

УДК 343.97

Олена Бугера,

канд. юрид. наук, доцент,

доцент кафедри права

Київського національного лінгвістичного університету

ІНТЕРНЕТ РЕЧЕЙ ТА ЗАПОБІГАННЯ ЗЛОЧИННОСТІ

Стаття присвячена дослідженню проблем використання Інтернету речей для запобігання злочинності. Зроблено висновок про доцільність концептуального обґрунтування можливостей використання Інтернету речей для запобігання злочинності. При цьому використання Інтернету речей для запобігання злочинності можливе шляхом формування комплексної системи збору кримінологічно значимої інформації та її аналізу з використанням звукових датчиків, відеокамер, безпілотних літальних апаратів та інших технологічних елементів. Важливим є також вирішення проблем правового регулювання Інтернету речей та формування відповідної законодавчої бази.

Ключові слова: мережа Інтернет, Інтернет речей, злочинність, запобігання, правове регулювання.

Постановка проблеми. Початок третього тисячоліття ознаменувався зміною епох: людство вступило в нове інформаційне суспільство, в якому не матеріальне і не енергетичне, а феноменологічне фізичне поняття «інформація» стало методологією розвитку суспільства, основою отримання нових знань, а її виробництво і створення відповідних ресурсів стали пріоритетними завданнями суспільства та держави. Сучасна людина живе в інформаційному середовищі. Інформацію отримують, зберігають, передають та використовують на всіх рівнях. Новітні засоби інтелектуальної праці, що електронну, цифрову, обчислювальну техніку, покладені в основу автоматизації управління складними фізичними і розумовими процесами. Інформація та інформатизація всіх сфер суспільної діяльності стали закономірністю, а виробництво інформації – важливим завданням. Розвиток у рамках сучасної науки таких її галузей, як загальна теорія систем, кібернетика, інформатика, теорія управління, що виникли у ХХ столітті, був пов'язаний, перш за все, з їх активним взаємним проникненням у тому числі і на рівні методології, з погодженням і поширенням знань на рівні якісно нового розуміння механізмів еволюції неживої, живої та соціальної матерії. Ці науки мали основоположний вплив на формування сучасної кримінології [1, с. 12].

Розвиток можливостей мережі Інтернет та поява такого поняття, як Інтернет речей, не лише відкриває нові можливості для удосконалення життєдіяльності людини, але й дозволяє підвищити рівень запобігання злочинності, що потребує проведення відповідних наукових досліджень.

Аналіз останніх досліджень і публікацій. Питаннями інформаційного забезпечення

кримінологічних досліджень та використання мережі Інтернет для запобігання злочинності займалися такі вчені, як: В. М. Бесчастний, Д. І. Голосніченко, О. М. Джужа, А. П. Закалюк, О. Г. Кальман, А. В. Кирилюк, О. М. Литвак, О. М. Литвинов, П. С. Луцюк, Д. М. Цехан та ін.

Мета статті – дослідження можливостей використання Інтернету речей для запобігання злочинності та формування відповідних пропозицій для практичного застосування.

Виклад основного матеріалу дослідження. Інтернет речей (англ. Internet of Things, IoT) – концепція мережі, що складається із взаємоз'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу й обмін даними між фізичним світом і комп'ютерними системами за допомогою використання стандартних протоколів зв'язку. Окрім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини за рахунок використання інтелектуальних інтерфейсів. Набуває поширення також термін Internet of Everything, IoE – всеохоплюючий, або всеосяжний, Інтернет. Загалом основною концепцією Інтернету речей є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад холодильник, кондиціонер, автомобіль, велосипед і навіть

кросівки. Усі ці об'єкти (речі) повинні бути оснащені вбудованими датчиками або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії залежно від отриманої інформації. Прикладом впровадження такої концепції є система «розумний будинок» або «розумна ферма». Вже зараз Інтернету речей приділяється увага на найвищому рівні: зокрема, починаючи з 2009 року у Брюсселі за підтримки Єврокомісії проходять конференції Annual Internet of Things, на яких виступають із доповідями єврокомісари, науковці та керівники провідних ІТ-компаній. За прогнозами аналітиків найближчими роками очікується справжній бум Інтернету речей. Так, передбачається, що до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів [2].

