аналізуючи цей документ, маємо відзначити, що самі критерії, на затвердження яких уповноважений (згідно з ПКУ) Мінфін, містяться лише в п. 6 цього документа. А інші пункти Критеріїв містять правила, що врегульовують порядок зупинення реєстрації податкових накладних – що згідно з ПКУ належить до компетенції Кабміну, а не Міністерства фінансів. Правила зупинення реєстрації ПН прописані на рівні акту Кабміну в Порядку ведення Єдиного реєстру податкових накладних, затвердженому постановою Кабміну від 29 грудня 2010 р. № 1246 (у редакції постанови від 26 квітня 2017 р. № 341).

Так згідно з пунктами 12, 13 цього Порядку, Після надходження ПН до ДФС в автоматизованому режимі здійснюється їх розшифрування та проводиться ряд перевірок, за результатами яких формується квитанція про прийняття або неприйняття, або зупинення реєстрації ПН.

Згідно з п. 1 Критеріїв (згаданий наказ Мінфіну № 567), оцінка ступеня ризиків, достатніх для зупинення ПН в Єдиному реєстрі податкових

накладних здійснюється ДФС шляхом проведення постійного автоматизованого моніторингу відповідності ПН цим Критеріям.

До основних критеріїв автоматичного моніторингу податкових накладних належать обсяг постачання товару/послуги, зазначений у податковій накладній (який порівнюється з різними величинами) та відсутність анулювання ліцензій, інших дозвільних документів. Слід наголосити на тому, що критерії визначені в правових нормах недостатньо чітко, і тому на практиці по суті йдеться про машинні алгоритми, що визначаються постановниками задач при програмуванні відповідних комп'ютерів, що обслуговують Систему електронного адміністрування ПДВ. Саме на підставі цих алгоритмів система блокує податкові накладні.

Відсутність чітко прописаних критеріїв на практиці часто призводить до блокування ПН, складених виробничими підприємствами (коли підприємство закуповує одні товари, а продає зовсім інші), підприємствами, які розфасовують товари, і продають їх в інших одиницях виміру (наприклад купують у тонах, а продають у літрах, кілограмах, грамах чи штуках), в інших сумлінних платників ПДВ. Причому доволі часто реальних причин зупинення реєстрації ПН з'ясувати не вдається. Наприклад часом система може заблокувати лише одну накладну з кількох, виписаних у взаємовідносинах між постійними контрагентами. При чому цей самий товар або послуга, або цей же контрагент можуть міститися в інших податкових накладних, за якими система податкові накладні зареєструвала без зауважень.

Відповідно до пп. 201.16.1. ПКУ, в разі зупинення реєстрації ПН в Єдиному реєстрі податкових накладних платнику податку протягом операційного дня контролюючий орган в автоматичному режимі надсилає (в електронному вигляді у текстовому форматі) квитанцію про зупинення реєстрації такої ПН. Така квитанція є підтвердженням зупинення такої реєстрації.

У квитанції про зупинення реєстрації ПН, згідно з ПКУ зазначаються:

- а) порядковий номер та дата складення ПН;
- б) визначення критерію(їв) оцінки ступеня ризиків, достатніх для зупинення реєстрації ПН в Єдиному реєстрі податкових накладних, на підставі яких було здійснено зупинення реєстрації податкової накладної/розрахунку коригування;
- в) пропозиція щодо надання платником податку пояснень та/або копії документів (за вичерпним переліком), достатніх для прийняття контролюючим органом рішення про реєстрацію такої ПН в Єдиному реєстрі податкових накладних.

Вичерпний таких документів у розрізі критеріїв оцінки ступеня ризиків, достатніх для зупинення реєстрації ПН в Єдиному реєстрі податкових накладних також затверджено згаданим наказом Мінфіну №567.

Таким чином схема функціонування системи електронного адміністрування ПДВ з реєстрації податкових накладних, розрахунків коригування (у випадках зупинення їх реєстрації) виглядає приблизно так:

1. Платник ПДВ надсилає в Систему електронного адміністрування ПДВ податкову накладну (або розрахунок коригування), складену в електронному вигляді;

2. Система електронного адміністрування ПДВ з допомогою завчасно заданих машинних алгоритмів аналізує кожну податкову накладну чи розрахунок коригування з ПДВ на предмет відповідності визначеним Мінфіном критеріям;

3. У разі знаходження підстав для зупинення реєстрації ПН, така реєстрація зупиняється в автоматичному режимі, і платнику ПДВ надсилається відповідна квитанція, яка за законом має офіційний статус – ця квитанція підтверджує юридичний факт зупинення реєстрації ПН (пп. 201.16.1 ПКУ).

4. Платник податків вправі надати до органу ДФС необхідні для реєстрації ПН пояснення та документи (пп. 201.16.2 ПКУ), це подання здійснюється виключно в електронному вигляді.

5. Комісія ДФС приймає рішення про реєстрацію бо відмову в реєстрації ПН (пп. 201.16.3 ПКУ).

6. Рішення комісії може бути оскаржене в адміністративному або судовому порядку.

7. Реєстрація ПН відбувається в разі прийняття рішення про реєстрацію ПН (зазначеною комісією або за результатами скарги на її рішення), а також в разі прийняття рішення суду про реєстрацію ПН (201.16.3 ПКУ).

Окрім того ПКУ передбачає в пп. 56.23.4 правило (принцип) мовчазної згоди, згідно з яким в разі, якщо вмотивоване рішення за скаргою платника податків на рішення про відмову у реєстрації ПН в Єдиному реєстрі податкових накладних не надсилається платнику податків протягом 10-денного строку, така скарга вважається повністю задоволеною на користь платника податків з дня, наступного за останнім днем зазначеного строку. Як недолік необхідно відмітити, що ПКУ не містить механізму або правила, що забезпечували би реалізацію цього принципу. Це є важливим для багатьох платників ПДВ, оскільки на практиці на початку роботи системи зупинення реєстрації ПН дуже багато скарг не були розглянуті в строк, і водночас автоматичної реєстрації ПН за такими скаргами не відбулося.

Отже на сьогодні Податковий кодекс України та прийняті на його виконання підзаконні нормативно-правові акти передбачають проведення ряду автоматичних операцій за встановленим алгоритмом та прийняття автоматичних офіційних рішень, що оформлюються у вигляді квитанцій. Такі офіційні рішення приймаються: а) про реєстрацію податкової накладної; б) про зупинення її реєстрації. Можливе також прийняття рішень про відмову в прийнятті податкової накладної. Відповідні рішення є юридичними фактами, адже вони призводять до виникнення та зміни певних правовідносин. Вони приймаються машиною (автоматично), надсилаються платнику ПДВ засобами електронного зв’язку (через Інтернет), і можуть бути оскаржені (переглянуті) в установленому порядку. Правове регулювання функціонування

Системи електронного адміністрування ПДВ потребує вдосконалення, зокрема шляхом внесення змін до ПКУ та підзаконних актів, в т.ч. і згідно з пропозиціями, наведеними вище в цій статті.

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

Бевз С. І,
к.ю.н., доцент, доцент кафедри
ФСП КПІ ім. І. Сікорського.

ДЕРЖАВНЕ УПРАВЛІННЯ ГОСПОДАРСЬКОЮ ДІЯЛЬНІСТЮ В УКРАЇНІ ТА ІНТЕРНЕТ РЕЧЕЙ: ПОГЛЯД НА ПИТАННЯ

Сьогодні все більша кількість видів діяльності виконується за допомогою комп'ютерних мереж. 20 вересня 2017 року було схвалено Концепцію розвитку електронного урядування в Україні [1], в якій електронне урядування розуміється як форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян. Однією з таких технологій вбачається «Інтернет речей».

Як зазначено в Вікіпендії [2], Термін «Інтернет речей» (IP) вперше був введений Кевіном Ештоном у 1999 року під час його роботи над *Procter & Gamble*, щоб описати систему, в якій фізичні об'єкти могли бути пов'язані з давачами і мережею Інтернет. Ештон ввів цей термін, щоб проілюструвати можливості радіочастотної ідентифікації (*RFID*), яка використовується в корпоративних системах поставок, щоб порахувати і відстежити товари без потреби в людському втручанні. Сьогодні, інтернет речей став популярним терміном для опису сценаріїв, у яких інтернет з'єднання і обчислювальна здатність поширюються на безліч об'єктів, пристроїв, давачів і повсякденних об'єктів.

На основі використання технологій Інтернету речей, включаючи мережу Інтернет, вже сьогодні стає можливим або без участі людини, або з міні-

мальною її участю управління господарською діяльністю певного суб'єкта господарювання. Проте застосування технологій Інтернету речей для здійснення державного управління господарською діяльністю на загальнодержавному рівні видається дискутивним. Для розуміння можливості поєднання цих двох явищ спробуємо визначити сутність кожного з них.

В своїй статті « «Інтернет речей» як правовий термін» [3, с.101] О. Баранов відмічає, що «загальноприйнятого визначення терміну «інтернет речей», який би відповідав інтересам правової науки, не запропоновано» та пропонує таку дефініцію терміна «інтернет речей» - це сукупність 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).

В той же час під державним управлінням господарською діяльністю пропонуємо розуміти організаційно-владну діяльність державних органів (посадових осіб), в процесі якої реалізуються функції державного управління відносно суспільних відносин, що виникають, змінюються і припиняються у зв'язку з зайняттям або реалізацією наміру займатися господарською діяльністю невизначеним колом осіб та яка спрямована на виконання економічної функції держави [4, с.174]. Господарська діяльність є, напевно, однією з тих сфер, в якій найкраще відображається діалектика приватних та публічних інтересів. Адже учасниками відносин у цій сфері є як суб'єкти господарювання (суб'єкти приватного права), так і органи державної влади (суб'єкти публічного права). Як відомо, здійснювати господарську діяльність без взаємодії з органами державної влади неможливо. В той же час зміст діяльності органів державної влади щодо здійснення державного управління господарською діяльністю має диференціюватися в залежності від сфер її здійснення та її видів.

Виходячи з такого розуміння державного управління господарською діяльністю, його здійснення за допомогою технологій Інтернету речей можливо у разі представлення державного управління господарською діяльністю як взаємодії двох систем: господарська діяльність та процес державного управління, спрямований на виконання економічної функції держави, показники зв'язку між якими обчислюються за допомогою інтернет мережі.

Однією з першочергових реформ і програм, що мають бути реалізовані задля руху вперед за вектором розвитку відповідно до Стратегії сталого розвитку "Україна - 2020" [5] є дерегуляція та розвиток підприємництва. При цьому функціонування органів державної влади спрямоване на реалізацію економічної функції держави має здійснюватися системно – з виконанням всіх функцій державного управління. Тож ключовими в представленні процесу державного управління як системи є його функції - прогнозування та планування, організація, регулювання у вузькому сенсі, координація, облік та контроль. Поступова реалізація (одна за одною) цих функцій державного управління сприятиме забезпеченню системності здійснення цієї діяльності органами державної влади.

Враховуючи зміст сучасного типу методологічного аналізу, який визначається в основному двома новими методологічними парадигмами – системним підходом і синергетикою, яка поєднує системно-інформаційний, структуралістський підходи з принципами самоорганізації [6, с.92], господарська діяльність має сприйматися як певна система, що складається з різних взаємопов'язаних елементів, здатна до самоорганізації та розвитку внаслідок зовнішнього впливу, який має прояв, зокрема, через державне управління. При цьому, безпосереднє здійснення господарської діяльності різними суб'єктами господарювання повинне мати зворотній вплив на систему державного управління. Лише взаємодія двох систем зможе забезпечити досягнення мети державного управління господарською діяльністю - встановлення правового господарського порядку, при якому забезпечується баланс публічних і приватних інтересів як в діяльності

суб'єктів владних повноважень, так і в діяльності суб'єктів господарювання або бажаючих займатися господарською діяльністю.

Таким чином, розуміння державного управління господарською діяльністю можливе через представлення 2-х взаємодіючих систем як технічних комплексів, що зумовлює необхідність перетворення елементів таких систем в певні показники, бази даних. Можливий і інший варіант: застосування Інтернету речей лише для системи «господарська діяльність», якою здійснюється державне управління, в тому числі у формі електронного урядування. Тобто застосування технологій Інтернету речей до державного управління господарською діяльністю можливе лише за умови «оречевлення» елементів або обох систем, або хоча б однієї з них.

Як відмічається в Концепції розвитку електронного урядування в Україні «Ефективне управління будь-якою галуззю у сучасних умовах неможливе без широкого застосування сучасних інструментів електронного урядування, у тому числі автоматизації обробки великих об'ємів даних та інформаційно-аналітичного забезпечення прийняття управлінських рішень, оптимізації та автоматизації адміністративних процесів, запровадження електронних форм взаємодії. Основними завданнями із забезпечення розвитку електронного урядування у базових галузях України є запровадження інформаційно-телекомунікаційних систем підтримки прийняття управлінських рішень та автоматизації адміністративних процесів (зокрема з використанням перспективних геоінформаційних технологій, Інтернету речей …)». При цьому визначаючи способи запровадження ІТС у певні сфери не виокремлюється сфера господарської діяльності або економіки в цілому, що потребує додаткового дослідження. Крім того, розробляючи механізм державного управління господарською діяльністю варто враховувати , що господарська діяльність може являти собою певну технічну систему, яка представляється за допомогою технологій Інтернет речей.

Таким чином, можемо припускати можливість застосування технологій Інтернет речей при здійсненні державного управління господарською

діяльністю, подальші дослідження яких має зумовити формування фундаменту для побудови «розумної» економіки в межах всієї держави.

Література:

1. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження Кабінету Міністрів України від 20 вересня 2017 року №649-р
2. https://uk.wikipedia.org/wiki/Інтернет_речей
3. Баранов О.А. «Інтернет речей» як правовий термін / О.А. Баранов // Юридична Україна. – 2016. - №5-6. – с.96-103
4. Бевз С.І. Розмежування відносин з державного управління господарською діяльністю / С.І. Бевз //Науковий вісник Херсонського державного університету. Серія «Юридичні науки». Випуск 3. Том1.- 2017., с.172 - 176
5. Про стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12 січня 2015 року № 5/2015
6. Комарова А.И. История и методология юридических наук: учебное пособие / А.И. Комарова. – М.: Московский университет «им. С.Ю. Витте», 2015. – 207 с.

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

Гайдученко Д.,
студент ФСП КПІ ім. Ігоря Сікорського
Науковий керівник:
Мельник Б. Б.

ПРОБЛЕМИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ У РІЗНИХ СФЕРАХ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ

Технологія Інтернету речей має широкий круг скептиків, які вважають, що якщо така технологія й реалізується у недалекому майбутньому, то від неї буде більше шкоди аніж користі.

З кожним роком про Інтернет речей дізнаються все більше людей. Все більше ресурсів виділяється на розробку платформ за допомогою яких у майбутньому стануть доступними дослідження і навіть медичні операції на відстані. Представимо, що хірурги вже можуть проводити дистанційні операції з якоїсь однієї платформи, яка знаходиться в іншій державі. З першого погляду це звучить дуже футуристичне і захопливе. Але якщо якийсь датчик або перемикач не отримає чи не відправить сигнал до цієї

платформи? У результаті хірург отримає неточний аналіз й зробить помилку. Тоді операція може зашкодити або навіть й вбити пацієнта. Хіба тоді можна казати, що відповідальність за операцію несе тільки хірург? Звичайно ні, бо хірург оперував тільки тим набором інформації, що отримував дистанційно. І все із-за невеликого порушення зв'язку. Виходить, що людське життя у такому разі буде залежати не тільки від знань хірурга та його досвіду, але й від надісланої інформації мережею. Людський досвід ніколи не потрібно ставити на друге місце. Дистанційний спосіб не завжди корисний.

Як нам відомо, Інтернет речей – це усі пристрої, які так чи наче підключені до мережі. Не потрібно забувати й про атаки хакерів. Припустимо, є єдина медична мережа, до якої підключені багато медичних пристроїв. Це можуть бути як звичайні комп'ютери так і апарати які підтримують життя у хворих. Якщо хакер проникне у цю мережу, то з легкістю зможе відключити апарати для підтримання життя: один, два або навіть усі одразу. Або цей же хакер зможе скористатися інформацією про хворобу тої чи іншої людини. Тут панівну роль можуть грати різні характери дій зловмисника: політичний, інтимний тощо. Якийсь відомий політик вирішить прооперуватися у клініці, яка відома тим, що рівень смертності серед пацієнтів дуже низький. Хакер проникає у мережу й виключає всю апаратуру, або посилає неповну інформацію хірургу. Хірург робить помилку – політик або каліка на все життя, або помирає на операційному столі. У цьому випадку буде нанесений ущерб не тільки репутації клініки, але й навіть усій державі, якщо той політик грав важливу роль у вдосконаленні його країни. І такі вбивства можуть траплятися кожний день з різними людьми які просто захотіли підлікуватися у клініці.

У наш час існує немало різновидів заробітку, але підприємницький спосіб залишається найпопулярнішим. Багато хто хоче мати все й одразу, й заради цього навіть готові на крадіжки. Це може бути не тільки крадіжка за «старим» засобом: витаскувати гаманець із штанів або проникати зі зломом до квартир. Наше століття породило новий вид крадіжок – цифрові. Головна

проблема технології Інтернету речей – це вкрай слабка система захисту від крадіїв. А це іноді призводить до поганих наслідків. Якщо казати саме про крадіжки, то «підключення усіх пристроїв до мережі» робить працю крадія легкою. На якихось приватних випадках це не так відчувається як на крадіжках у корпорацій або саме у бізнесменів. Припустимо, що корпорація надійно захистила свою базу даних, ніхто не зможе туди проникнути крім працівників й директорів. Здається, що проблема вирішена - просто зробили більш надійнішу систему захисту. І так і є, але кмітливий крадій завдяки технології Інтернету речей підключиться до камери у кабінеті директора і зможе побачити як директор вводить пароль на комп'ютері. Така маленька деталь може зруйнувати всю систему безпеки корпорації або навіть й саму корпорацію.

Річ навіть не в корпораційних війнах, адже хакер може бути просто використаний іншою корпорацією-конкурентом для ліквідації свого конкурента. Через недосконалості цієї самої мережі, де може бути підключено багато різних пристроїв, може постраждати або навіть загинути багато людей. Наприклад, бізнесмен, якого потрібно ліквідувати, відправився на зустріч у іншу країну, купив місце у бізнес-класі і конкурент про це дізнався. Завдяки технології речей вбивця зможе проникнути в бортову мережу через Wi-Fi і зробити так, щоб літак розбився. Таке стане можливим, якщо в єдину мережу літака об'єднати різні кластери: авіоніку літака і інфраструктуру бездротового зв'язку для пасажирів. Цікаво те, що таке рішення вже застосоване в Boeing 737 MAX. Тобто, вже зараз, пасажири цієї моделі літака знаходяться у ще більшій небезпеці ніж завжди.

Отже я вважаю, що технологія Інтернету речей дуже недооцінена у сенсі безпеки. Використання такої мережі може нашкодити людському життю.

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

Маньгора В. В.,
к.пед.н., доцент, професор кафедри права ПрАТ «Вищий навчальний заклад «МАУП» Вінницького інституту (м. Вінниця).

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ПРИ ПІДГОТОВЦІ МАЙБУТНІХ ЮРИСТІВ

В жовтні 2017 р. Україні з'явиться перша професійна хмарна CRM-система для юристів. Проблему вибору і адаптації під потреби галузі якісної CRM-системи вирішила команда добре відомого в Україні правового ресурсу «Будинок юриста». Вони запропонували першу професійну хмарну CRM-систему для юристів і незабаром дадуть можливість для її безкоштовного тестування. За допомогою системи юристи зможуть виставляти рахунки клієнтам, вести власний білінг, швидко і просто формувати різні звіти, керувати своїми справами і користуватися іншими можливостями [1].

Підготовка висококваліфікованих спеціалістів потребує, йти в ногу з часом, враховувати ті зміни, які відбуваються в інформаційному середовищі, професійній освіті. В сучасних умовах при підготовці майбутніх спеціалістів ширше використовують хмарні технології.

Стратегія розвитку інформаційного суспільства в Україні на 2013-2020 роки, передбачає формування сучасної інформаційної структури на основі хмарних технологій [3]. На думку Н.А. Хміль метою інтеграції хмарних технологій у педагогічний процес ВНЗ є створення інформаційного середовища, або інформаційної інфраструктури навчального закладу, котра в «Стратегії розвитку інформаційного суспільства в Україні» визначається як «сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування» [5, с. 129].

Уперше термін «хмарні технології» у 1997 р. запровадив Р. Челлаппа.

Хмарні технології – технологія обробки даних, в якій комп’ютерні ресурси та потужності надаються користувачеві як інтернет-сервіси. Користувач має доступ до власних даних, але йому не потрібно піклуватись про інфраструктуру, операційну систему та безпеку збереження даних. Термін «хмара» використовується як метафора складної інфраструктури, за якою ховаються всі технічні деталі [6, с. 149].

Перевагами використання хмарних технологій є: непотрібні потужні комп'ютери; менше витрат на закупівлю програмного забезпечення і його систематичне оновлення; необмежений обсяг збереження даних; доступність з різних пристроїв і відсутня прив’язка до робочого місця; забезпечення захисту даних від втрат та виконання багатьох видів навчальної діяльності, контролю і оцінювання, тестування он-лайн, відкритості освітнього середовища; економія коштів на утримання технічних фахівців.

Хмарні системи не позбавлені недоліків, які більшою мірою стосуються звичайних користувачів, і в меншій - провайдерів: постійне з'єднання з мережею Інтернет; погано працюють з повільним Інтернет-доступом; програми можуть працювати повільніше ніж на локальному комп'ютері; не всі програми або їх властивості доступні віддалено; безпека даних може бути під загрозою; далеко не кожен хмарний додаток дозволяє зберегти отримані результати в зручному для користувача вигляді на потрібний носій даних; ризик масової втрати даних багатьма користувачами через технічний збій у постачальника хмарних послуг; втрата свободи - більша частина хмарних сервісів не має чітких стандартів, і тому при переході від одного постачальника хмарних послуг до іншого можуть виникнути серйозні проблеми. Не зважаючи на недоліки, багато експертів вважають, що переваги і зручності переважують можливі ризики використання подібних сервісів.

Розглянемо основні можливості використання хмарних технологій у навчальному процесі при підготовці майбутніх юристів. Найбільш поширеними у використанні є хмарні сервіси призначені для набуття навичок роботи

з веб-сервісами та звичайними документами. Серед них розглянемо хмарну платформау Microsoft Live@edu, завдяки якій на основі хмарних технологій надається можливість вивчати на практиці відомі офісні додатки через web-браузер, при чому до сервісів даної платформи відносять електронну пошту, календар, веб-конференції (з можливістю відео- зв'язку); віртуальну дошку; конструктор створення та підтримки веб-сайтів; можливість створення, редагування документів Word, Excel, Power Point [2, с. 98].

Служба Office 365 пропонує класичні програми Microsoft Office та хмарні сервіси, зокрема пошту корпоративного рівня, спільні календарі, миттєві повідомлення, портал для зберігання та одночасної роботи з документами та відео-конференції в HD якості.

Windows Azure надає хмарний сервіс для зменшення витрат та розвитку бізнесу на базі розташованих в різних регіонах світу центрів обробки даних Microsoft.

Хмарна платформа Google Apps Education Edition, основними інструментами якої для використання студентами і викладачами є: електронна пошта Gmail (перевагами даного сервісу є підтримка текстового та голосового чату Google Talk, а також відеочату); календар Google; диск Google – сховище для зберігання власних файлів та можливістю настройки прав доступу до них; Google Docs – сервіс для створення документів, таблиць і презентацій з можливістю надання прав спільного доступу декільком користувачам; сайти Google – інструмент, який дозволяє створювати сайти за допомогою встроєних шаблонів. Також набувають все більшої популярності хмарні сервіси, за допомогою яких надається можливість розробляти власні або використовувати існуючі тести. Прикладом такого сервісу для швидкої та якісної розробки власних тестів є OpenTest, який надає можливість безкоштовно обслуговувати (у режимі Lite) близько 100 студентів на місяць з одним аміністратором тесту. Досить зручними у використанні є також хмарні сховища. До найбільш відомих відносять Google Drive, SkyDrive, Dropbox та інші. Однією з основних переваг у використанні хмарних платформ та

сервісів є безперечно доступність навчання у будь-якому місці та у будь-який час. Студент може почати виконання завдання в університеті, при цьому продовжити роботу він може й будучи вдома не маючи необхідності копіювати виконане завдання на носії інформації. Це все можливо завдяки тому, що всі необхідні відомості та дані можна зберігати на віддаленому сервері [2, с. 99].

Найбільш популярними у світі системами управління навчання є: Moodle, Edmodo, Blackboard.

При дистанційній підготовці майбутніх юристів можна використовувати систему дистанційного навчання Moodle (Modular Object Oriented Distance Learning Environment), яку відносять до вільного програмного забезпечення освіти. Ця система призначена для організації навчання он-лайн у мережевому середовищі з використанням технологій Інтернету. Система забезпечує різноманіття процедур навчання он-лайн, комбінуванням яких може бути організоване ефективне навчання в навчальному закладі. Moodle надає можливість інсталяції освітніх ресурсів (навчальних матеріалів) і забезпечує засобами доступу до ресурсів та управління ними; забезпечує комунікаційну взаємодію учасників освітнього процесу, що реалізовується у формі інтернет-конференцій, форумів, дискусій, а також обміну посланнями, що містять, зокрема, завдання для тих, хто навчається, виконання завдань і коментарі. У системі передбачено можливість специфікації категорій (Category) навчальних курсів, наприклад, таких, як Office work [4].

Edmodo – віртуальне навчальне середовище, подібне до соціальної платформи Facebook, для підтримки взаємодії викладачів та студентів в реальному часі. Це неймовірно легкий у використанні та потужний освітній інструмент, який може бути адаптовий до будь-якого навчального курсу.

Blackboard є додатком штучного інтелекту, який ґрунтується на архітектурній моделі Blackboard, де загальна база знань оновлюється фахівцями з різних галузей знань. Доцільно зазначити, що спочатку модель

Blackboard була створена для вирішення комплексних і складних завдань, але сьогодні цей додаток широко використовують з метою самоосвіти.

Зараз у багатьох ВНЗ, які здійснюють підготовку юристів створюються сайти, Інтернет-платформи та інші освітні ресурси, на яких розміщують навчально-методичне забезпечення, завантажують відеолекції, інтерактивний перелік літератури, онлайн-курси юридичних дисциплін, таким чином, підвищуючи професійну підготовку майбутніх юристів та формують професійні компетенції.

Використання хмарних технологій під час підготовки в ВНЗ майбутніх юристів сприяє активізації навчального процесу, підвищенні мотивації студентів отримувати майбутню спеціальність, забезпечує мобільність студентів, співпраці студентів та викладачів, формуванню професійних компетенцій.

Література:

1. В Україні з'явиться перша професійна хмарна CRM-система для юристів [Електронний ресурс] – Режим доступу: http://zib.com.ua/

2. Вакалюк Т. А. Можливості використання хмарних технологій в освіті / Т.А. Вакалюк // Актуальні питання сучасної педагогіки. Матеріали міжнародної науково-практичної конференції (м. Острог, 1-2 листопада 2013 року). – Херсон: Видавничий дім «Гельветика», 2013. – С. 97–99.

3. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядж. Кабінету Міністрів України від 15 травня 2013 р. № 386-р [Електронний ресурс] / Верховна Рада України : офіційн. веб-портал. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/386-2013-%D1%80. – Назва з екрану.

4. Фоменко Н.А. Правова педагогіка : Навчальний посібник [Електронний ресурс] / Н.А. Фоменко, М.І. Скрипник, О.В. Фатхутдінова. – Херсон: Олді-плюс, 2015. – 326 с. – Режим доступу http: pidruchniki.com /78577

5. Хміль Н.А. Зарубіжний і вітчизняний досвід інтеграції хмарних технологій у педагогічний процес вищого навчального закладу / Н.А. Хміль // Інформаційні технології і засоби навчання. – 2015. – Том 50. - № 6. – С. 128-136.

6. Яценко О.І. Основні поняття та переваги хмарних технологій / О.І. Яценко // Інформаційні технології [Текст] : зб. тез І Української конференції молодих науковців, 22-23 трав. 2014 р., м. Київ / Київ. ун-т ім. Б. Грінченка, Інститут суспільства, Кафедра інформатики, Кафедра

інформаційних технологій і математичних дисциплін. - Київ : Київ. ун-т імені Бориса Грінченка, 2014. -. – 2014. – С. 148-150.

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

Колесов Н.,
студент ІІ курсу ФСП КПІ ім. Ігоря Сікорського.
Науковий курівник:
Мельник Б. Б.

ПРОБЛЕМИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ У РІЗНИХ СФЕРАХ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ

В зв’язку з тим, що тема Інтернету речей у наш час набирає обертів, потрібно розглянути її проблематику, яка присутня у різних сферах суспільної діяльності. Розглянемо декілька основних сфер, в яких застосовується технології Інтернету речей: охорона здоров’я, промисловість, сільське господарство, освіта, управління державою, транспорт і торгівля.

Першою і основною проблемою, що заважає розвитку технологіям Інтернету речей – це фінансове забезпечення. На даному етапі розвитку наша держава не спроможна підтримати усі сфери суспільної діяльності в тому обсязі у якому це необхідно, по причині того що існують труднощі з перерозподілом державного бюджету, від якого напряму залежить розвиток цих технологій.

Другою причиною можна назвати відсутність стабільної роботи кадрової політики. Тобто недостатня кількість висококваліфікованих спеціалістів у сфері ІТ – послуг, науки, інженерії, які могли б підтримувати стабільну роботу усіх функціональних властивостей, що присутні у технологіях Інтернету речей.

Третьою проблемою, що випливає з двох попередніх є застій у виробництві. Він пов'язаний з тим що присутня недостатня кількість робочих місць на виробництвах, відсутня справедлива оплата праці. Тобто прогалина в мотиваційних факторах на виробництві, у взаємовідносинах породжує збої в виробничих процесах.

Також важливим моментом в розгляді цієї теми є консервативність нашого суспільства. Люди дуже важко адаптуються до нових технологій, їм важко в швидкому порядку вийти з теперішнього рівня комфорту. Ще не слід забувати про те що розвиток технологій Інтернету речей потребує високого рівня безпеки, тому що через несанкціоноване втручання, його робота може бути погіршена. Якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, за допомогою надійного криптографічного алгоритму, замість користі вони принесуть шкоду, надавши кібер-злочинцям лазівку для підриву інформаційної безпеки.

Оскільки наприклад, речі із вбудованими комп'ютерами зберігають дуже багато інформації про свого власника, зокрема можуть знати його точне місцезнаходження, доступ до такої інформації може допомогти зловмисникам вчинити злочин. Відсутність на даний час стандартів для захисту таких автономних мереж дещо сповільнює впровадження Інтернету речей у повсякденне життя.

Підводячи підсумок, можна зазначити що без виправлення вищесказаних факторів існування стабільного функціонування Інтернету речей в наш час досить проблематичне і складно уявити, які можуть бути з цього наслідки. Для того щоб це виправити, необхідно корегувати проблеми, які знаходяться на більш державному і політичному рівні країни, тому що вони мають дуже тісний зв'язок, і мають колосальний вплив один на одного.

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

Акімов О. О.,
к.н.держ.упр., доцент, Заслужений економіст України Національної служби посередництва і примирення.

ПРІОРИТЕТИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОННОЇ УЧАСТІ ГРОМАДЯН У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

Участь громадян в системі електронного врядування є ознакою демократичного суспільства та розбудови громадянського суспільства. У

нормативних документах міжнародних організацій (наприклад, щорічний аналітичний звіт ООН про світовий розвиток електронного урядування) представлена модель трирівневої електронної участі громадян: «від пасивної до активної взаємодії» публічного управління та громадян, а саме:

- *отримання інформації* (пасивний рівень), доступ громадян до публічної інформації в онлайн-режимі;
- *електронні обговорення,* залучення людей до дискусій щодо державної політики, надання громадянам можливості коментувати урядові ініціативи;
- *електронні пропозиції,* розробка громадянами рекомендацій для органів публічного управління, що дозволяє покращити ситуацію в країні.
- В демократичних країнах визнано, що перехід від пасивної до активної участі громадян у системі електронного врядування сприяє розширенню прав та свобод у суспільстві, є важливою умовою розбудови правової, демократичної країни та громадянського суспільства [1].

До активних способів електронної участі громадян у системі публічного управління відноситься:

- *електронне законодавство,* що дозволяє громадянам коментувати / вносити правки до проектів нормативно-правових актів;
- *електронне голосування,* що дозволяє громадянам брати участь у електронних виборах або ж у електронному референдумі (у т.ч. місцевому);
- *електронні консультації,* що дозволяє громадянам долучатися до дискусій, обговорень економічних гуманітарних та соціально-політичних питань суспільного розвитку;
- *електронні ініціативи,* що дозволяє громадянам висувати ідеї, надавати пропозиції щодо процесів державотворення, впливати на розробку соціально-економічної політики держави;

- *електронні петиції,* що дозволяють громадянам висловлювати своє ставлення (схвалення ти протест), надати рекомендації правлячім елітам щодо вирішення того чи іншого питання;
- *електронні кампанії,* що дозволяє громадянам поширювати ідеї, співзвучні тим чи іншим соціально-політичним кампаніям в онлайн-просторі (якщо вони поділяють чи проти тих чи інших ідей, пропозицій, реформ);
- *електронні опитування, електронне анкетування* дозволяє громадянам висловити власну позицію щодо тих чи інших питань, що виносяться на обговорення. Електронні опитування створюють фундамент для формування громадської думки та її врахування у роботі органів влади всіх рівнів. Перелік інструментів електронної участі громадян у житті суспільства представлено у «Рекомендаціях CM/Rec (2009) Комітету Міністрів Ради Європи країнам-членам ЄС щодо електронної демократії» [2]. Водночас, переважна більшість з цих інструментів в Україні законодавчо не унормована, що потребує активної роботи у цьому напрямі системи української юриспруденції.

Натомість, в Україні вже унормовано такий спосіб електронної участі громадян в системі публічного управління як *електронне звернення*. Так, на офіційному веб-сайті Державної системи електронних звернень України електронні звернення визначаються як «викладені в електронному документі пропозиції, заяви, скарги, які відправлені автором в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем» [3].

Активізація електронної участі громадян у системі публічного управління потребує розвинутої системи *електронної демократії*. У країнах ЄС це питання унормовується у «Рекомендації CM/Rec(2009)1 Комітету Міністрів Ради Європи країнам-членам ЄС щодо електронної демократії» (2009). У додатку до документу визначені принципи е-демократії, а також

визнано, що електронна демократія грунтується на електронної участі громадян, системному використанні Інтернет-ресурсу [2].

В Україні у сфері електронного врядування існує спосіб електронної участі громадян у системі публічного управління як *електронне партнерство* («…поглиблений етап взаємодії громадян із владою, де відповідальність за прийняття рішень покладається на обидві сторони, передбачає внесок кожного у розвиток громадянського суспільства») [4].

ООН розглядає електронні петиції, електронні голосування, електронні опитування як технічні інструменти для участі громадян під час електронних обговорень рішень та заходів у сфері публічного управління, що реалізується за допомогою *соціальних мереж* та *онлайн-форумів* [1]. Технічно реалізувати електронну участь громадян у системі публічного управління можливо за допомогою різних ресурсів Інтернет, різних веб-рішень. Це може онлайн-форум, соціальні мережі, або ж – новий веб-ресурс для електронної участі громадян. Як приклад – веб-сайт для подання електронних петицій, веб-портал відкритих даних тощо.

ОЕСР (Організація економічного розвитку та співробітництва) визначила системні принципи політики е-демократії в інформаційно-аналітичному документі «Перспективи та проблеми е-демократії: виклики у сфері електронного залучення громадян» [5]. ОЕСР зазначає, що «е-демократія є рушійною силою активізації політики щодо демократії», «е-демократія передбачає двосторонній зв'язок між громадянами та урядовцями», «е-демократична ініціатива має вирізнятись чітко визначеною метою, базуватись на необхідних для її реалізації ресурсах та бути законодавчо закріпленою» [5]. Отже, відповідно до міжнародного права, в Україні необхідно законодавчо унормувати всі різновиди електронної участі громадян у розбудові громадянського суспільства та взаємодії з органами публічного управління.

Україна обрала шлях євроінтеграції. Європейський досвід залучення громадян до електронного врядування свідчить, що цей процес відбувається

не тільки на державному, регіональному та місцевому рівні, але й на міжнародному рівні. Як приклад – проведення у ЄС електронних публічних консультацій урядовців з громадськістю, під час яких активно використовується веб-ресурс «Твій голос у Європі» [6]. Кожна відкрита консультація представників публічної влади та представників громадськості має певну назву та короткий опис, правила участі, цільову групу та дату завершення консультації. Результати проведення консультацій є доступними і впродовж певного часу після їх завершення. Учасники консультацій отримують можливість ознайомитись з ідеями інших користувачів та дізнатись, які пропозиції/ідеї були враховані Європейською Комісією для прийняття політичних та управлінських рішень [7]. Такі приклади участі громадян у системі публічного управління є важливі для України, адже врахування інтересів та пропозицій громадян робить публічну владу результативною та соціально-зорієнтованою.

В Україні започатковано нормативно-правове забезпечення електронної участі громадян в системі публічного управління, зокрема, йдеться про положення законів України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», «Про Концепцію Національної програми інформатизації», «Про Національну програму інформатизації», «Про інформацію». У 2015 р. прийнято Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» (від 2 липня 2015 р.), що свідчить про унормування електронної участі громадян у житті українського суспільства. Натомість, низка питань у цій сфері ще потребує вирішення. Нормативно-правове забезпечення електронної участі громадян у системі публічного управління є вимогою часу, відповідає вимогам ЄС щодо розбудови демократичного громадянського суспільства, а отже – має бути обов'язково реалізовано в Україні.

Література:

1. Мережа ООН з питань державного управління [Електронний ресурс]. – Режим доступу: http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf
2. Рекомендації CM/Rec(2009)1 Комітету Міністрів Ради Європи країнам-членам ЄС щодо електронної демократії. Рада Європи [Електронний ресурс]. – Режим доступу:https://wcd.coe.int/ViewDoc.jsp?id=141062 249
3. Державна система електронних звернень. Питання та відповіді. Держінформресурс [Електронний ресурс]. – Режим доступу: http://z.gov.ua/index.php/main/answers
4. E-Transformation [Електронний ресурс]. – Режим доступу: http://etransformation.org.ua/2014/11/24/355/
5. Перспективи та проблеми електронної демократії: виклики залучення громадян в електронному просторі. ОЕСР [Електронний ресурс]. – Режим доступу: http://www.keepeek.com/Digital-Asset-Management/ oecd/governance/promise-and-problems-of-e-democracy_9789264019492-en#page1
6. Твій голос у Європі. Європейська комісія [Електронний ресурс]. – Режим доступу: www.ec.europa.eu/yourvoice/index_en.htm
7. Твій голос у Європі: новий портал Комісії націлений на збільшення ролі громадян у формуванні політичного курсу. Agris [Електронний ресурс]. – Режим доступу: www.agris.cz/clanek/119423

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

Біла С. О.,
д.н.д.у., професор, Заслужений економіст України, рофесор кафедри міжнародних економічних відносин і бізнесу Навчально-науковий інститут міжнародних відносин Національний авіаційний університет (ННІМВ НАУ, м.Київ).

ВИКЛИКИ ЩОДО ІНСТИТУЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНТЕРНЕТ-ТРЕНДІВ В ЕКОНОМІЦІ

Нормативно-правове забезпечення всіх процесів та явищ (економічного, соціального, господарського, гуманітарного та ін. профілю), чинних на даний період часу, характеризується певною консервативністю, стабільністю, еволюційністю удосконалення. Дотримання у суспільстві законів та підзаконних актів є невід'ємною складовою правової держави. Поряд з цим, в умовах глобалізації, відкритості економіки, інформатизації та

компьютеризації, розповсюдження впливу Інтернет на всі сфери господарського, соціального, політичного та культурного життя країни, у XXI ст. швидко змінюється реальність існування людської цивілізації, що вимагає гнучкості та швидкої адаптації до цих процесів системи правового регулювання та впровадження.

У XXI ст. інноваційні зміни, повязані з розвитком Інтернет-системи, Інтернет-послуг, Інтернетом речей стосуються майже всіх сфер життєдіяльності людини, всіх сфер функціонування національного та світового господарства. З 2009 по 2016 рр. кількість користувачів Інтернет у світі збільшилось з 1,6 до 3,4 млрд осіб. На Землі у 2017 р. проживає майже 7,5 млрд осіб, отже, варто очікувати, що у 2018 - 2020 рр. кількість землян, що користуватиметься Інтернет-послугами та Інтернетом речей перевищить половину мешканців Землі. Кількість користувачів Інтернет швидко зростає внаслідок появи на ринку поряд зі стаціонарними (персональними) комп'ьютерами та ноутбуками і персональних смартфонів, які забезпечують мобільність доступу користувачів до Інтернет-ресурсів. З 2010 по 2017 рр. кількість власників смартфонів у світі збільшилась з 0,3 до 2,8 млрд. осіб, а половина з них проживає у країнах Азії [1].

Стрімкий розвиток ринку смартфонів у світі відбувається паралельно з розвитком та удосконаленням ринку стаціонарних компьютерів (так званих «десктопів») та ринком ноутбуків (так званих «лептопів»). Переважна більшість користувачів (середній клас, бізнес-агенти, верстви населення з доходом вище середнього по країні) надають перевагу одночасному володінню всіма означеними технічними засобами (і у декількох екземплярах), що дає можливість користувачу у конкретний період часу обирати найбільш оптимальний варіант роботи з Інтернет-ресурсами.

У XXI ст. Інтернет швидко та кардинально модифікує всю систему виробничих, соціально-економічних відносин, бізнес-систему, змінює закономірності функціонування ринку праці, ринку послуг (у т.ч. і публічних, адміністративних послуг), змінює традиційний уклад суспільного

розвитку. Економічні, інституційні, соціальні, ресурсні втрати від недосконалого нормативно-правового забезпечення функціонування ринку Інтернет-речей та Інтернет-послуг досягає великих сум. Так, лише на ринку інтерактивних компьютерних ігор за 2016 р. доходи фірм у світі становили: Північна Америка – 25,4 млрд дол. США (приріст за 2015 – 2016 рр. +4,1 %); Західна Європа – 17,3 млрд дол. США (приріст: +4,4 %); Азійсько-Тихоокеанський регіон – 46,6 млрд дол. США (приріст: +10,7 %); Латинська Америка – 4,1 млрд дол. США (приріст: +20,1%); Близький Схід та Африка – 3,2 млрд дол. США (приріст: +26,2%); Східна Європа – 3 млрд дол. США (приріст: +7,3 % відповідно). Тільки в Україні доходи від ринку інтерактивних ігор за 2016 р. досягали 142 млн.дол. США. В цілому, по світу доходи ринку інтерактивнпх ігор у 2016 р. становили 89,4 млрд.дол США [2]. Натомість, провове регулювання тільки цієї сфери Інтернет-послуг в Україні перебуває у початковому стані, що обмежує можливості держави щодо оподаткування, контролю за створенням нових робочих місць, сплатою роялті за інтелектуальну власність тощо.

