УДК 347.77:(007:004.056.5:004.738.5)

Некіт Катерина Георгіївна,
кандидат юридичних наук, доцент, доцент кафедри цивільного права
Національного університету «Одеська юридична академія»

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ВІДШКОДУВАННЯ ШКОДИ, ЗАПОДІЯНОЇ ПРИСТРОЯМИ, ПІДКЛЮЧЕНИМИ ДО ІНТЕРНЕТУ РЕЧЕЙ

Постановка 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 у 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).

Стан дослідження теми. Проблеми Інтернету речей на сьогодні є практично недослідженими, оскільки це явище є абсолютно новим. Серед сучасних дослідників, якими було приділено увагу дослідженню проблематики Інтернету речей, можна згадати О. Баранова, М. Ожеван, А. Білощицького, І. Доронина, Є. Харитонова, О. Харитонову, Н. Отрешко та інших. Втім, розвідки у цьому напрямку ще тільки починаються, а тому проблеми Інтернету речей потребують подальших поглиблених досліджень.

Метою цього дослідженняє аналіз поняття та елементів Інтернету речей, визначення кола проблем, що виникають із розвитком Інтернету речей, приділення окремої уваги проблемі відшкодування шкоди, заподіяної пристроями, що є елементами Інтернету речей.

Виклад основного матеріалу. 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:

- фізичні об'єкти, оснащені датчиками та механізмами для прийому та обробки сигналів;

- Інтернет-доступ: стандарти і протоколи зв'язку для підключення датчиків до єдиної мережі;

- Мережа (зв'язок): доступ в Інтернет: бездротовий/дротовий доступ, Wi-Fi, Bluetooth, ZigBee, VPN, мережі покоління 2G/3G/4G;

- 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;

- додатки і взаємодія з користувачами: взаємодія людей, додатків і бізнес-процесів [3].

За прогнозами дослідників ще одним елементом Інтернету речей можуть стати «вкладені освіти», тобто вбудовані у пристрої системи, які виконуватимуть навчальні функції. Наприклад, микрохвильовка, яка навчає готувати, посудомийка, яка навчає правильно закладати посуду, компілятори, які навчають програмуванню, медичний пристрій, який одночасно навчає як знімати показання та інтерпретувати їх [4]. Тобто вбудовані системи, які представляють собою спеціалізовані мікропроцесорні системи управління, контролю і моніторингу, які

працюють, будучи вбудованими безпосередньо у пристрої, якими вони управляють [5], також можна вважати елементом Інтернету речей.

Іноді Інтернет речей називають своєрідною екосистемою, побудованою не на біологічних, а на технологічних зв'язках [6].

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 [7]. 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 впровадження рішень IoT в сферах охорони здоров'я і транспорту, вдома 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 [3].

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 [8].

Але до вирішення питання про правосуб'єктність речей, що входять до IoT, необхідно вирішити проблему відповідальності за шкоду, заподіяну пристроями, що входять до системи IoT. Це питання є доволі складним, оскільки існує кілька компонентів, в результаті використання яких спричиняється шкода, і права на які належать різним суб'єктам. Але залишати це питання невирішеним і далі неможливо, оскільки кількість випадків

вчинення кіберзлочинів із використанням Інтернету речей невпинно зростає.

Об'єкти, що входять до Інтернету речей, є набагато менш захищеними, ніж комп'ютери, а тому часто використовуються хакерами для зловмисних дій. Так, у червні 2016 р. був виявлений так званий ботнет (зомбі-мережа), який складався з більш, ніж 25 тисяч міських та приватних камер та використовувався хакерами для здійснення DDoS-атак [9]. Така прикра ситуація стає можливою завдяки тому, що більш ніж 70% пристроїв, які входять до Інтернету речей, мають вразливості, у 60% з них небезпечний web-інтерфейс. При цьому більшість з них має доступ до персональних даних своїх володільців, таких, як адреса, e-mail і навіть банківський рахунок. Часто це пов'язано з тим, що виробники, намагаючись зменшити свої витрати, радикально економлять на забезпеченні безпеки. Наприклад, постачальними дешевих камер практично ігнорують включення до своїх продуктів засобів захисту, оскільки, за їх оцінками, для більшості користувачів камер низька вартість набагато важливіше [9].

