DOI: 10.18372/2307-9061.57.15074
УДК 34.096:004.056.5(045)

В. В. Філінович,
кандидат юридичних наук
ORCID ID: https://orcid.org/0000-0001-8824-615X

КІБЕРБЕЗПЕКА ТА ІНТЕРНЕТ РЕЧЕЙ: ПРАВОВИЙ АСПЕКТ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: vvfilinovich@gmail.com

Мета: *дослідити особливості та сутність Інтернету речей та правові можливості захисту такої системи.* ***Методи дослідження:*** *дослідження було проведено із застосуванням загальновизнаних методів наукового пізнання, таких як: аналітичний, порівняльно-правовий, системно-структурний та інші.* ***Результати:*** *досліджено поняття, суть, характеристики Інтернету речей та пов'язаних із ним аспектів кібербезпеки, вказано на проблеми захисту користувачів та надано пропозиції щодо подолання таких проблем.* ***Обговорення****: дискусія у статті ведеться щодо пошуку шляхів вирішення проблеми забезпечення достатнього рівня кібербезпеки у системі Інтернету речей та необхідності гармонізації вітчизняного законодавства щодо захисту персональних даних із міжнародними стандартами.*

Ключові слова: *кібербезпека; інформаційна безпека; Інтернет речей; управління Інтернетом; кіберпростір; кіберзлочини; кібератака.*

Постановка проблеми та її актуальність. Сьогодні багато пристроїв (також відомі як гаджети) можуть підключатися до Всесвітньої Мережі Інтернет, отримуючи і відправляючи певну інформацію. Така здатність робить пристрій «розумним» (тобто «смарт» - від англ. *Smart*), відповідно, він стає більш ефективним. Як приклади подібного варто згадати розумні годинники, систему «розумний будинок», «розумне авто» тощо. При цьому сама така річ (пристрій) не повинна бути зверх-високотехнологічною, досить того, щоб вона могла підключатися до серверів такого «надкомп'ютера».

Але із безсумнівними благами Інтернет речей приніс нам і велику кількість негативних моментів, пов'язаних із «ударами» по кібербезпеці: підвищився рівень збільшення векторів атак. Так, кожен із нас може стати жертвою кіберзлочинців, всього лише використовуючи звичні речі.

Аналіз останніх досліджень і публікацій. Цій проблемі були присвячені роботи таких дослідників і вчених як Г. Фрідер, Д. Пушман, П. Притула, П. Барнагі, Ф. Каррез, С. Власко та інших.

Мета статті. В даному науковому дослідженні автор хоче розкрити суть і особливості Інтернету речей і надати критичну оцінку пов'язаних із ним прогалин у кібербезпеці, а також надати шляхи вирішення такої проблеми.

Виклад основного матеріалу. Інтернет речей (також IoT, абр. від англ. *Internet of Things*) став буденністю, частиною нашого повсякденного життя. І використання його елементів нерідко призводить до зростання ризиків, пов'язаних із кібербезпекою. Так, згідно з В. Дащенко, рівень збільшення векторів атак за допомогою Інтернету речей став істотно вищим, ніж був раніше [14].

Галузь Інтернету речей розвивається семимильними кроками. Так, якщо в 2009 році кількість підключених до Мережі гаджетів перевищила чисельність населення нашої планети, то в 2020 році речі системи IoT за вказаним параметром вже перевершили за кількістю реальних

користувачів у декілька разів [13]. І такий стрімкий розвиток принесло нам крім користі ще й проблеми інформаційної безпеки. Їх можна і потрібно всіляко намагатися подолати, про способи чого і буде розказано далі.

Але, перш ніж перейти до зазначеного питання, варто пролити світло на основні використовувані нами в цій статті терміни. Так, Європейське агентство із мережевої та інформаційної безпеки (ENISA) під Інтернетом речей розуміє кіберфізичну екосистему взаємопов'язаних датчиків та виконавчих механізмів, які дають можливість приймати інтелектуальні рішення [2]. На підставі зазначеного можна зробити висновок про те, що інформація лежить в основі IoT, підтримуючи безперервний цикл прийняття рішень і вчинення дій.

IoT у розумінні вчених Г. Фрідеріха, Д. Пушманна, П. Барнагі та Ф. Каррези – це система взаємодії та обміну інформацією між мільярдами пристроїв, які виробляють і обмінюються даними та відносяться до об'єктів реального світу (тобто речей) [1, с. 340].