Загалом Інтернет речей не лише спростить повсякденне життя, а й суттєво змінить світову економіку. Кількість пристроїв у недалекому минулому може у п'ятеро перевищити кількість населення планети [3].

Разом із цим можливістю Інтернету речей розглядаються також з точки зору використання правоохоронними органами та військовими. Зокрема, сьогоденні технічні можливості виявлення супротивника і наявність високоточного озброєння змушують до високої мобільності та швидкого прийняття рішень. Це можливо лише за умови оперативного отримання інформації з різних джерел у режимі реального часу усіма задіяними в операції підрозділами. Одним зі способів вирішення цієї проблеми стало застосування рішень, які отримали назву Інтернет бойових речей (Internet of Battle Things, IoBT) [4].

Можливості Інтернету бойових речей охоплюють збирання та обробку будь-якої корисної інформації; вона виступає у ролі агентів, які допомагають здійснити скоординовані оборонні дії; забезпечують керування та логістичну підтримку комбінованих операцій; здійснюють контроль стану транспортних засобів, моніторинг навколишнього середовища. Необхідно зазначити, що у 2016 році Нідерланди стали першою країною світу, яка повністю покрила себе національною мережею для Інтернету речей. В основі ідеї лежить створення енергоефективної мережі, яка б дозволила передавати невеликі обсяги інформації на значні відстані [5].

Використання Інтернету речей може забезпечити також якісно новий рівень запобігання злочинності, про що свідчить зарубіжний досвід. Так, у США Інтернет речей не тільки використовується на практиці для запобігання злочинності, але й розглядається

як один з елементів штучного інтелекту. Ідеї цього проекту полягають у тому, що злочини є відносно передбачуваними, однак для цього необхідно здійснити аналіз відповідних даних у короткий часовий проміжок. Цей вид аналізу був технологічно неможливим кілька десятиліть тому, але ситуація змінилася з появою мережі Інтернет та розвитком інформаційних технологій. При цьому використання Інтернету речей передбачається як для виявлення злочинців, так і для запобігання їм. Це досягається насамперед тим, що міська інфраструктура стає більш «розумнішою» та з'єднаною. А це, своєю чергою, дає змогу отримувати інформацію в режимі реального часу – від камер відеоспостереження до спеціальних датчиків. При цьому рівень технічних можливостей відеокamer, звукових та інших датчиків суттєво підвищився. Так, камери нового покоління здатні краще сканувати номерні знаки на автомобілях, здійснювати розпізнавання обличчя для пошуку потенційних злочинців або зниклих людей, а також автоматично виявляти підозрілі ситуації, як-от залишені без нагляду різноманітні предмети в публічних місцях та ін. Відеоспостереження дає змогу також аналізувати поведінку людини. Окремим напрямом розвитку Інтернету речей для запобігання злочинності є використання датчиків для відстежування пострілів з вогнепальної зброї. Технічні можливості обладнання дозволяють розпізнавати тип зброї, місце розташування, формувати відповідну базу даних [6].

Треба зазначити, що систему відстежування пострілів з використанням спеціальних датчиків називають також локатором пострілів. Практичне використання системи відбулось у 90-х роках минулого століття в США [7]. З розвитком інформаційних технологій та можливостей мережі Інтернет система фіксації пострілів удосконалювалась. Натепер існують спеціалізовані компанії, які займаються розробкою відповідного обладнання та програмного забезпечення. Зокрема, компанія ShotSpotter за результатами оброблення інформації щодо здійснених пострілів надсилає співробітникам поліції та іншим зацікавленим особам інформацію у вигляді SMS-повідомлень або на електронну пошту, вказуючи точне місце пострілу, час, дату та іншу інформацію [8].