На ринку Інтернет-речей та Інтернет-послуг особливе місце у світі займають NBIC – технології. NBIC – технології («nano, bio, info, cogno») поєднують розвиток нанотехнологій, біотехнологій, інформаційних технологій, когнітивістики, що функціонують на основі міждисциплінарного підходу (синтезу, синергії), сприяють появі на цій основі великої кількості принципово нових напрямків НДДКР та бізнес-стартапів – біомедицини, нанотехнологій, штучного інтелекту та ін.

Серед стратегічних пріоритетів розвитку NBIC-технологій – взаємодія інформаційних технологій і когнітивної науки [3]. Матеріалізацією цього напрямку є діяльність щодо створення штучного інтелекту, який зможе повністю імітувати процес мислення людини (без емоційної складової). До 2020 року фахівці NBIC очікують на появу «штучного інтелекту» – комп’ютерної «нервової системи», кібернетичного «мозку», який зможе управляти складними виробничими системами (у т.ч. зі швидкістю, що

кардинально перевищує швидкість роботи традиційних компь'ютерних систем, а також – і в екстремальних умовах). Сфера застосування «штучного інтелекту» не обмежена: військово-промисловий комплекс; охорона суспільного порядку; національна безпека; публічні послуги; охорона здоров'я; інформаційні послуги, «економіка здоров'я» тощо. «Штучний інтелект» є необхідною умовою для переходу промисловості розвинених країн світу до «Індустрії-4.0», що грунтується на «промисловому Інтернеті», заснована на робототехниці та високотехнологічних засобах виробництва (що діють автономно, без участі традиційного «найманого працівника») [4]. Перехід до «Індустрії-4.0», яку у розвинених країнах світу часто називають «Четвертою промисловою революцією» потребує принципово нового законодавчого забезпечення, у т.ч. – вирішення питань щодо оподаткування бізнесу, що використовує робототехніку замість людей; прийняття нової системи законів, що забезпечать процеси стандартизації, сертифікації продукції, контроль за якістю та безпекою виробництва «промислового Інтернету», контроль за наслідками його діяльності для природи, людини, суспільства. «Індустрія-4.0» загострить і безліч соціальних питань: працевлаштування та зайнятість; безробіття; перекваліфікація; система соціального захисту працюючих та тимчасово непрацюючих (виплата лікарняних, вагітні жінки тощо); пенсійне забезпечення; соціальне страхування тощо. Ці та споріднені з ними питання потребуватимуть чіткого нормативно-правового врегулювання, у т.ч. і в Україні. Адже внаслідок розвитку «промислового Інтернету» у країнах-лідерах (розвинені країни світу) переважна більшість працівників реального сектору як в цих країнах, так і в країнах, що розвиваються (імпортерах продукції «Індустрії-4.0») – втратять роботу, стикнуться з необхідністю кардинального реформування сфери соціального забезпечення.

NBIC-технології, роботизація, Інтернет речей логічно призведе до кардинальних зрушень на ринку праці. Зникнуть традиційні професії, а на їх зміну будуть приходити принципово нові спеціальності та професії,

наприклад: персональний консультант з соціальних комунікацій, зі здорового способу життя; керуючий таксі-дроном; «ейчар»; працівники «креативної економіки» та інші спеціальності, назви яких ще тільки формуються. Внаслідок розвитку Інтернет на ринку робочої сили будуть домінувати «віддалені співробітники», «фрілансери», «ситуативні працівники», що не потребують стаціонарного робочого місця під час виконання роботи. В таких умовах для юриспруденції формується виклик щодо реформування системи оподаткування, відрахувань на соціальні потреби, пенсійних внесків. Або ж, як один з варіантів, виникає виклик повної відмови від традиційної системи «адміністрування податків» з бізнесу та працюючих (оподаткування прибутку та доходів) і пошук нових, інноваційних підходів щодо оподаткування та соціального забезпечення. Як варіант – виникають пропозиції «перенести» увагу оподаткування у XXI ст. виключно у сферу обігу.

Стратегічним пріоритетом розвитку NBIC – технологій у XXI ст. стає сектор «економіка здоров'я», що охоплює широкий спектр бізнес-інтересів – від сфери органічного харчування, фітнес-центрів і до сучасної нано-медицини, де використовуються останні новинки мікрохірургії, генетики, біотехнології, лікування на біо-клітинному рівні. За експертними оцінками, глобальний ІТ-ринок «економіки здоров'я» до 2020 року у вартісному вимірі зростатиме щорічно на 10 – 15 % [5]. Перспективним для «економіки здоров'я» є застосування «3D-прінтерів», розвиток біопрінтінгу та регенераційної медицини, що поєднує «3D-друк» стовбурових клітин і тканин, органів людини (для трансплантації органів). Медичні працівники та біоінженери вже мають позитивний досвід «друку» на «3D-прінтері» кровоносних судин, придатних для пересадки людині. Проводяться дослідження у сфері нано-медицини щодо виготовлення нових (штучних) органів тіла людини, які будуть «друкуватися» із здорових клітин самого ж пацієнта. Це може вирішити питання дефіциту донорських органів, покінчити з «чорною трансплантацією». Такий блок проблем потребує створення відповідної нормативно-правової бази.

Фахівці у сфері нано-медицини стверджують, що все сьогодні є реальністю подовження активного (працездатного) періоду життя людини до 120 – 130 років. Водночас такі наукові дослідження до певного часу тримаються у таємниці, адже їх масове впровадження на практиці може призвести до загострення низки соціально-економічних та екологічних проблем: зміни вікових меж виходу людини на пенсію та загострення проблеми працевлаштування людини, зростання безробіття; дефіцит продовольства (ризики голоду); перенаселення та масова міграція людей у планетарному масштабі (одночасно із зростанням кількості «кліматичних біженців») та ін. Збільшення віку проживання людини загострить питання пенсійного забезпечення, а роботизація виробництва («Індустрія-4.0», промисловий Інтернет) [3; 4; 5], взагалі поставить питання про відмову від традиційної системи оплати праці та системи соціальної допомоги (соціальних виплат), що призначаються для працюючих та соціально-вразливих верств населення. На порядку денному може постати питання про введення «безумовного базового доходу» (ББД). Експеримент щодо виплати ББД уже триває у деяких країнах світу (Фінляндія). Водночас законодавче забезпечення виплати ББД відсутнє.

Для переважної кількості споживачів застосування NBIC – технологій, насамперед, пов’язується із сферою інформаційних технологій (комп’ютерна та інформаційна техніка), що у XXI ст. активно інтегруються з усіма сферами бізнесу: банківською діяльністю, ринком страхових послуг, фондовим та валютним ринком, зі сферою грошового обігу (у т.ч. йдеться про Інтернет як фундамент існування кріптовалют). Bitcoin, Ripple, NEO, emCash та ін. Кріптовалюти ставлять під сумнів традиційну монополію держави на емісію грошей та на державний контроль за обсягом грошової маси (традиційно – це є сфера дії Національного банку). Відповідно – порушується монополія держави на розробку макроекономічної, монетарної, стабілізаційної економічної політики. Законодавче унормування фінансових трансакцій, здійснених за допомогою кріптовалюти, в Україні відсутнє та потребує розробки.

Інтернет кардинально змінює систему соціально-економічних відносин, модифікує право власності, порядок володіння, користування, розпорядження благом (матеріальним та нематеріальним), засобами виробництва, змінює традиційні уявлення про ринок товарів та послуг, робочу силу, про ринок фінансів та торгівлю. Інтернет змінює «правила гри» на ринку, змінює інструменти та механізми регулювання господарських процесів, модифікує уявлення про роль та повноваження держави. Все це потребує кардинальних змін правового регулювання та впровадження у всіх сферах господарської діяльності, у т.ч. і у сфері таких його важливих складових як Інтернет речей та Інтернет послуг.

Література:

1. Internet Trends 2017 – CODE CONFERENCE Mary Meeker May 31, 2017 (kpcb.com/ Internet Trends 2017). KLEINER PERKINS [Електронний ресурс]. – Режим доступу: http://www.smartinsights.com/digital-marketing-strategy/9-global-internet-trends-inform-2017-strategy/
2. 2016 Global Games Market Report. AN OVERVIEW OF TRENDS & INSIGHTS. Newzoo Games [Електронний ресурс]. – Режим доступу: https://cdn2.hubspot.net/hubfs/700740/Reports/Newzoo_Free_2016_Global_Games_Market_Report.pdf
3. Converging Technologies for Improving Human Performance NANOTECHNOLOGY, BIOTECHNOLOGY, INFORMATION TECHNOLOGY AND COGNITIVE SCIENCE *NSF/DOC-sponsored report* / Edited by Mihail C. Roco and William Sims Bainbridge National Science Foundation 2003 Kluwer Academic Publishers (currently Springer) Dordrecht, The Netherlands (482 pages, Web version. See ISBN 1-4020-1254-3 for archival print version). [Електронний ресурс]. – Режим доступу: http://www.wtec.org/ ConvergingTechnologies/ Report/NBIC_report.pdf
4. Industry 4.0. Summit. (2017). / [Accessed 22 Apr. 2017]. [online] Available at [Електронний ресурс]. – Режим доступу: http:// www. industry40summit.com
5. Nibc.com. (2017). Nanotechnologies, Biotechnologies, Information technologies and Cognitive sciences (NBIC convergence) [Accessed 27 Apr. 2017]. [online] Available at: [Електронний ресурс]. – Режим доступу: http://nibc.com/

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

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

ПІДХОДИ ЩОДО ВИЗНАЧЕННЯ СТАТУСУ КРИПТОВАЛЮТ: УКРАЇНСЬКІЙ ПІДХІД

Законопроекти про легалізацію криптовалют: «Про обіг криптовалюти в Україні» та «Про стимулювання ринку криптовалют та їх похідних в Україні» [1], подані до Верховної ради у жовтні 2017 року, пройшли обговорення у комітеті з питань фінансової політики і банківської діяльності. До обговорень долучилися представники Національного банку України (НБУ), Міністерства фінансів України, інших державних органів ринку криптовалюти та експерти. 30 жовтня цього ж року подано ще один законопроект «Про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні)»[2].

Законопроекти визначають основні напрями державної політики у відносинах щодо криптовалют. Метою цих законопроектів, перш за все, є намагання підвести обіг криптовалют під фінансове регулювання.

У пояснювальній записці до проекту Закону України «Про обіг криптовалюти в Україні» зазначається, що Україна входить до країн-лідерів у сфері застосування криптовалюти і технології блокчейн та є ідеальним місцем для розвитку новітніх технологій [3].

Мабуть саме це спонукало Національний банк України (НБУ) змінити свою думку про таке, вже досить реальне, явище (реальне не тільки в Україні а й в усьому світові), як криптовалюта. Адже центральна державна регуляторна інституція України вперто не признавала криптовалюту, зокрема і біткойн (Bitcoin). Офіційне непризнання було заявлено ще в 2014 році. Так, 10.11.2014 року у соцмережах з'явилося «Роз'яснення щодо правомірності використання в Україні "віртуальної валюти/криптовалюти" Bitcoin» [4]. Нацбанк у зазначених роз'ясненнях посилався на відповідні норми чинного законодавства, починаючи з Конституції України. Зокрема було підкреслено,

виходячи з Декрету «Про систему валютного регулювання і валютного контролю»[5], що валюта України є єдиним законним засобом платежу на території України, який приймається без обмежень для оплати будь-яких вимог та зобов'язань, якщо інше не передбачено цим Декретом, іншими актами валютного законодавства України. Так само було вказано і на частину другу статті 32 (чинну на сьогодні) Закону України "Про Національний банк України" [6], яка встановлює, що випуск та обіг на території України інших грошових одиниць і використання грошових сурогатів як засобу платежу забороняються. З того часу Нацбанк України не змінював свого ставлення до криптовалюти і ще в серпневих (2017 року) прес-релізах намагався пояснити своє ставлення до криптовалюти, виходячи зі складності однозначної трактовки цього явища і віднесення його до тих чи інших термінів, які існують у чинному законодавстві.

Подібну думку висловив у роботі круглого столу на тему "Криптовалюта в Україні: фінансова бульбашка чи гроші майбутнього?" зокрема й Емал Бахтарі, - керівник проектів і програм департаменту відкритих ринків НБУ, зазначивши, що виходячи зі ставлення Нацбанку, він повторюється, що «дане явище складне, воно не підпадає ні під одне з визначень, які ми сьогодні маємо. Це не валюта, не іноземна валюта, не електронні гроші. Це не грошовий сурогат, - навіть в цьому плані ми на сьогодні впевнені, що це явище не можна назвати однозначно таким терміном»[7]. Більш того, НБУ вважає підготовку законопроектів про легалізацію криптовалют передчасною, а самі законопроекти – недоробленими, враховуючи той факт, що природа криптовалюти виглядає досить заплутаною і юридично не визначеною.

Виходячи з багатьох джерел, що присвячені проблемам визначення поняття «криптовалюта», слід зазначити, що однозначно пояснити що ж таке криптовалюта не можуть і відомі і ключові регулятори світу, зокрема Європейський центробанк (ЄЦБ). У жовтні 2012 р. ЄЦБ під віртуальною валютою розглядав тип нерегульованих цифрових грошей, які випускаються

і, як правило, контролюються їх розробниками та використовуються серед членів певного віртуального співтовариства. Проте вже у лютому 2015 р. ЄЦБ уточнив свій підхід: віртуальна валюта як цифрове подання вартості, не виданих центральним банком, кредитною організацією або установою електронних грошей (e-money institution), яка в деяких випадках може бути використана як альтернатива грошам [8]. А взагалі, Захід на сьогодні пропонує зачекати і подивитись, що буде у недалекому майбутньому.

Фактичне становище на рику криптовалют дозволяє говорити про те, що у біткоїни та інші види криптовалют на сьогодні повірила суттєва кількість людей. Не секрет, що на біткоїні (та інших криптовалютах) багато людей заробили чимало грошей. Біткоїнами вже розраховуються і вони отримують все більшу популярність. У багатьох країнах у тому числі і в Україні є термінали з обміну біткоїнів на реальні гроші. І якщо люди продовжують вкладати у свої очікування і вірять у великі прибутки то, звісно, що ціна на біткоїни і іншу популярну криптовалюту буде зростати.