Інтернет-фахівець М. Глущенко під розглянутою категорією розуміє відразу кілька феноменів:

– це безпосередньо самі гаджети, підключені до Інтернету (він же Мережа) і взаємодіючі між собою;

– це спосіб підключення, відомий як «M2M» (англ. *Machine-to-Machine*), тобто «машина до машини», при цьому участь людини у зазначеному процесі не потрібна;

– це дані, які генеруються пристроями та підлягають збору, аналізу і подальшому використанню з метою підвищення комфорту користувача або прийняття ним певних бізнес-рішень [6].

Таким чином, можна зробити висновок про те, що ***Інтернет речей*** *– це технологічна концепція підключення пристроїв по всьому світу до Мережі Інтернет з метою управління ними віддалено.* Здійснюватися це може як через сервер, так і безпосередньо шляхом використання спеціального програмного забезпечення (далі – ПЗ) і обміну даними в режимі real time, тобто реального часу.

Сьогодні IoT-пристрої використовуються у багатьох секторах економіки та соціального життя, наприклад, у:

– логістиці – ми можемо відстежити рух транспорту або навіть поштового відправлення;

– медицині та оздоровчому секторі – багато хто носить фітнес-браслет для відстеження щоденної активності, а персональні пристрої моніторингу стану здоров'я допомагають вчасно передбачити недуги;

– аграрному секторі – аграрії стежать за станом грунтів, зростанням тварин, об'ємом врожаю тощо;

– адміністративній та соціальній сферах – збір штрафів ведеться автоматично, зі свого смартфона ви завжди можете ознайомитися із заторами і ДТП на дорогах;

– міській інфраструктурі – освітлення, камери спостереження, банкомати, навіть світлофори - все це управляється системою IoT.

І це лише мала дещиця прикладів взаємодії в системі Інтернету речей. На думку П. Притули масовому впровадженню Інтернету речей сьогодні перешкоджають певні проблеми, серед яких:

– «дірки» у безпеці. Тільки уявіть на хвилину, як ваш «розумний» автомобіль перестає вас слухатися, а робить те, що вказують йому хакери, тобто кіберзлочинці, які зламали систему управління механізмом. Якщо ж поглянути на проблему більш глобально, то сьогодні кібербезпека виробничих об'єктів знаходиться на досить низькому рівні, щоб суб'єкти відчували себе спокійно, адже, наприклад, кібератака на АЕС або інший подібний об'єкт інфраструктури може мати незворотні наслідки. Проблема сьогодні є загальновизнаною, в звіті Всесвітнього економічного форуму сказано, що розробка вирішення проблеми безпеки являє собою життєво-важливий щабель у розвитку IoT;

– застарілі формати даних. Зараз все ще функціонують системи, впроваджені ще близько 3-4 десятиліть назад, при цьому кількість сенсорів і ПЗ величезна. На просторах країн СНД відповідні суб'єкти не поспішають заміняти застарілі датчики і подібне обладнання, адже це вимагає серйозних інвестицій. Тому теперішнім фахівцям, що працюють у сфері IoT, доводиться за-

довольнятися тим, що є, а після - переробляти весь цей обсяг інформації у зрозумілі і прийнятні сьогодні формати. Наприклад, для побудови сучасної системи однієї нафто-газокомпанії були задіяні навіть дані з рукописних журналів;

– брак фахівців. Для роботи в IoT потрібні відповідні професіонали, особливо аналітики даних, технічні співробітники, які здійснюють підготовку цих даних для подальшого аналізу, а також галузеві фахівці, націлені на отримання прибутку і створення сучасних бізнес-моделей. І таких дуже мало;

– інструментарій, далекий від ідеального. Сучасні інструменти, без яких IoT неможливий повинні бути інтуїтивно зрозумілими, а сама технологія – максимально демократизованою;

– нестійкість зв'язку. Багато пристроїв, особливо, смарт-автомобілі, не можуть у повній мірі функціонувати через нестійкість зв'язку та недостатнє покриття. Сюди ж П. Притула відносить і проблему зайвої дорожнечі оплати зв'язку в роумінгу;

– небажання громадян взаємодіяти зі смарт-системами. Так, багато городян побоюються, що інноваційний інструментарій IoT хоч і вирішує проблеми міста, але одночасно веде збір даних про їхнє особисте життя. І переконати людей у безпеці систем дуже складно. При цьому більшість із них цілком охоче діляться своєю інформацією із інтернет-гігантами на кшталт Google і Apple, але не зі своєю державою [10].