Іншим прикладом недобросовісного підходу виробників до захисту пристроїв, що стають елементами Інтернету речей, може стати ситуація зі зломом холодильнику Sumsung, в якого спеціалістам з безпеки вдалося отримати дані від акаунта Gmail. Це стало можливим тому, що компанія-виробник не потурбувалася про правильну перевірку сертифікату SSL при встановленні захищеного з'єднання із сервером Google. Попри те, що в холодильнику була реалізована підтримка SSL, перевірка сертифікату де-факто не здійснювалася, що робило можливим проведення атаки MiTM. З урахуванням того, що пристрій підключався до Мережі через Wi-Fi, таку атаку можна було провести із-за меж квартири, від сусідів чи з вулиці [10].

Сьогодні вже існують випадки звернення з позовами до суду з причини незабезпечення належної безпеки пристроїв, що входять до системи Інтернету речей. Так, 9 січня 2017 р. Федеральна торгівельна комісія США подала позов проти тайванської компанії D-Link за те, що виробник не забезпечив безпеки своїх продуктів, залишивши їх вразливим до хакерських атак. Відповідно до позовної заяви, D-Link не реалізувала необхідні механізми захисту у маршрутизаторах і відеокамерах, що підключаються до Інтернету, і цим поставила під загрозу безпеку тисяч споживачів. Причиною звернення до суду стало використання кіберзлочинцями незахищених пристроїв Інтернету речей для створення ботнетів, які використовувалися для потужних DDoS-атак. До таких, зокрема, відноситься ботмережа Mirai, яка складається з маршрутизаторів, веб-камер і відео реєстраторів з ненадійними заводськими паролями, за допомогою якої були здійснені найпотужніші за всю історію DDoS-атаки. При цьому D-Link за допомогою реклами ввела користувачів у оману щодо безпеки своїх продуктів, стверджуючи, що були прийняті всі міри безпеки проти відомих загроз, у тому числі незмінюваних паролів. Тож внаслідок того, що виробник не потурбувався про безпеку свого програмного забезпечення, його продукція дозволяла хакерам стежити за місцезнаходженням користувачів з метою здійснення крадіжок чи інших злочинів [11].

Для запобігання таким ситуаціям дослідники проблем кібербезпеки підкреслюють необхідність взяття професійним співтовариством відповідальність з цього питання, у тому числі здійснювати тиск на споживачів. Інструментами такого тиску називають державні регулятивні органи та товариства із захисту прав споживачів. Так, відповідаючи на такого роду ініціативи, Федеральна торгівельна комісія США провела більше п'ятидесяти справ щодо компаній, які не забезпечують достатнього рівня захищеності мереж, продуктів та сервісів, що використовуються ними, та провела серію семінарів Start With Security, присвячених необхідності включати розробку методів забезпечення приватності і безпечного використання на ранні етапи розробки продуктів [9].

Крім регулятивних дій у цій сфері обговорюється і можливість саморегуляції, яка сприяла б розвитку IoT, не стримуючи інноваційних технологій. Така альтернатива можлива шляхом введення системи сертифікації, як у Національного управління безпеки на транспорті в США [9].Про необхідність сертифікації IoT-гаджетів зазначають спеціалісти у сфері IoT, зокрема, про це було заявлено спеціалістом з розробки програмного забезпечення, головою SF Internet Society IoT Working Group М. Шпігельмоком. Ним було зазначено, що, якщо уявити собі усі IoT-пристрої як рух по одній дорозі, то сьогодні, складається ситуація, при якій кожен із виробників вважає, що він є єдиним, хто рухається по цій дорозі, тоді як насправді дорога єдина, а машин багато, і всі вони рухаються по цій дорозі, поділяючи ресурси – зовнішню IP-адресу, Wi-Fi, радіочастоти, і раніше чи пізніше ці машини почнуть стикатися, конфліктувати між собою. Тому необхідно узгодити їхнє співіснування шляхом введення відкритої сертифікації IoT-продуктів. Сертифікація допоможе дати гарантію, що той чи інший пристрій не є очевидно доступним для першого хакера [12; 13].