Насправді ж, невідомо що собою представляє криптовалюта, чому вона так дорого котирується на відповідних біржах? Можливо це завершиться крахом, а можливо і ні. Так чи інакше, але не можна не помічати того явища, що існує об’єктивно і, відповідним чином, держави повинні мати певну юридичну визначеність.

Щодо юридичної визначеності то над цим слід ще працювати. Так вважає і Національна комісія з цінних паперів і фондового ринку (НКЦПФР). Вона наполягає на доопрацюванні, поданих до Верховної ради законопроектів про криптовалюти [9].

Зазначені законопроекти викликали не аби яку увагу не тільки з боку державних інституцій. У соцмережах можна побачити різні коментарі з цього приводу і від громадян – користувачів різних соціальних мереж. І, мабуть, більшість з них висловлюють приблизно таку думку: «… криптовалюту треба залишити у спокою, краще не регулювати, не «допомогати», краще не заважати…» .

Певні запитання викликає і законопроект № 206. Питання у даному випадку у першу чергу постають перед податковими органами і в Україні і в інших країнах. Знову ж таки, - яким саме чином визначити правову природу такого явища, як криптовалюта? І звідси вже, - як кваліфікувати певну операцію, з якої необхідно стягнути податки?

До речи, законопроектом № 7183 (част 1 ст. 7) встановлюється, що до криптовалютних транзакції застосовуються загальні положення про договір міни, у відповідності до законодавства України. То, якщо розглядати, наприклад, операцію з купілі-продажу майна, скажімо квартири, як договір міни, то за чинним законодавством слід стягнути податок як з однієї операції так і з зустрічної операції. Якщо ж йдеться про купівлю-продаж, як таку, то податок справляється тільки з того, хто продає (непряме оподаткування). Такі саме дії і що до доходу. Також, слід зазначити, що за чинним законодавством України, сьогодні не існує операцій, які б не обкладалися податками. Тому, у законопроекті «Про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні)» передбачені певні можливості оподаткування операцій за участю криптовалют. Чи реально законодавчо врегулювати ці та інші зазначенні намагання, покаже розгляд цих законопроектів Верховною Радою України остаточне їх прийняття, як Закону.

Література:

1. Проект Закону від 6.10.2017 № 7183 «Про обіг криптовалюти в Україні», вноситься народними депутатами України Єфремовою І.О. Денісовою Л.Л. Котвіцьким І.О. Рибаком І.П. Войцеховською С.М. - [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684; Проект Закону від 10.10.2017 № 7183-1 «Про стимулювання ринку криптовалют та їх похідних в Україні», народним депутатом України Рибалкою С.В.

2. Проект Закону про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні)від 30.10.2017 № 206, вноситься народним депутатом України Рибалкою С.В. - [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62816

3. Див.: Пояснювальна записка від 06.10.2017. Проект Закону Про обіг криптовалюти в Україні. - [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/ webproc4_1?pf3511=62684.

4. Роз'яснення щодо правомірності використання в Україні "віртуальної валюти/криптовалюти" Bitcoin. – Національний банк України. Офіційне веб-предстваництво. - [Електронний ресурс]. – Режим доступу: https://www.bank.gov.ua/control/uk/ publish/article?art_id=11879608

5. Про систему валютного регулювання і валютного контролю. Декрет Кабінету міністрів від 19.02.1993N 15-93. - [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/ laws/show/15-93

6. Про Національний банк України . Закон України **від** 20. 05. 1999 № 679-XIV. - [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/679-14

7. Див.: Криптовалюти в Україні: фінансова бульбашка чи гроші майбутнього? Конспект. Матеріали круглого столу, що відбувся 6.10.2017 в Інституті Горшеніна. - [Електронний ресурс]. – Режим доступу: https://ukr.lb.ua/economics/2017/10/26/379452_kriptovalyuti_ ukraini_finansova.html

8. С. В. Волосович. Віртуальна валюта: глобалізаційні виклики і перспективи розвитку Науковий журнал "Економіка України". — 2016. — 4 (653). – С. 69

9. Позиція НКЦПФР щодо законопроектів з питань врегулювання обігу криптовалют. - Офіційний сайт НКЦПФР. - [Електронний ресурс]. – Режим доступу: https://www.nssmc.gov.ua/ 2017/11/02/pozitsya-nktspfr-shtodo-zakonoproektv-z-pitany-vregulyuvannya-obgu-kriptovalyut/

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

Чорнолуцький Р. В.,
докторант Інституту законодавтсва Верховної Ради України, адвокат, старший партнер адвокатської групи "Катеринчук, Моор і партнери"

ДОРОЖНЯ КАРТА ЗАКОНОДАВЧИХ ІНІЦІАТИВ ЩОДО ВРЕГУЛЮВАННЯ ТА ВИКОРИСТАННЯ КРИПТОВАЛЮТ В УКРАЇНІ

№1 Яку політику вибрати: дозволити або заборонити криптоактиви ?

Ще пару років тому сама думка про те, щоб на державному рівні в Україні обговорювали б перспективи розвитку крипто валюти, технології блокчейн

здалася б утопічною. Спочатку , виникнувши як засіб платежу в окремих групах, віртуальна валюта стала поширюватися настільки стрімко, що вже перевершила найсміливіші очікування своїх розробників. Обсяги її обороту ставлять перед вченими і практиками ряд гострих питань, пов'язаних з правовим регулюванням сучасних платіжних систем, економічними вигодами і кримінологічними ризиками використання крипто валюти, проблемами технічного забезпечення її обороту, а також перспективами розвитку крипто валюти в світі і, звичайно, в Україні. На сьогодні, саме в Україні можна визначити такі тренди щодо питання блокчейна, криптовалют і всіх інших похідних можливостей, які дає ця технологія з боку суспільства і державних органів:

1. Тотальну повну заборону - чорна зона

2. Не забороняти і не дозволяти - сіра зона

3. Дозволити і дати правове визначення з правом регулювання - зона комфорту

4. Дозволити тотально все і не втручатися - біла зона (утопічна позиція)

№2 Що визначає привабливість юрисдикції? Слід зазначити, що поки питання використання криптовалюта підлягає більшому регулюванню, особливо на законодавчому рівні. Стосовно цього в Україні поки повна тиша, і крім деяких публічних заяв про наміри, нічого конкретного не робиться. Такі передові технології, як електронна готівка, рано чи пізно, прийдуть в Україну, ставши звичним способом для взаєморозрахунків для громадян. Загалом, використання криптовалют є новим способом здійснення платежів в електронній комерції. При належному удосконаленні технології, законодавче регулювання та поліпшення відповідної інфраструктури дана технологія займе значне місце в повсякденному житті. Однак, висловлювання деяких юристів і кріптоінвесторов про те, що краще залишити зараз в Україні все як є - зробити зразкову сіру зону в питанні просування криптовалюта і технології блокчейна це тим паче шлях в нікуди. Мотивувати тим, що сіра зона - це повна свобода від регулювання, які не є практичний і

ефективний підхід. Якщо подивитися на список країн, які є сьогодні лідерами в просуванні віртуальної економіки, згідно Bitcoin Foundation, а ми говоримо про Швейцарію, Канаду, Австралію, Сінгапур та ще ряд держав, то зрозуміло, що їх високий рейтинг і потенціал, перш за все, обумовлений тим , що вони прописали чіткі правила гри, дали визначення і пояснення в особі регуляторів, і гарантують моніторинг в правовому полі взаємовідносин всіх учасників кріпторинку. Чіткі прописані правила гри - ось що визначає привабливість юрисдикції, а не політика невтручання. Щоб не винаходити власний велосипед, варто подивитися, як інші юрисдикції ставляться до питання кріптовалютного регулювання. Мета такого обов'язкового аналізу для законотворців - має бути СПІЛЬНЕ РОЗУМІННЯ ПРАВОВИХ АСПЕКТІВ І МЕХАНІЗМІВ ФУНКЦІОНУВАННЯ НОВОЇ ТЕХНОЛОГІЇ, а не традиційна для України - правова бравада і не системність. Провівши і проаналізувавши основні правові тези і пріоритети провідних країн, можна побачити, що Закон не повинен прагнути регулювати будь-яку нову технологію. Регулювати треба-ризики.

№3 Висновки основних правових пріоритетів провідних світових юрисдикцій:

1.Позитивні

1. Ліцензування кріптобірж

2. Офіційни заяви про те, що криптовалюта - не гроші, але віртуальна валюта. Можна розплачуватися

3. Регулювання, в першу чергу, з метою дотримання ПОД / ФТ (Протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансуванню тероризму)

4.Створення «регуляторних пісочниць» і пом'якшення вимог

2.Негативні

1.Високи вимоги до отримання ліцензії (дорого!)

2.Офіційни негативні висловлювання

3.Логіка регулювання

1.Існує об'єктивний ризик - поява нових можливостей для відмивання доходів, одержаних злочинним шляхом, фінансування тероризму

2.Окремі органи окремих країн - операції з криптовалютою – гарний заробіток для державної скарбниці (Японія)

3.Регулювання поширюється, в першу чергу, на хаби (біржі, обмінники), а не на творців токенов.

№4 Дорожня карта законодавчих ініціатив Безсумнівно, слід зазначити актуальність і новизну розгляду питань використання технології блокчейн як в контексті розробки національної стратегії економічної безпеки, так і в рамках міжнародного співробітництва. Основний пріоритет тут - вирішення проблеми фінансової безпеки держави і зацікавленість законодавчої влади у вивченні механізмів впровадження в національне законодавство «складної матерії криптовалюта», звичайно, ж, детально вивчивши вже наявні напрацювання в світі по даному питанню. Основним завданням державного регулювання в Україні повинна стати мета в з'ясуванні природи сучасних фінансових технологій і розширення меж права шляхом визначення ризикоорієнтованих факторів, і на цій основі поетапного включення в ці регулятори перспективних розрахункових інструментів. Успіх криптовалют безпосередньо залежить від того, як швидко законодавець зможе звести нанівець ризики її обороту і визначити «зону гарантованої свободи» користувачів. Всі лідируючі світові юрисдикції намагаються знайти відповідь на таке питання! Тому первинно слід зрозуміти і правильно виявити відповіді на наступні питання, пов'язані з обігом криптовалюти:

1) в чому полягає економічна і предметна сутність крипто валюти;

2) які ризики несе в собі обіг крипто валюти і як вони співвідносяться з перевагою її впровадження?

3) чи є крипто валюта грошовим сурогатом?

4) які стратегії її легалізації можливі в короткостроковій і довгостроковій перспективі?

При розробці механізмів безпеки обігу крипто валют, варто пам'ятати завжди про три моделі ризикоорієнтованого підходу до кримінальних схем використання крипто валют, які практикуються сьогодні:

1) доходи від кібератак обмінюються на біржах, кошти надходять в кредитний кооператив, а потім переводяться на ошфорні рахунки;

2) крипто валюта, отримана в результаті незаконної мережевої торгівлі, обмінюється на товарних біржах, далі перекладається на карти і знімається в банкоматах;

3) використовується електронний гаманець, в який незнайомі один одному люди закладають гроші у вигляді крипто валюти, і згодом ці гроші частинами повертаються відправникам.

Звідси, з огляду на світовий досвід боротьби з відмиванням брудних доходів, варто в українському законодавстві застосувати три стратегії легалізації крипто валюти:

1) прирівнювання крипто валюти до платіжних інструментів;

2) збереження переваг блокчейн як платформи, на якій працює крипто валюта;

3) створення своєрідної національної крипто валюти, яка дозволила б виключити ризик маніпулювання курсами (до речі, Естонія вже думає про це!).

Взагалі, перш ніж починати питання регулювання, слід на рівні держави і національного нормопроектування з'ясувати основні три аспекти обговорення природи крипто валюти:

1) технічна сторона - блокчейн має перспективи і істотно знижує витрати на вироблені транзакції;

2) правова природа - розробка легального визначення «грошовий сурогат»;

3) економічна сторона – мильна бульбашка, не забезпечена активом.

4) З точки зору правових питань крипто валюту необхідно розцінювати як об'єкт правового регулювання, і в зв'язку з цим юристам і економістам

необхідно прийти до консенсусу щодо її визначення як формального інституту.

5) З небезпек варто відзначити ризик падіння економічної цінності криптовалют в разі її обміну фінансовими посередниками на фіатни гроші. Наприклад, в світовому просторі піонером в сфері мінімізації ризиків обігу криптовалюти можна визнати Канаду, яка ще в 2014 р. регламентує діяльність фінансових установ та прямо вказала на обіг криптовалюти як ліцензованої діяльності. Як приклад комплексного підходу до регулювання питань обігу біткоіни був відзначений і закон штату Нью-Йорк 2015 р, де закінчення необхідно відзначити недоцільність регламентації в національному кримінальному та адміністративному законодавстві відповідальності користувача криптовалюта. Прикладом можна використовувати такий зарубіжний досвід легалізації обігу криптовалюти в США, Японії, Швейцарії, і ряді інших держав.

6) Безсумнівно, при грамотному національному регулюванні питання сутності блокчейн-технології, полегшенні і спрощенні процедури інвестування в розподілені реєстри, у користувачів з'являється можливість позбутися від більшості бюрократичних процедур за допомогою системи «розумних контрактів»; підвищується рівень кібербезпеки і виключається «чорна бухгалтерія». Але, щоб досягти таких результатів, державі слід виробити єдиний алгоритм - єдиний системний підхід правового регулювання.Асаме:

7) Провідні державні регулятори у сфері фінансової, банківської, податкової, телекомунікаційної, інформаційної, правоохоронної, реєстраційної та інших сфер, повинні разом створити Колегію для вироблення колективних думок, стратегії і плану імплементації регуляторних актів.

8) Регулятори повинні чітко визначитися, що є таке біткоіни - валюта, актив, віртуальні гроші, електронні гроші і так далі. І тільки виходячи з єдиної концепції будувати вже під єдину думку законодавчу ініціативу, щоб

уникнути правових колізій, чим славиться національне законодавство.