Від себе додамо також людську боязнь перед нововведеннями. Як не дивно, більшість із нас боїться нових технологій, вважаючи за краще використовувати застарілі, але такі зрозумілі й звичні, при цьому не бажаючи розбиратися із інноваційними розробками.

Але найслабшим місцем IoT, на думку автора статті, є кібербезпека. Взагалі, згідно з І. Суриковою, пов'язані з інтелектуальними «речами» ризики можна розділити на дві групи:

– збої ПЗ, коли користувачів відключають від обслуговування у зв'язку із пошкодженням гаджета;

– вплив кібератак і вірусів на речі із системи IoT [12].

Особливий ризик для кібербезпеки становлять пристрої з обмеженими функціями захисту, безпосередньо пов'язаними з Інтернет-технологіями. Так, на перших порах допоможе технічний інструментарій типу VPN-сервера компанії (мова про приватну віртуальну мережу (від англ. *Virtual private network*), тобто зашифрований тунель між двома об'єктами, що дозволяє отримати доступ до веб-сервісів безпечно і конфіденційно [4]). Але часто у багатьох компаній цифрова безпека не є пріоритетом, відповідно, використовувані технології захисту є застарілими, а штат ІТ-фахівців має не найвищий рівень професійних навичок.

Якщо кіберзлочинець (хакер) отримає доступ навіть до одного вашого пристрою, то зможе інфікувати його шкідливим ПЗ, через яке підключиться і до інших «речей». Незабаром після такого зловмисник легко добереться до ваших персональних даних, наприклад, платіжних, тим самим відкривши собі шлях для розкрадань коштів із вашої банківської картки.

В Україні на законодавчому рівні проблема викрадання персональних даних (далі – ПД) врегульована деякими нормативно-правовими актами. Так, відповідно до Закону України «Про захист персональних даних» (ст. 12) збір ПД – це один із елементів процесу їх обробки, що передбачає активність за добором або упорядкуванням інформації про фізичну особу (тобто власника ПД, суб'єкта ПД). Такий суб'єкт повинен бути повідомлений про склад і зміст зібраної інформації, свої права у зв'язку із цим, про цілі збору та інших суб'єктів, які отримають його ПД [11, ст. 12]. Цей НПА було прийнято у 2010, а роком пізніше президент наділив Державну службу України із питань захисту ПД повноваженнями щодо їх захисту. Але вже в 2013 році відповідальним органом у цій сфері став український Омбудсмен, адже, на думку європейських фахівців, попередній орган не був дефакто наділений достатньою незалежністю. В Європі ж уповноважений із прав людини часто виконує функції державного регулятора щодо захисту ПД [5].

Крім зазначеного, питання захисту і поводження із чужими ПД піднято у статті 32 Конституції України, згідно з якою збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не допускають-

ся. Але таке все ж можливо у виняткових випадках, і тільки в інтересах національної безпеки, економічного добробуту та прав людини [8, ст. 32]. Також деякі норми щодо особистої інформаційної безпеки містяться у Цивільному кодексі України, ЗУ «Про інформацію» та інших НПА.

Що стосується відповідальності за порушення у даній сфері, то, згідно зі ст. 188-39 КУпАП, на зловмисника, за порушення правових норм щодо захисту ПД, чекає адміністративна відповідальність. До подібних порушень Кодекс відносить:

– ухилення від держреєстрації бази ПД і недотримання встановленого законодавцями порядку захисту ПД, що вилилося у надання незаконного доступу до них;

– несвоєчасне повідомлення або неповідомлення суб'єкта ПД про його права при включенні персональних відомостей про нього в базу ПД;

– непокору вимогам омбудсмена щодо запобігання та усунення таких порушень тощо [7, ст. 188-39].

Також можна говорити і про кримінальну відповідальність для зловмисника, який своїми діями порушує недоторканність особистого життя людини, а саме робить нелегітимний збір, зберігання, застосування тощо конфіденційних відомостей про індивідуума або незаконну модифікацію таких відомостей [9, ст. 182].

Висновки. Отже, сьогодні технології майбутнього дійсно сприяють розвитку та автоматизації нашого сьогодення. Але усілякі гаджети, які отримали доступ в Інтернет, також принесли нам і проблеми інформаційної безпеки на кшталт незаконного заволодіння персональними даними користувача, недотримання прав людини у Мережі, незахищеності інформаційних систем перед іншим кіберзагрозами.