Ключові концепції безпеки у сфері IoT були обговорені в рамках заходу Rights Con, це, зокрема: безпека даних, поділ оновлень безпеки та функціо-

нальності, оновлень безпеки для розумного строку служби даного продукту і більш широку цифрову безпеку – з використанням шифрування і інформаційної безпеки для забезпечення конфіденційності і цілісності пристроїв, служб і даних, які вони створюють. Було підкреслено, що незважаючи на те, що влада може здійснювати деякі засоби захисту прав людини, компанії також повинні активізувати та вводити засоби захисту на рівні програмного та/або апаратного забезпечення і, звісно ж, самі користувачі повинні мати можливість будувати власний захист. Це потребує стійкого співробітництва між громадянським суспільством, групами із захисту прав споживачів та технологічними компаніями [14].

Висновки. Отже, серед заходів забезпечення інформаційної безпеки у сфері IoT та профілактики заподіяння шкоди Інтернетом речей, у першу чергу необхідно виділити саморегуляцію, яка повинна забезпечуватися за допомогою тісної співпраці технологічних компаній та громадянського суспільства. Це мінімізує втручання держави в цю сферу, що сприятиме швидкому розвитку інноваційних технологій. Виникає лише потреба у правовому регулюванні відносин між громадянським суспільством, організаціями із захисту прав споживачів та технологічними компаніями. Перш за все, зусилля мають бути спрямовані на охорону прав людини від порушень, пов'язаних з функціонуванням Інтернету речей, що передбачає необхідність профілактики таких порушень шляхом контролю за встановленням належного захисного програмного забезпечення на всі пристрої, що входять до екосистеми IoT.

Проблема захисту прав людини та відшкодування шкоди, спричиненою Інтернетом речей, виникає вже у випадку, коли відбувся факт правопорушення. Тут слід врахувати, що умови відшкодування шкоди, заподіяної пристроєм, що входить до Інтернету речей, включатимуть: 1) наявність шкоди; 2) протиправність поведінки заподіювача шкоди (яким виступатиме виробник пристрою), що виражається в неприйнятті заходів забезпечення безпеки пристрою; 3) причинний зв'язок між поведінкою заподіювача та шкодою; 4) вина заподіювача шкоди. Слід також зазначити, що при визначенні розміру шкоди, заподіяної пристроєм, включеним до системи Інтернету речей, необхідно враховувати вину споживача за незастосування засобів забезпечення особистої безпеки, якщо виробник попередив про необхідність застосування таких заходів. Крім того, представляється за доцільне покласти на споживачів обов'язок застосовувати всі можливі заходи безпеки, оскільки тут вступає в силу правило про необхідність врахування суспільного інтересу під час використання власності. Так, оскільки власність (пристрої, включені до системи Інтернету речей) в даному випадку може використовуватися зловмисниками з метою вчинення злочинів, тобто несе в собі загрозу інтересам держави та суспільства, представляється за можливе обмежити право власності покладанням на власників обов'язку вчинити всі можливі дії, спрямовані на забезпечення захисту пристрою від стороннього втручання (хакерських атак).

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. – 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 вещей: правовые аспекты (Российская Федерация)». – 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. – Режим доступу: http://www.ey.com/Publication/vwLUAssets/EY-mne-internet-of-things-rus/$File/EY-mne-internet-of-things-rus.pdf
4. Куда движется рынок образования и EdTech? Прогноз на 10–15 лет. Часть 4. – Режим доступу: http://alexeykrol.com/blog/2017/04/16/educationmarket_4/
5. Встраиваемая система. – Режим доступу: https://ru.wikipedia.org/wiki/%D0%92%D1%81%D1%82%D1%80%D0%B0%D0%B8%D0%B2%D0%B0%D0%B5%D0%BC%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0
6. Staying Ahead of Privacy and Security Risks in Internet of Things. – Режимдоступу: https://www.natlawreview.com/article/staying-ahead-privacy-and-security-risks-internet-things
7. Храмцов П. Всеобъемлющий интернет: прогнозы и реальность / П. Храмцов // Открытые системы. – 2013. – № 4. – Режим доступу: http://www.osp.ru/os/2013/04/13035552/