9) Такий же підхід стосується визначення токенов, що це таке в правовому плані. Це цінний папір, актив, пайова участь або що - небудь ще. І тільки після єдиної концепції будувати вже правові визначення і рамкиICO

10) Тільки спільно з участю всіх перерахованих вище регуляторів і фахівців (експертів) в частині права, економіки, даної технології розробляти спільно базовий законопроект щодо регулювання і правовим статусом криптовалюта та інших похідних можливостей

11) Такий законопроект в ідеалі повинен визначити наступне:

➢ Природу криптовалюта

➢ Основних учасників ринку і операційної діяльності

➢ Основні принципи діяльності (статус)

➢ Визначити основні взаємопов'язані параметри

➢ Систематизувати процедури використання криптовалюта для здійснення розрахунків, перерахування цифрових активів між учасниками ринку, включаючи фізичних осіб

➢ Дати можливість банківському сектору запускати нові системи взаєморозрахунків і спростити процедуру покупки ІТ підприємств (і не тільки)

➢ Дати визначення і прописати основні положення і правила для діяльності кріптовалютних бірж в Україні

➢ Прописати основні вимоги і процедуру отримання ліцензії на здійснення такої цифрової біржової діяльності

➢ Прописати і продумати основні пріоритети контролю і моніторингу, аудиту діяльності кріптовалютних бірж

➢ Детально виявити весь список внесення необхідних поправок і доповнень (включаючи прикінцеві положення) до Цивільного, Кримінального та інші кодекси і взаємопов'язані законодавчі чинні акти і закони

➢ Окремо подумати про питання оподаткування такої діяльності в частині податку на прибуток, прибуткового, і інших. Використовувати при цьому найбільш ефективні інструменти і ставки, які використовуються в передових економіках в частині розвитку та просування крипто ринку

➢ Врахувати основні міжнародні вимоги в частині боротьби з відмиванням доходів, одержаних злочинним шляхом та фінансування тероризму

➢ Необхідно все ж таки налагодити діалог між представниками даної індустрії і урядом. Те, що є сьогодні - розрізнені групи впливу з різними індивідуальними інтересами, які в принципі не враховують інтересів держави та представників кріптобізнеса.

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

Соловйов С. Г.,
к. н. із соц. ком., доцент,докторант кафедри інформаційної політики та цифрових технологій Національної академії державного управління при Президентові України

МЕРЕЖЕЦЕНТРИЧНІСТЬ У ПУБЛІЧНОМУ УПРАВЛІННІ

Сприйняття інтернету як останнього на останнього на сьогодні, одинадцятого рубежу комунікації [1] уже потребує дискусійного погляду через феномен інтернету речей (IoT), який відображається на рівні соціально-економічних аспектів життя. Мережецентричний характер IoT демонструє комунікативний потенціал як усередині певної локальної системи, так і на рівні зв'язку з іншими системами. Якщо це обговорювати крізь призму рубежу комунікації, це може привести до висновку про технологічну революцію, і навіть про нову форму управлінських стосунків.

Вжитий вище термін "комунікативний" варто сприймати доволі умовно, оскільки насамперед окреслюється обмін інформацією між технічними пристроями. Проте людина, володіючи цими пристроями, затребує частину інформації, може передавати її іншій людині і таким чином комунікувати.

Головним у цьому вбачаємо те, що описувана інформація генерується мережею для мережі, а людина при цьому вибірково її використовує (наприклад, для уточнення, перевірки, налаштування роботи системи).

Мережецентричність у людській діяльності не обов'язково потребує технічних рішень. Такі конструкти з різними типами відносин, як ланцюжок (послідовна передача інформації від суб'єкту до суб'єкту), зірка (передача інформації через центр до периферії), колесо (багатоканальний рух інформації і через центр, і між суб'єктами периферії) описані дослідниками "Rand corporation" [2] і цілком реалізуються у практиці людських спільнот при безпосередньому спілкуванні. Соцмережі з їх горизонтальним комунікаціями і різноманітними групами є прикладом втілення подібних варіантів, але вже з використанням інтернету. У цьому разі мережа фізичних суб'єктів нарощується за допомоги віртуальних учасників.

Зайвим буде говорити, що саме остання наведена тут модель (рух інформації і через центр, і між віддаленими суб'єктами) практично нівелює центр, який стає рядовим суб'єктом у цьому процесі, що лише позитивно впливає на ефективність виконання завдань системи. Але для публічно-управлінських процесів, це, вочевидь, виклик. Адже рішення приймаються на рівні влади, а це ознака центру, навіть коли прийняття рішення відбувається під впливом периферії, тобто в даному разі громадськості.

Тому, зважаючи на характеристики багатоканальності цієї моделі у публічному управлінні, центр не нівелюється, а набуває ознак динамічності.

Відповідно, постають питання:

1)де є центр у кожен конкретний момент; 2)який саме учасник мережі у цей момент є центром; 3)за яких умов центр переміщується; 4)у яку точку він переміститься в наступний момент; 5)як можна утримати центр у заданих параметрах.

Можна вважати вірогідною мережецентричність у публічному управлінні, яка з цього погляду – процес здійснення більш-менш постійних і формалізованих зв'язків між громадянами, бізнесом та владою. Тут варто

цілком погодитися із тим, що “поняття «багатосторонні зацікавлені сторони в управлінні» повинно сприйматися як новий шлях на користь включення всього суспільства” [3]. Відповідно, суспільство зацікавлене застосувати IoT як технологію, за допомоги якої досягаються блага, приміром, консенсус. І здійснення такого кроку означає перехід на мережецентричність відповідно до моделей е-урядування G4G – “уряд для уряду”, G4C – “уряд для громадян”, G4B – “уряд для бізнесу”, G4E – “уряд для службовців”.

Якщо G4G – це своєрідна розумна державна установа, то G4C можна назвати розумною публічною владою. Це мережа, яка працює для всіх, тому центр може переміщатися в залежності від цілей і контексту їх реалізації. Це особливо виразно виявляється у практиці е-демократії на прикладі одного з найновіших її інструментів – партисипаторних бюджетів (бюджетів участі). Влада, відповідальна за формування місцевого бюджету, і громадяни, які пропонують, на що бюджет витратити (у певних межах) – де тут усталений центр? Ще один приклад мережецентричності – перехід державного земельного кадастру на блокчейн, втілений у Міністерстві аграрної політики та продовольства України [4]. Звісно,на цьому етапі не задіяний власне публічно-управлінський вимір, проте гарантується захист мережею реєстру, що вказує на перспективність безпеки е-ресурсів в операціях впливу.

У дослідженнях, присвячених розгляду проблем мережецентричного суспільства часто цитуються спостереження про характер останнього: зміна фокусу з платформи на мережу; перехід від розгляду акторів як незалежних суб’єктів до їх трактування як частини постійно змінюваної системи; важливість прийняття стратегічних рішень, спрямованих на адаптацію чи навіть виживання в змінних екосистемах [5].

По двох десятиліттях після згаданої публікації можна впевнитися у справедливості викладених положень, при цьому для України ще попереду багато нового. Громадське суспільство продемонструвало і демонструє нині значний потенціал: активісти, які жертвували життями під час Революції Гідності, добровольці, які йшли в зону бойових дій на Сході, волонтери, які

організовували допомогу війську. Зараз зусилля громадянського суспільства значною мірою спрямовані на вирішення актуальних проблем, наприклад, у сфері боротьби з корупцією. Ці приклади – водночас і приклади мереж. Проте невідомо, якою мірою вітчизняне публічне управління сприйме мережецентричність як прояв IoT.

Вбачається доречним навести коментар до вищезгаданого джерела – не такий цитований, як сама книга, але який може виявитися важливим для розуміння шляхів реалізації моделі розумної публічної влади.

Отже, Г.Рубенштейн, як практик у бізнесі, державному управлінні, стратегічному плануванні, комунікаціях пише, що в неприбутковому середовищі домовленості про розподіл доходів та інших ресурсів можуть бути тим клеєм, який створює міцний зв'язок між неприбутковими організаціями та серед неприбуткових організацій. Кожна зацікавлена сторона повинна мати додаткові, а не конкуруючі інтереси. Повинна бути спільна етика, яка дозволяє всім зацікавленим сторонам працювати разом, і нікому не обманювати інших [6].

Можна заперечити, що це не обов’язково стосується ознак мережецентричного публічного управління. Проте варто погодитися, що це бачення принесе користь при його здійсненні.

Отримавши для себе відповідь на питання про необхідність мережецентричності у публічному управлінні та готовності подолати виклики для переходу в цю якість, можна стверджувати: інтернет речей із часом перейде у явище, що дістане назву, наприклад, інтернет трансформацій. Це, розширення можливостей суспільства, в якому публічне управління відіграватиме інакшу роль, для характеристики якої у нас поки що мало даних.

Література:

1. Партико З.В. Теорія масової інформації та комунікації : Навч.посібник. – Львів : Афіша, 2008.

2. J. Arquilla, D. Ronfeldt. The Advent Of Netwar [Електронний ресурс]. – Режим доступу: https://www.rand.org/pubs/monograph_reports/MR789.html.

3. Rolf H. Weber, Romana Weber. Governance of the Internet of Things. Legal Perspectives. Springer-Verlag Berlin Heidelberg, 2010. – 135 p. – P.69

4. Державний земельний кадастр перейшов на технологію Blockchain [Електронний ресурс]. – Режим доступу: http://www.minagro.gov.ua/uk/node/24722.

5. James F. Moore, “The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems,” HarperBusiness, 1996.

6. Book Review and Commentary by Herb Rubenstein, President, Sustainable Business Group [Електронний ресурс]. – Режим доступу: http://www.herbrubenstein.com/articles/THE-DEATH-OF-COMPETITION.pdf

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

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

РЕЗУЛЬТАТИ ТВОРЧОЇ ДІЯЛЬНОСТІ ЯК ОБ’ЄКТИ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ: СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ

Сьогодення – час глобалізації, ера стрімкого розвитку та нових технології, де світ - величезне інформаційне поле. Масштаби поширення інформації зумовлюють появу нових інформаційних потреб і викликів.

Інформація, незалежно від того, який вона має вигляд – це цінний ресурс, що впливає на нашу діяльність: економічну, соціальну, культурну, та навіть творчу. Саме творчість та інформація в цій сфері діяльності є об`єктом даних роздумів.

Для початку необхідно розібратися, що ж таке «творчість». Відповідно до визначення, що дається в Словнику української мови, творчість – це діяльність людини, спрямована на створення духовних і матеріальних цінностей, а також те, що створено внаслідок такої діяльності, сукупність створеного кимось. Тобто творчість може охоплювати будь-яку сферу діяльності людини (створення творів мистецтва, наукові відкриття, інженерно-технічні інновації тощо), якщо процес спрямований на створення духовних чи матеріальних цінностей.Також необхідно визначити чи регулюються питання пов’язані з творчістю українським законодавством.

Відповідно до Закону України «Про авторське право і суміжні права» об’єктами авторського права є твори у галузі науки, літератури і мистецтва. Таким чином, якщо об’єктом творчої діяльності є твори в галузі науки, літератури або мистецтва, то питання пов’язані з їх захистом регулюватимуться Законом України «Про авторське право і суміжні права». З кожним роком кількість людей, які бажають захищати свої творчі доробки збільшується, а різноманіття «результатів» творчої діяльності нестримно зростає, інколи дивуючи не тільки пересічних громадян, а й правозахисників, на яких падає тягар їх захисту. Саме тому ця тема є актуальною.

Україна взяла курс на євроінтеграцію й усіма своїми силами намагається адаптувати вітчизняне законодавство до європейського. Але варто бути справедливими й зауважити, що навіть ідеально прописані норми, не забезпечують повноцінної інформаційної безпеки даних, у випадку відсутності реального механізму їх захисту.

Ще однією проблемою вітчизняного законодавства є деяка «відсталість» від часу. Стрімкий розвиток, поява все нових і нових технологій, продуктів та каналів передачі інформації, як правило, дуже сильно випереджає наші закони.Українські реалії зараз такі, що все більше і більше сфер діяльності знаходять свою нішу саме в Інтернет - мережі. Економічна, культурна, соціальна та творча діяльність рік за роком все більше переносяться саме на простори Інтернету.В Законі України «Про авторське право і суміжні права» є лише кілька положень стосовно захисту авторських і суміжних прав, зокрема, визначений порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет. Таким чином, питання захисту інформації на теренах Інтернету стає ще гострішим, адже фактично нормативно-правові акти, які б регулювали вже такий звичний та «всюдисущий» Інтернет відсутні, а тому і захистити продукти своє творчої діяльності напрочуд важко.

Плагіат, копіювання, незаконне розміщення, піратство – незмінні характеристики сучасного українського Інтернет - простору. Інтернет дає нам

великий спектр нових можливостей, але в той самий час і створює ряд проблем пов'язаних з ефективністю захисту та охорони інтелектуальної власності. Поширення продуктів творчої діяльності в мережі Інтернет призводить до можливості їх розповсюдження з порушенням авторських прав. Це відбувається перш за все через недостатність нормативно-правових актів які б регулювали дану сферу відносин і відсутність механізму впливу на порушників авторського права та суміжних прав в Інтернеті.

Творчість має бути об'єктом інформаційної безпеки ще й тому, що все частіше результати творчої діяльності стають об'єктами майнових правовідносин, маючи чітко визначений грошовий еквівалент, а значить їх незаконне використання спричиняє не лише моральну, а й матеріальну шкоду особам, які займаються творчою діяльністю. Тому питання захисту творчості заслуговує на увагу не лише безпосередніх суб'єктів творчої діяльності, а й правозахисників та законодавців.

Література:

1. Закон України «Про авторське право і суміжні права» від 23.12.1993 №3792-XII / Верховна Рада України . – Відомості Верховної Ради України (ВВР), 1994, N 13, ст.64
2. Словник української мови: в 11 тт. / АН УРСР. Інститут мовознавства; за ред. І. К. Білодіда. — К.: Наукова думка, 1970—1980. — Т. 10. — С. 54.

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

Коваленко Л. П.,
д.ю.н, доцент,професор кафедри адміністративного права та адміністративної діяльності Національного юридичного університету імені Ярослава Мудрого.
Ламанова А. В.,
студентка бакалаврату Національного юридичного університету імені Ярослава Мудрого.

ПОНЯТТЯ «ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Велике значення в наш час мають ЗМІ, мережа Інтернет, які надають громадянам різного виду інформацію. З кожним роком безпека наданої нам

інформації потребує контролю, бо більшість інформації є завідомо неправдивою. Розпочинаються інформаційні війни, які втілюються в життя спеціальними інформаційними операціями.

Раніше вважалося, що інформація всього лише забезпечує поінформованість людей про події й факти в навколишньому світі, але поступово ця поінформованість населення набирає більш вагомого значення. ЗМІ, мережа Інтернет використовуються як електронна зброя масового ураження, яка з кожним роком стає небезпечнішою.