Наша держава все ще не виробила достатню законодавчу базу і методики, які зможуть ефективно захистити користувачів системи IoT. Тому Україна, у питанні захисту ПД, в основному спирається на міжнародний досвід, зокрема країн ЄС.

На нашу думку, найбільш актуальними і якісними для захисту ПД і кібербезпеки у зв'язку із зазначеним можна вважати Правила нового Закону про захист персональних даних в Інтернеті, відомі як GDPR (від англ. The General Data Protection Regulation), що вступили в силу 25.05.2018 р. Під їх дію повинні підпадати всі учасники Мережі, які пов'язані зі збиранням, зберіганням і обробкою ПД [3].

Разом із зазначеним правовим напрямком у забезпеченні захисту користувачів IoT, також варто застосовувати методи технічного і соціального впливу, а саме:

– забезпечити дотримання і захист прав людини у Мережі, недопущення дискримінаційних дій проти користувачів;

– впровадити інструментарій, що забезпечує конфіденційність спілкування в Інтернеті і можливість проведення користувачами самостійного контролю використання своїх ПД;

– забезпечити правову визначеність, транспарентність і легкість у сприйнятті нормативно-правових актів для кожного жителя нашої країни;

– провести реформування чинної української системи захисту ПД із метою поліпшення її ефективності;

– удосконалити і забезпечити виконання законодавства щодо захисту прав споживачів у частині, що стосується використання пристроїв у системі IoT.

Забезпечення високого рівня кібербезпеки має стати основним критерієм при проектуванні нових пристроїв, рішень і технологій. Влада повинна скооперуватися із міжнародними партнерами у боротьбі за забезпечення ефективного правового захисту користувачів Мережі Інтернет. Також важливою є просвітницька робота серед українських громадян із питань самостійного забезпечення захисту своїх прав у цифровому середовищі. І тільки так ми зможемо захистити систему Інтернету речей і себе у ній.

Література

1. A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things / G. Frieder, D. Puschmann, P. Barnaghi, F. Carrez. *IEEE Internet of Things Journal*. 2015. № 2. С. 340–354. https://doi.org/ 10.1109/ JIOT.2015.2411227

2. Internet of Things (IoT). European Union Agency for Cybersecurity. 2018. URL: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da). European Parliament and of the Council. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

4. VPN для чайников: руководство для начинающих. *ExpressVPN*. 2020. URL: https://www.expressvpn.com/ru/what-is-vpn/vpn-for-dummies.

5. Власко С. Защита персональных данных: чей опыт может пригодиться Украине. *Европейская правда*. 2018. URL: https://www.eurointegration.com.ua/ rus/experts/ 2018/01/16/ 7076152/.

6. Глущенко Н. Что такое интернет вещей? Даже ваша бабушка это поймет. *AIN*. 2018. URL: https://ain.ua/special/what-is-iot/.

7. Кодекс України про адміністративні правопорушення (статті 1 – 212-24): Закон від 07 груд. 1984 р. № 8073-X. *Відомості Верховної Ради Української РСР*. 1984. Додаток до № 51. Ст. 1122.

8. Конституція України від 28 чер. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

9. Кримінальний кодекс України від 05 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131.

10. Притула П. 5 проблем интернета вещей, которые предстоит решить. *CNews*. 2016. URL: https://www.cnews.ru/articles/2016-05-27_5_ problem_ interneta_veshchej_kotorye_ predstoit_ reshit.

11. Про захист персональних даних: Закон України від 01 чер. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

12. Сурикова И. Кибербезопасность и риски интернета вещей. Насколько умен ваш холодильник? *Le VPN*. 2019. URL: https://le-vpn.com/ ru/iot-risks/.

13. Технология «Интернет вещей»: автоматизация настоящего благодаря разработкам будущего. *IT рейтинг UA*. 2020. URL: https://it-rating.in.ua/ tehnologiya-internet-veschey-avtomatizatsiya-nastoyaschego-blagodarya-razrabotkam-buduschego.

14. Что следует знать о кибербезопасности и Интернете вещей подробнее. *SecurityLab*. 2017. URL: https://www.securitylab.ru/news/488259.php.

References

1. A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things / G. Frieder, D. Puschmann, P. Barnaghi, F. Carrez. *IEEE Internet of Things Journal*. 2015. № 2. C. 340–354.