Ще одним напрямом використання Інтернету речей для запобігання злочинності є безпілотні літальні апарати. Необхідно зазначити, що у 2012 році Федеральна авіаційна адміністрація США надала дозвіл правоохоронним органам на підготовку операторів безпілотних літальних апаратів.

Передбачається застосування безпілотних літальних апаратів для загального спостереження, виявлення потенційно небезпечних ситуацій, пошуку людей, контролю дорожньо-транспортної ситуації та інших потреб правоохоронних органів. Загалом вони повинні заповнити прогалини у відеоспостереженні та створити умови для швидкого та якісного отримання інформації [9].

У США також передбачається автоматичне відправлення безпілотних апаратів на місце, де були зафіксовані постріли за допомогою датчиків. Безпілотний апарат повинен прибути на місце раніше поліції, знімати подію на камеру та передавати інформацію у режимі реального часу. Передбачається, що автоматизовані безпілотники будуть забезпечувати кращу тактичну обізнаність поліції, швидше фіксувати інформацію щодо потенційних підозрюваних у скоєнні злочину, їхнього переміщення (в тому числі на транспортних засобах), наявності свідків, осіб що потребують медичної допомоги та ін. [10].

Використання Інтернету речей із залученням безпілотних апаратів для розслідування злочинів та попередження злочинності практикується також поліцією Великої Британії. Головними завданнями, які при цьому вирішуються, зокрема, є: здійснення фотота відео-фіксації злочинів, проявів антисоціальної поведінки, дорожньо-транспортних пригод, допомога у розшуку зниклих людей та ін. При цьому отримана інформація може бути використана в суді, наприклад, для демонстрації місця злочину присяжним. Важливим є також те, що використання безпілотних літальних апаратів є набагато дешевшим, ніж використання гелікоптерів [11].

Зважаючи на розвиток мережі Інтернет та можливості запуску після 2020 року технології мобільної передачі даних 5G, багато країн приділяють значну увагу формуванню державної політики у сфері Інтернету речей. Зокрема, у США прийнято рішення про розробку національної стратегії Інтернету речей (2016 р.) та подано до Сенату законопроект «Розвиток інновацій і сприяння Інтернету речей» (січень 2017 р.). У Великій Британії прийнято «Цифрову стратегію Великої Британії 2017», у Південній Кореї – Генеральний план створення Інтернету речей (2014 р.), у Японії – «Стратегію розвитку Японії – 2016», що передбачає також розвиток Інтернету речей. У Китаї розроблена та виконується державна програма розвитку Інтернету речей до 2020 року (вартість 127,5 млрд. дол.), а також заплановано перетворення 500 міст на так звані „smart city” [12, с. 8-9].

Висновки.

Отже, розвиток Інтернету речей є загальносвітовою тенденцією, що створює нові умови функціонування людського суспільства. Технологічні можливості Інтернету здатні забезпечити виконання різних завдань: від якісного підвищення побутових умов людини до використання у сфері штучного інтелекту. Безперечно, кримінологічна наука не може стояти осторонь цих процесів. На нашу думку, доцільним є концептуальне обґрунтування використання можливостей Інтернету речей для запобігання злочинності. При цьому використання Інтернету речей для запобігання злочинності можливе шляхом формування комплексної системи збору кримінологічно значимої інформації та її аналізу з використанням звукових датчиків, відеокамер, безпілотних літальних апаратів та інших технологічних елементів. Важливим є також вирішення проблем правового регулювання Інтернету речей та формування відповідної законодавчої бази.