Має місце підвищення ролі інформаційної сфери в житті людини, а відповідно, й інформаційної діяльності. Так, згідно зі ст. 12 Закону України «Про інформацію» від 2 жовтня 1992 р. «інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави». Основні напрямки інформаційної діяльності: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Головними видами інформаційної діяльності є: отримання, використання, поширення та зберігання інформації.

Для того, щоб суспільство отримувало правильну інформацію про певні події та факти, держава повинна забезпечити інформаційну безпеку. У національному законодавстві відсутня норма, яка містила б поняття «інформаційна безпека».

Спроба надати поняття «інформаційна безпека» – була енциклопедична група, представлена першою в Україні багатотомною юридичною енциклопедією, в другому томі (виданому в 1999 р.).

Інформаційна безпека України – один із видів національної безпеки, важлива функція держави. Інформаційна безпека України означає:

- законодавче формування державної інформаційної політики;
- створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;

- гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;
- всебічний розвиток інформаційної структури;
- підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки та техніки й особливостей духовно-культурного життя народу України;
- створення і впровадження безпечних інформаційних технологій;
- захист права власності держави на стратегічні об'єкти інформаційної інфраструктури України;
- охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою;
- створення загальної системи охорони інформації, зокрема, охорони державної таємниці, а також іншої інформації з обмеженим доступом;
- захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;
- встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів на основі договорів з іноземними державами;
- законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України.

Отже, проблема забезпечення національних інтересів і національної безпеки в інформаційній сфері поки перебуває на стадії розроблення. Інформаційна безпека стає можливою завдяки проведенню єдиної державної політики національної безпеки в інформаційній сфері, вжиттю системи заходів економічного, політичного й організаційного характеру, адекватних загрозам та небезпекам національних інтересів особи, суспільства та держави в інформаційній сфері. Для створення і підтримання належного рівня національної безпеки в інформаційній сфері розробляється система правових

норм, що регулюють відносини в інформаційній сфері, визначаються основні напрями діяльності органів державного управління, формуються або перетворюються органи та сили забезпечення інформаційної безпеки і механізм контролю та нагляду за їх діяльністю.

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

Коваленко Л. П.,
д.ю.н., доцент, професор кафедри Адміністративного права та адміністративної діяльності Національного юридичного університету ім. Ярослава Мудрого
Милейко К. С.,
студент Національного юридичного університету ім. Ярослава Мудрого

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАКОННОСТІ ІНФОРМАЦІНОЇ БЕЗПЕКИ

Забезпечення інформаційної безпеки України, безпеки її національних інтересів в інформаційній сфері передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у сфері протидії загрозам цих інтересів та впорядкування відповідного правотворчого процесу. Це пояснюється, по-перше, тим, що в умовах побудови правової держави та громадянського суспільства діяльність органів державної влади, які несуть основну відповідальність за національну безпеку, повинна регулюватися визначеними правовими нормами, які забезпечують конституційні права та свободи громадян. По-друге, інтеграція України в міжнародне співтовариство суттєво розширює можливості закріплення інформаційної безпеки держави за рахунок участі в розробці норм міжнародного права, створення міжнародної системи забезпечення безпеки інформаційної сфери як світу в цілому, так і кожної окремої держави. По-третє, реалізація гарантій прав та свобод громадян, захист національних інтересів України передбачає суттєве посилення ролі держави в регулюванні відповідних суспільних відносин, наявність відкритої та зрозумілої державної політики у цій сфері. У

зв’язку з цим останнім часом органи державної влади та науковці приділяють значну увагу обговоренню проблем удосконалення правового забезпечення інформаційної безпеки України[1, с. 25-27].

Дане правове забезпечення створюється сукупністю системи правового регулювання забезпечення інформаційної безпеки та процесу формування цієї системи. Система правового регулювання інформаційної безпеки, у свою чергу, включає масив правових норм, які регулюють відносини в даній сфері, правовідносини, що виникають на основі застосування правових норм, та відповідні правозастосовчі акти[3,с.250]. Правові норми становлять базу за безпечення інформаційної безпеки і визначають ефективність діяльності держави, суспільства та окремих громадян із захисту національних інтересів України в інформаційній сфері. До складу цієї бази входять і норми міжнародних договорів України, закони України, акти Президента України, постанови уряду, нормативні акти органів державної влади, які регулюють відносини у даній сфері.

Під нормативно-правовим регулюванням інформаційної безпеки України розуміється форма владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення і забезпечення. На сьогодні аналіз та удосконалення нормативно-правового регулювання в цій сфері є одним із важливих напрямів стратегії адміністративно-правового забезпечення інформаційної безпеки України. Так, як уже було неодноразово зазначено, нормативно-правове регулювання інформаційної безпеки у сфері прав та свобод здійснюється Конституцією України і такими базовими законами України: «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про поштовий зв’язок» та ін [4]. Вказані документи регламентують питання забезпечення інформаційної безпеки, захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації, інформаційних ресурсів, а також спрямовані на

реалізацію положень Доктрини безпеки особистості, держави і суспільства. Нині чітко простежується кількісний пріоритет нормативно-правових актів, покликаних забезпечити регулювання інформаційно-технічної безпеки щодо інформаційно-психологічної та інформаційної безпеки у сфері прав та свобод, що пов'язано, на нашу думку, з інтенсивним розвитком інформаційних технологій, а отже, з необхідністю оперативного реагування на зміни певних стандартів у цій сфері. Особливим недоліком нормативно-правового регулювання інформаційної безпеки України є розпорошення положень з цих питань у численних нормативно-правових актах різної юридичної сили[2, с.124-129].

Слід зазначити, що вимоги інформаційної безпеки повинні органічно входити у законодавство всіх рівнів, у тому числі і в конституційне законодавство, основні загальні закони, закони щодо організації державної системи управління, спеціальні закони, відомчі правові акти тощо. У цьому контексті вважаємо за необхідне навести таку структуру правових актів, орієнтованих на забезпечення інформаційної безпеки держави. Перший блок – конституційне законодавство. Норми, що стосуються питань інформатизації, інформаційної безпеки тощо, входять у нього як складові. Другий – загальні закони, кодекси (про власність, про надра, про землю, про права громадян, про громадянство, про податки, про антимонопольну діяльність тощо), які включають норми з питань інформаційної безпеки. Третій блок – закони про організацію управління, що стосуються окремих структур господарства, економіки, системи державних органів та їх статусу. Вони включають окремі норми із забезпечення інформаційної безпеки. Разом із загальними питаннями інформаційного забезпечення та інформаційної безпеки конкретного органу ці норми повинні встановлювати його обов'язки щодо формування, актуалізації інформаційної безпеки, що представляє загальнодержавний інтерес[1, с.71-75].

Четвертий блок – спеціальні закони, які регламентують конкретні сфери відносин, галузі господарства, процеси. Спеціальне законодавство у сфері

безпеки інформаційної діяльності (інформаційної безпеки) може бути представлено сукупністю законів. Особливе місце належить базовому Закону «Про інформацію», який закладає основу правового визначення всіх найважливіших компонентів інформаційної діяльності, закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. Серед інших спеціальних законів можна назвати, зокрема, «Про інформацію», Концепцію інформаційної безпеки України, закони, які забезпечують інформаційну безпеку в конкретних сферах життєдіяльності особи, суспільства, держави за напрямами державної політики забезпечення інформаційної безпеки: політичній, економічній, оборонній, державної безпеки і правопорядку, соціально-гуманітарній, науково-технологічній, екологічній, інформаційній. Підзаконні нормативні акти, як правило, регулюють правовідносини у сфері забезпечення інформаційної безпеки, що стосуються взаємодії органів державної влади, координації діяльності з цих питань тощо[1, с.75-78].

Отже, інформаційна безпека є складовою національної безпеки. У Законі досить системно формулюються основні функції, які має виконувати система забезпечення національної безпеки в усіх зазначених сферах. Їх конкретизація (з урахуванням особливостей інформаційної сфери) дає можливість визначити основні функції системи забезпечення інформаційної безпеки України. Саме склад і зміст цього блоку законів і утворює спеціальне законодавство як основу правового забезпечення інформаційної безпеки. П’ятий блок – підзаконні нормативні акти із забезпечення інформаційної безпеки. Шостий – законодавство України, що містить норми про відповідальність за правопорушення у сфері інформаційної безпеки.

Підсумовуючи, можемо зробити висновок про те, що зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах. Проблема забезпечення національних інтересів і національної безпеки в інформаційній сфері поки перебуває на стадії розроблення. Інформаційна безпека стає

можливою завдяки проведенню єдиної державної політики національної безпеки в інформаційній сфері, вжиттю системи заходів економічного, політичного й організаційного характеру, адекватних загрозам та небезпекам національних інтересів особи, суспільства та держави в інформаційній сфері.

Література:

1. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – Київ : МК-Прес, 2005. – 432 с.
2. Коваленко Л. П. Теоретичні проблеми розвитку інформаційного права України: монографія /Л. П. Коваленко. – Харків: Право, 2012. – 248 с.
3. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія / Б. А. Кормич.– Одеса: Юрид. л-ра, 2003.– 472 с.
4. Про інформацію: Закон України // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

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

Коваленко Л. П.,
д.ю.н., доцент, професор кафедри Адміністративного права та адміністративної діяльності Національного юридичного університету ім. Ярослава Мудрого.
Горбунова А. Р.,
студент Національного юридичного університуім. Ярослава Мудрого.

ЩОДО ОСНОВНИХ ЗАВДАНЬ КІБЕРПОЛІЦІЇ В СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Особливістю розвитку сучасного суспільства є підвищення ролі інформаційної сфери в житті людини, а відповідно, й інформаційної діяльності. Так, згідно зі ст. 12 Закону України «Про інформацію» від 2 жовтня 1992 р. «інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави». [2] Основні напрямки інформаційної діяльності: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо.

Багато уваги приділяється підвищенню ефективності державного управління як одній з пріоритетних функцій держави. [5, с. 227-229]

У ст. 17 Конституції України закріплено, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. [1]

У Законі України «Про основи національної безпеки України» від 19 червня 2003 р. йдеться «про основні сфери національної безпеки», серед яких виокремлюється й інформаційна.

Об'єктами інформаційної безпеки України є:

1. людина і громадянин, оскільки державою гарантуються: додержання їх конституційних прав і свобод, фізичне та психологічне здоров'я, захищеність від негативного впливу інформаційних технологій та інформації;

2. суспільство і держава, з огляду на обов'язок держави захищати їх законних інтересів в інформаційній сфері;

3. інформаційні ресурси та інформаційна інфраструктура, а саме їх цілісність, доступність та захищеність. [3]

В рамках впровадження нових суб'єктів захисту інформаційної безпеки, в Україні було створено кіберполіцію.

Діяльність підрозділу буде направлена на протидію кіберзлочинності, яка являє собою вчинене за допомогою інформаційних технологій або пов'язане з втручанням у роботу комп'ютерів, програмного забезпечення, мереж, а також інші дії вчинені за допомогою пристроїв доступу до інформаційного простору, а також на кібербезпеку, тобто стан захищеності людини і суспільства, держави у кіберпросторі від протиправних посягань, захист персональних даних.

Головною метою створення цього підрозділу є виявлення та знешкодження злочинної діяльності в мережі Інтеренет, а також міжнародна співпраця по знешкодженню транснаціональних злочинних угрупувань у даній сфері. Крім того, на кіберполіцію буде покладена задача завчасного інформування населення про появу нових кіберзлочинів.

Цілями кіберполіції є:

1. Забезпечити он-лайн безпеку кожного громадянина України
2. Сформувати безпечний кіберпростір на теренах нашої держави
3. Моментальне опрацювання та оперативне реагування на інформацію про злочин та правопорушення
4. Належне представлення поліцейського органу на міжнародній Кіберарені (підвищення іміджу України та і поліції в цілому)

Основними завданнями та функціями згідно з Законом України "Про Національну поліцію" виділяють наступні:

1. Реалізація державної політики у сфері протидії кіберзлочинності
2. Протидія кіберзлочинам в сфері використання платіжних систем (несанкціоноване списання грошей з банківських рахунків за допомою систем дистанційного банківського обслуговування), електронної комерції та господарської діяльності (онлайн-шахрайство), сфері інтелектуальної власності (піратство) та інформаційної безпеки (створення і розповсюдження вірусів)
3. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності [4]

Основними завданнями у сфері інформаційної безпеки є:

- а) соціальна інженерія — технологія управління людьми в Інтернет просторі;
- б) мальвер (англ. malware) — створення та розповсюдження вірусів і шкідливого програмного забезпечення;
- в) протиправний контент — контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;
- г) рефайлінг — незаконна підміна телефонного трафіку.

Отже, як ми бачимо, формування такого підрозділу поліції є одним із дуже важливих кроків, адже своїм головним завданням кіберполіція ставить попередження, виявлення та знешкодження кіберзлочинності, яка за останні роки в Україні зростає з великою швидкістю.

Література:

1. Конституція України від 28 червня 1996 р. //Відомості Верховної Ради України.-1996.- №30. – ст.17
2. Закон України «Про інформацію» від 2 жовтня 1992 р. //Відомості Верховної Ради України, 1992, - N 48. – ст. 12
3. Закон України «Про основи національної безпеки України» від 19 березня 2003 р. // Відомості Верховної Ради України (ВВР), - № 39
4. Закон України «Про Національну поліцію» від 2 липня 2015 року // Відомості Верховної Ради (ВВР), 2015, № 40-41
5. Настюк В.Я. Інформаційне право [підруч.] /за ред. проф. Настюка В.Я. - Х.: Право, 2015.- С. 227-229.

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

Коваленко Л. П.,
д.ю.н., доцент, професор кафедри Адміністративного права та адміністративної діяльності Національного юридичного університету ім. Ярослава Мудрого.
Романенко Ю. І.,
Студент Національного юридичного університету ім. Ярослава Мудрого.

СПІВВІДНОШЕННЯ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНОЇ СФЕРИ ТА ІНФОРМАЦІЙНОГО ПРАВА

На сьогодні інформація є засобом комунікації людей і нерідко виступає об’єктом їх діяльності. «Інформація» є одним із ключових понять для багатьох галузей знань. Правознавство, філософія, політологія, соціологія, історія та інші науки приділяють велику увагу зазначеній категорії. Будь-які суспільні відносини предмет регулювання права тісно пов’язані з інформацією.