2. Internet of Things (IoT). European Union Agency for Cybersecurity. 2018. URL: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da). European Parliament and of the Council. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

4. VPN dlja chajnikov: rukovodstvo dlja nachinajushhih. *ExpressVPN*. 2020. URL: https://www.expressvpn.com/ru/what-is-vpn/vpn-for-dummies.

5. Vlasko S. Zashhita personal'nyh dannyh: chej opyt mozhet prigodit'sja Ukraine. *Evropejskaja pravda*. 2018. URL: https://www.eurointegration.com.ua/ rus/experts/2018/01/16/7076152/.

6. Glushhenko N. Chto takoe internet veshhej? Dazhe vasha babushka jeto pojmet. *AIN*. 2018. URL: https://ain.ua/special/what-is-iot/.

7. Kodeks Ukrai'ny pro administratyvni pravoporushennja (statti 1 – 212-24): Zakon vid 07 grud. 1984 r. № 8073-X. *Vidomosti Verhovnoi' Rady Ukrai'ns'koi' RSR*. 1984. Dodatok do № 51. St. 1122.

8. Konstytucija Ukrai'ny vid 28 cher. 1996 r. № 254k/96-VR. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 1996. № 30. St. 141.

9. Kryminal'nyj kodeks Ukrai'ny vid 05 kvit. 2001 r. № 2341-III. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2001. № 25-26. St. 131.

10. Pritula P. 5 problem interneta veshhej, kotorye predstoit reshit'. *CNews*. 2016. URL: https://www.cnews.ru/articles/2016-05-27_5_ problem_interneta_ veshchej_kotorye_predstoit_reshit.

11. Pro zahyst personal'nyh danyh: Zakon Ukrai'ny vid 01 cher. 2010 r. № 2297-VI. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2010. № 34. St. 481.

12. Surikova I. Kiberbezopasnost' i riski interneta veshhej. Naskol'ko umen vash holodil'nik? *Le VPN*. 2019. URL: https://le-vpn.com/ru/iot-risks/.

13. Tehnologija «Internet veshhej»: avtomatizacija nastojashhego blagodarja razrabotkam budushhego. *IT rejting UA*. 2020. URL: https://it-rating.in.ua/ tehnologiya-internet-veschey-avtomatizatsiya-nastoyaschego-blagodarya-razrabotkam-buduschego.

14. Chto sleduet znat' o kiberbezopasnosti i Internete veshhej podrobnee. *SecurityLab*. 2017. URL: https://www.securitylab.ru/news/488259.php.

V. Filinovych

CYBERSECURITY AND THE INTERNET OF THINGS: A LEGAL ASPECT

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: vvfilinovich@gmail.com

Purpose: *the main goal of this paper is to study the features and essence of the Internet of Things and the legal possibilities of protecting such a system.* ***Research methods:*** *the research was carried out using generally recognized methods of scientific knowledge, such as analytical, comparative-legal, systemic and structural, and others.* ***The results:*** *the author has investigated the concept, essence, characteristics of the Internet of Things, and aspects of cybersecurity related to it, pointed out the problems of protecting users, and provided suggestions for overcoming such problems.* ***Discussion:*** *the discussion in the article is aimed at finding directions to solve the problem of ensuring a sufficient level of cybersecurity in the Internet of Things system and the need to harmonize domestic legislation on the protection of personal data with international standards. The Internet of Things today has become commonplace, a part of our daily life. And the use of its elements often leads to an increase in the risks associated with cybersecurity. The works of such researchers and scientists as G. Frieder, D. Pushman, P. Pritula, P. Barnaghi, F. Carrez, S. Vlasko, and others were devoted to this problem. In this research study, the author wants to uncover the essence and features of the Internet of Things and provide a critical assessment of the related cybersecurity gaps, as well as provide ways to solve this problem.*

Today, many devices also known as gadgets can connect to the World Wide Web, receiving and sending certain information. This ability makes the device «smart», respectively, it becomes more efficient. As examples of this, it is worth remembering smartwatches, smart home systems, smart cars, and others. Moreover, such a thing (device) itself should not be super-high-tech, it is enough that it can connect to the servers of such a «supercomputer».

But with undoubted benefits, the Internet of Things has brought us a large number of negative aspects associated with «attacks» on cybersecurity: the level of increase in attack vectors has expanded. So, each of us can become a victim of cybercriminals by using familiar things.

Keywords: *cybersecurity; Information Security; Internet of Things; Internet governance; cyberspace; cybercrime; cyberattack.*