Список використаних джерел:

1. Бандурка О.М., Литвинов О.М. Про кримінологічний сценарій світу інформаційної епохи. Актуальні проблеми кримінального права та кримінології у світлі реформування кримінальної юстиції: зб. тез доп. Міжнар. наук.-практ. конф. (19 трав. 2016 р., м. Харків, Україна) / МВС України, Харків. нац. ун-т внутр. справ; Кримінол. асоц. України; Ун-т Англія Раскін; Праз. ін-т дослідж. з питань безпеки (PSSI); Чес.кримінол. т-во; Харків. міськ. осередок гром. орг. «Всеукр. асоц. кримін. права». Харків: ХНУВС, 2016. 192 с.
2. Інтернет речей. URL: https://uk.wikipedia.org/wiki/Інтернет_речей (дата звернення: 22.05.2018).
3. Сич О. До 2020-го на Інтернет речей витратять 6 трильйонів доларів. URL: <http://energylife.info/ua/2016/Science/1550/До-2020-го-на-інтернет-речей-витратять-6-трильйонів-доларів.htm> (дата звернення: 22.05.2018).
4. Інтернет речей: цивільне і військове застосування. URL: <https://defence-ua.com/index.php/statti/4250-internet-rechey-tsyvilnei-viyskove-zastosuvannya> (дата звернення: 22.05.2018).
5. Левков О. Військовий Інтернет речей та українські реалії. URL: <https://defence-ua.com/index.php/statti/4224-viyskoviy-internet-recheyta-ukrayinski-realiyi> (дата звернення: 22.05.2018).
6. Faggella D. AI for Crime Prevention and Detection – 5 Current Applications. URL: <https://www.techemergence.com/ai-crime-prevention-5-current-applications/> (дата звернення: 22.05.2018).
7. Локатор выстрела. URL: https://ru.wikipedia.org/wiki/Локатор_выстрела (дата звернення: 22.05.2018).

8. Shotspotter technology. URL: <http://www.shotspotter.com/technology> (дата звернення: 22.05.2018).

9. Hill S. From drones to body cams, tech is changing the fight against crime. URL: <https://www.digitaltrends.com/features/dt10-crime-from-drones-to-body-cams-tech-is-changing-the-fight-against-crime/> (дата звернення: 22.05.2018).

10. Sonka J. Louisville seeks FAA approval for pilot program to fly automated drones to gunshot sites. URL: <https://insiderlouisville.com/metro/louisville-seeks-faa-approval-for-pilot-program-to-fly-automated-drones-to-gunshot-sites> (дата звернення: 22.05.2018).

11. Camber R. Take off for police drones air force: Remote-controlled 'flying squad' to chase criminals and hunt for missing people. URL: <http://www.dailymail.co.uk/news/article-4329714/Remote-controlled-flying-squad-chase-criminals.html> (дата звернення: 22.05.2018).

12. Баранов О. А. Интернет речей (IoT): огляд правових проблем. Интернет речей: проблеми правового регулювання та впровадження: матеріали науково-практичної конференції, 24 жовтня 2017 р., м. Київ. / упоряд.: В.М. Фурашев, С.Ю. Петряев. Київ: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. 238 с.

Статья посвящена исследованию проблем использования Интернета вещей для предотвращения преступности. Сделан вывод о целесообразности концептуального обоснования возможностей использования Интернета вещей для предотвращения преступности. При этом использование Интернета вещей для предотвращения преступности возможно путем формирования комплексной системы сбора криминологически значимой информации, ее анализа с использованием звуковых датчиков, видеокамер, беспилотных летательных аппаратов и других технологических элементов. Важным также является усовершенствование правового регулирования Интернета вещей и формирование соответствующей законодательной базы.

Ключевые слова: сеть Интернет, Интернет вещей, преступность, предотвращение, правовое регулирование.

The article is devoted to the investigation of the problems of using the Internet of things to prevent crime. The conclusion is made about the expediency of substantiating the possibilities of using the Internet of things to prevent crime. In this case, the use of the Internet of things to prevent criminal activity is possible by forming an integrated system for collecting criminologically significant information, analyzing it using sound sensors, video cameras, unmanned aerial vehicles and other technological elements. Important is also the improvement of the legal regulation of the Internet of things and the formation of an appropriate legislative framework.

Key words: Internet network, Internet of things, crime, prevention, legal regulation.