Поняття «інформація» можна розглядати у широкому (який відображає використання даного поняття у загальній системі суспільних відносин) і у вузькому (правовому, тобто такому, який відображає особливості інформації як елементу лише правовідносин) сенсі.

У повсякденному житті під інформацією розуміють різні повідомлення, відомості про навколишній світ, процеси, що в ньому відбуваються, про

події, ситуації. Вона багатоаспектна: існує у неживій природі, кібернетичних (управлінських) системах, у живих організмах (генетична інформація), циркулює в суспільстві (соціальна інформація) тощо. На жаль, нині не існує єдиного загальнонаукового визначення цього поняття. У теорії інформації, наприклад, вона трактується через знання про навколишній світ, усунення невизначеності, у філософії як відображення багатоманітності.

Щодо правового змісту поняття «інформація», то вона виступає як об'єкт багатофункціональний. Наприклад, її розглядають як засіб реалізації конституційних прав і свобод, як елемент управління суспільними, державними справами, прийняття управлінських рішень, як товар у процесах її створення, використання, поширення, як об'єкт права власності тощо.

Під інформацією у ст.1 Закону України «Про інформацію» розуміються документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Цивільний кодекс України дещо коригує дефініцію поняття «інформація»: документовані або публічно оголошені відомості про події та явища, що мали або мають місце в суспільстві, державі та навколишньому середовищі. У визначенні акцентується увага на динаміці подій та явищ, відомості про які є інформацією.

Аналіз змісту вказаних визначень, а також відповідних норм Закону України «Про інформацію» та Цивільного кодексу України дає підстави для виділення таких ознак поняття «інформація».

1. Інформація це відомості про події та явища, що відбуваються:

а) у суспільстві; б) у державі; в) у навколишньому природному середовищі.

2. Інформація це дані, які можуть зберігатися в будь-якій формі й вигляді. Однак для набуття певного правового статусу інформація має відповідати вимогам та ознакам, передбаченим правовими нормами, або ж відповідати букві та духу закону.

3. Інформація це відомості, які задокументовані або публічно оголошені.

4.Інформація є об’єктом цивільних прав і належить до категорії нематеріальних благ.

5. Джерелами інформації вважаються передбачені або встановлені законом носії інформації: документи, інші носії інформації, які являють собою матеріальні об’єкти, що зберігають інформацію, повідомлення засобів масової інформації, публічні виступи.

Сучасний стан розвитку суспільства характеризується тим, що підвищується роль інформаційної сфери. Слід зазначити, що сфера (від грец. sphaira – шар) – це область дій, межа поширення чого-небудь (наприклад, сфера впливу); суспільне оточення, середовище, умови . Так, згідно зі ст. 12 Закону України «Про інформацію» від 2 жовтня 1992 р., «інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави». Основними напрямками інформаційної діяльності можна назвати політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Головні види інформаційної діяльності – отримання, використання, поширення та зберігання інформації.

На сьогодні в національному законодавстві не легалізоване поняття «інформаційна сфера». (с. 21) Як уже наголошувалося в попередньому розділі, нині і на побутовому, і на науковому рівні інформаційна сфера розглядається, по-перше, як така, що формується та розвивається під час інформаційної діяльності, по-друге, як відносно самостійна сфера, і як допоміжна стосовно інших видів діяльності. В останньому випадку йдеться про те, що інформаційна сфера обслуговує майже всі боки суспільного життя (економіку, політику, управління, науку, культуру, побут, сім’ю), тобто займає підлегле положення є підпорядкованою.

Існуюча політика держави в інформаційній сфері (йдеться про вузьке тлумачення) спрямована як на безпосередньо її розвиток/еволюціону-

вання/прогрес, так і на підвищення ефективності розвитку державності, безпеки, оборони, пріоритетних галузей економіки, фінансової та грошової системи, соціальної сфери, галузей екології та використання природних ресурсів, науки, освіти і культури, міжнародного співробітництва, безумовно, за допомогою цієї сфери. Пріоритетом є підвищення ефективності/зростання дієвості державного управління як однієї з функцій держави. Це підтверджується і Концепцією Національної програми інформатизації, в якій інформаційна сфера, інформатизація розглядаються як важливий засіб розвитку України. Слід зауважити, що відповідна державна політика проводиться і щодо підтримки/стимулювання розвитку самої інформаційної сфери, тобто засобів масової інформації, сфери науково-технічної інформації, видавничої справи та реклами, сфери статистики, сфери бібліотечної та архівної справи, сфери інформатики та обчислювальної техніки тощо. У такому вигляді ця політика легалізована та легітимізована у законах України: «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації» , «Про інформацію» .

Зупинимося ще на одному моменті. На цей час у національному законодавстві не закріплена дефініція поняття «інформаційний простір України». У зв’язку з цим спробуємо навести власне визначення цього поняття, базуючись на дослідженнях деяких науковців. Інформаційний простір України – це соціальне середовище, у якому здійснюється виробництво, збирання, зберігання, поширення і використання інформації і на яке розповсюджується юрисдикція України.

На сьогодні, інформаційна сфера вважається системоутворюючим чинником життя суспільства та держави, вона активно впливає на політичну, економічну, воєнну та інші складові національної безпеки країни, а у багатьох країнах і «вбирає» їх.

Що стосується інформаційного права, то нині воно динамічно розвивається як наука, а його основні положення перебувають на стадії формування. Звичайно, на нього значно впливають такі галузеві науки, як:

конституційне, адміністративне, цивільне, трудове, кримінальне право. Окремі положення інформаційного права базуються на теоретичних засадах міжгалузевих інституцій законодавства та юридичної науки господарського, підприємницького і комерційного права, права інтелектуальної власності тощо.Категорія «інформаційне право» може розглядатися в кількох аспектах:

- як галузь суспільних відносин;
- як інституція в юридичній науці;
- як навчальна дисципліна.

Як галузь суспільних відносин інформаційне право може розглядатися у двох змістах: об'єктивному і суб'єктив-ному /сприйматися в об'єктивному і суб'єктивному сенсах.

Інформаційне право в об'єктивному значенні це вре-гульований нормативними актами комплекс суспільних відносин, об'єктом яких є інформація, а в суб'єктивному це комплекс прав і обов'язків суб'єктів суспільних відносин щодо інформації.

Як інституція в юридичній науці інформаційне право це відносно автономна інституція правової науки щодо дослідження проблем суспільних відносин, об'єктом яких є інформація.

Якщо підходити як до навчальної дисципліни, то інформаційне право це комплекс знань, що подаються для вивчення теорії і практики регулювання суспільних відносин, об'єктом яких є інформація.

Отже, об'єднуючою ланкою цих понять виступає інформація, яка формує інформаційну сферу і регулюється інформаційним правом.

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

Коваленко Л. П.,
д.ю.н., доцент, професор кафедри Адміністративного права та адміністративної діяльності Національногоюридичного ніверситету ім. Ярослава Мудрого.
Туров В. Д.,
Студент Національного юридичного університету ім. Ярослава Мудрого.

ЩОДО ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ

Конституція України (ст. 34) гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, на вільне збирання, зберігання, використання і поширення інформації [1] . Це важливе конституційне положення повністю відповідає ст.19 Загальної декларації прав людини та ст.10 Конвенції про захист прав і основних свобод людини.

Основними нормативними актами правового регулювання щодо ведення інформаційної діяльності, тобто одержання, використання, поширення та зберігання інформації і захисту прав суб'єктів інформаційних відносин містяться також у Цивільному кодексі України, Законах України «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про державну підтримку за-собів масової інформації та соціальний захист журналістів», «Про науково-технічну інформацію» та ін.

Інтернет є екстериторіальним інформаційним простором, що має глобальний, міжнародний характер. Інтернет – це єдина інформаційна мережа, в якій відбуваються глобальні процеси соціальних комунікацій та якому притаманний всесвітній загальний характер доступу.

Правовідносини, що виникають з приводу функціонування мережі Інтернет, характеризуються такими ознаками:

1. обмін інформації відбувається в електронній цифровій формі;
2. віддаленість суб’єктів цих відносин у просторі;

3. наявність суб’єктів, які не ініціювали ці відносини, проте мали організаційно-технічну можливість здійснити вплив на них;

4. використання програмного забезпечення, технічних стандартів і протоколів;

5. схильність цих відносин до саморегуляції;

6. технологічна складність мережі Інтернет;

7. поширені можливості порушення інформаційних прав суб’єктів цих відносин;

8. технічний, культурний та освітній ценз суб’єктів цих відносин [3].

Пріоритетними методами та способами правового регулювання суспільних відносин, що виникають з приводу використання всесвітньої комп’ютерної мережі Інтернет, є публічно-правовий та приватно-правовий методи (метод юридичної рівності сторін), позитивне зобов’язання та дозвіл, оскільки вони є засобами юридичного стимулювання поведінки учасників згаданих суспільних відносин [4;125].

Інтернет, не будучи керованою організаційною структурою і юридичною особою, не є суб’єктом правовідносин, у зв’язку з чим немає юридичних відносин між мережею Інтернет (або її національними сегментами) і державою. Структура інформаційних ресурсів в Інтернеті включає сторінки (сайти) існуючих традиційних засобів масової інформації (телебачення, радіо, газети і т. ін.), сторінки (сайти) засобів масової інформації, що не мають поза Інтернетом аналогів, сторінки (сайти), суб’єктів, які не є засобами масової інформації.

Із розвитком і поширенням Інтернету все більше країн світу усвідомлюють потребу в його правовому регулюванні. Передусім це зумовлено тим, що завдяки потужним темпам розвитку Інтернет сприяє революційним перетворенням в усіх сферах суспільного життя. Інтернет уже став потужним фактором соціального, освітнього і культурного розвитку, надаючи нові можливості як державним органам, так і звичайним громадянам і працівникам освіти, усуваючи бар’єри до створення і

поширення матеріалів, пропонуючи загальний доступ до джерел цифрової інформації, кількість яких постійно збільшується.

Однак Інтернет містить також і певну частину потенційно неналежної (непристойної, образливої) або протизаконної інформації і може іноді використовуватися як засіб злочинних дій. Хоча переваг Інтернету набагато більше, ніж його потенційних недоліків, ігнорувати ці проблеми не можна, бо вони вважаються гострими проблемами суспільного, політичного, комерційного і юридичного значення. Якщо не вирішити їх, то вони, можливо, набагато ускладнять користування Інтернетом, загальмувавши розвиток галузі, яка надає широкі й різноманітні можливості всім сферам суспільства. Саме тому проблема правового регулювання мережі набуває все більшого значення як на рівні міжнародного співтовариства, так і в окремих державах світу [5;192].

Так, наприклад у США набула поширення «Декларація про незалежність кіберпростору» Джона Барлоу, яка була написана як протест проти прийняття у 1996 р. Закону «Про пристойність у засобах зв'язку» (Акта про реформу телекомунікацій). Сама ймовірність втручання в мережу з боку влади розцінюється як обмеження свободи слова і відхід від демократії.

У червні 1997 р. Верховний Суд США відкинув положення Закону про пристойність у засобах зв'язку, за яким, зокрема, поширення матеріалів непристойного змісту, до яких може отримати доступ неповнолітня особа, кваліфікується як злочин, оскільки це було б порушенням захищеного конституцією права свободи слова; однак при цьому Верховний Суд підтримав положення закону щодо матеріалів непристойного змісту [5;194].

Основним питанням початкового етапу впровадження системи безпеки є призначення відповідальних осіб за безпеку і розмежування сфер їх впливу. Як правило, ще на етапі початкової постановки питань з'ясовується, що за цей аспект безпеки організації ніхто відповідати не хоче. Системні програмісти і адміністратори схильні зараховувати це завдання до компетенції загальної служби безпеки, тоді як остання вважає, що це питання

перебуває в компетенції спеціалістів по комп'ютерах.

До стратегічних рішень при створенні системи комп'ютерної безпеки повинна бути віднесена розробка загальних вимог до класифікації даних, що зберігаються і обробляються в системі.

На практиці найчастіше використовуються наступні категорії інформації.

Важлива інформація – незамінна та необхідна для діяльності інформація, процес відновлення якої після знищення неможливий або ж дуже трудомісткий і пов'язаний з великими затратами, а її помилкове застосування чи підробка призводить до великих втрат.

Корисна інформація – необхідна для діяльності інформація, яка може бути відновлена без великих втрат, причому її модифікація чи знищення призводить до відносно невеликих втрат.

Конфіденційна інформація – інформація, доступ до якої для частини персоналу або сторонніх осіб небажаний, оскільки може спричинити матеріальні та моральні втрати.

Відкрита інформація – це інформація, доступ до якої відкритий для всіх.

Керівництво повинно приймати рішення про те, хто і яким чином буде визначати степінь конфіденційності і важливості інформації. На жаль, у нашій країні ще не повністю сформоване законодавство, щоб розглядати інформацію як товар та регламентувати права інтелектуальної власності на ринку інтелектуального продукту, як це робиться в світовій практиці.

На окрему увагу заслуговує класифікація загроз безпеки. Під *загрозою безпеки* розуміють потенційні дії або події, які можуть прямо чи опосередковано принести втрати – привести до розладу, спотворення чи несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається або обробляється, а також програмні і апаратні засоби.

З огляду вище викладеного, можна дійти висновку, що здійснювати державний контроль у мережі Інтернет повинно бути прерогативою держави,

однак межі цього контролю слід чітко окреслити та не допускати будь-яких порушень прав людини та громадянина на право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, на вільне збирання, зберігання, використання і поширення інформації. На сьогоднішній день, потрібно докладати максимум зусиль для гарантування безпеки і користувачам, і власникам ресурсів. У цьому контексті додамо, що під безпекою електронної системи розуміють її здатність протидіяти спробам нанести збитки власникам та користувачам систем при появі різноманітних збуджуючих (навмисних і ненавмисних) впливів на неї.

Література:

1. Конституція України від 28 червня 1996 р. //Відомості Верховної Ради України.-1996.-№30.-ст.141.
2. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. – Київ: Софт Прес, 2005. – 316 с.
3. Еннан Р. Є. Правове регулювання відносин у мережі Інтернет/Еннан Р. Є. // ІТ ПРАВО: Проблеми і перспективи розвитку в Україні [електроний ресурс] - режим доступу: http://aphd.ua/publication-173/
4. Жилінкова І. Правове регулювання Інтернет – відносин / І. Жилінкова // Право України. – 2003 – № 5. – С. 124-128.
5. Настюк В.Я. Інформаційне право [підруч.] /за ред. проф. Настюка В.Я. - Х.: Право, 2015.- 281 с.

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