8. Исаков В.Б., Сарьян В.А., Фокина А.А. Правовые аспекты внедрения Интернета вещей // ИТ-Стандарт. – 2015. – № 4-1 (5). – С. 9-16. – Режим доступу: https://elibrary.ru/item.asp?id=25208816
9. Упитт О. Опасные предметы: кто и зачем взламывает Интернет вещей и как с этим быть. – Режим доступу: https://apparat.cc/world/internet-of-things/
10. Ализар А. Умный холодильник выдал хакерам пароль от Gmail. – Режим доступу: https://xakep.ru/2015/08/25/smart-fridge/
11. Федеральная торговая комиссия США подала в суд на D-Link. – Режим доступу:http://www.securitylab.ru/news/484958.php
12. Виндерских Н. Опасность интернета верей: зачем IoT рынку сертификация. – Режим доступу: https://ain.ua/2017/09/01/opasnost-interneta-veshhej
13. SpiegelmockM.IoT Security Through Open Certification. – Режимдоступу: http://www.sfbayisoc.org/2017/06/21/iot-security-through-open-certification/
14. Как защитить права человека в пространстве Интернета вещей. – Режим доступу: https://rublacklist.net/28562/

Некіт Катерина Георгіївна

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ВІДШКОДУВАННЯ ШКОДИ, ЗАПОДІЯНОЇ ПРИСТРОЯМИ, ПІДКЛЮЧЕНИМИ ДО ІНТЕРНЕТУ РЕЧЕЙ

Стаття присвячена дослідженнюпоняття та елементів Інтернету речей, визначенню кола проблем, що виникають із розвитком Інтернету речей. Зазначено, що серед таких проблем першочерговими є проблема захисту персональних даних та відшкодування шкоди, заподіяної пристроями, підключеними до Інтернету речей. Окрема увага приділена саме проблемі відшкодування шкоди, заподіяної пристроями, що є елементами Інтернету речей. Визначено засоби запобігання та умови відшкодування такої шкоди.

Ключові слова: Інтернет речей, шкода, речі, пристрої, персональні дані, відшкодування, інформаційна безпека, саморегулювання, обмеження права власності.

Некит Екатерина Георгиевна

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ВОЗМЕЩЕНИЯ ВРЕДА, ПРИЧИНЕННОГО УСТРОЙСТВАМИ, ПОДКЛЮЧЕННЫМИ К ИНТЕРНЕТУ ВЕЩЕЙ

Статья посвящена исследованию понятия и элементов Интернета вещей, определению круга проблем, которые возникают с развитием Интернета вещей. Отмечено, что среди таких проблем первоочередной является проблема защиты персональных данных и возмещения вреда, причиненного устройствами, подключенными к Интернету вещей. Отдельное внимание уделено именно проблеме возмещения вреда, причиненного устройствами, которые являются элементами Интернета вещей. Определены средства предотвращения и условия возмещения такого вреда.

Ключевые слова: Интернет вещей, вред, вещи, устройства, персональные данные, возмещение, информационная безопасность, саморегулирование, ограничение права собственности.

Nekit Kateryna

PROBLEMS OF ENSURING INFORMATION SECURITY AND THE COMPENSATION OF DAMAGES CAUSED BY THE DEVICES CONNECTED TO THE INTERNET OF THINGS

The article is devoted to a research of a concept and elements of the Internet of things, identifying the issues which arise with development of the Internet of things. It is noted that among such problems the problem of protection of personal data and the compensation of damages caused by the devices connected to the Internet of things is prime. Special attention is paid to a problem of the compensation of damages caused by devices which are elements of the Internet of things. Means of prevention and a conditions of compensation of such damage are defined.

Keywords: Internet of things, damage, things, devices, personal data, compensation, information security, self-regulation, limitation of ownership right.