УДК 340:004

Вадим Анатолійович Коршенко,
кандидат юридичних наук, завідувач науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ

Гаджети – прихована загроза

Слово «гаджет» щільно ввійшло в наш побут. Ми живемо в часи коли нікого не здивуєш функціональним смартфоном, смарт телевізором, розумним порохотягом, холодильником чи годинником. Деякі автори навіть стверджують що ми живемо в епоху гаджетів [1; 2]. Що означає це модне слово зможе пояснити навіть дитина – це портативний пристрій, який об'єднує в собі кілька функцій. У перекладі з англійської gadget – пристосування, технічна новинка. Тож щоб перетворити звичайну річ на гаджет потрібно додати їй новітніх функцій, інтелектуальності, електронної функціональності, іншими словами коп'ютерізовати її. Тобто щоб стати гаджетом, звичайна річ (годинник, дитяча іграшка, телефон, лампа освітлення тощо) повинна бути оздоблена власним процесором що перетворює її на мікрокомп'ютер. З розвитком технологій ці вбудовані мікрокомп'ютери стають дедалі потужнішими, обладнуються телекомунікаційними модулями, що надає їм можливість отримувати та передавати інформацію. З'явився термін «Інтернет речей», як концепція комунікації та взаємодії гаджетів між собою та з навколишнім середовищем.

Здавалось би від цього людство отримає тільки вигоду. Однак ця тенденція несе дуже серйозні потенційні загрози. Брюс Шнайер, консультант з безпеки, який досліджує так звані «дірки» в інтернеті речей та описує їх, у своїй книзі «Натисніть сюди, щоб вбити усіх» зазначає, що він не налаштований цілком песимістично, але тут складно зберігати спокій, адже економічні та технічні цілі індустрії інтернету речей, не відповідають тим заходам безпеки які необхідні для забезпечення конфіденційності суспільства. Вбудувавши комп'ютер у звичні нам речі, компанії перетворюють весь світ у суцільну загрозу [3].

Проблема полягає в тому, що бізнес-моделі більшості бюджетних гаджетів не передбачають того рівню безпеки, який розповсюджується на традиційні інтернет пристрої. Бюджетні виробники гаджетів не

мають ані досвіду ані стимулу підтримувати достатній рівень безпеки своєї продукції. Тому інтернет речей – це синонім до словосполучення «погана безпека» [4].

Погана безпека несе в собі як ризики витоку особистих даних користувача гаджету, таких як стану здоров'я, місця знаходження, фотографій, відеозаписів, телефонних та навіть звичайних побутових розмов, особистої переписки, фінансових даних, тощо, так і створення на базі заражених гаджетів ботнетів, проведення ними DDoS-атак, незаконного видобутку криптовалюти та ін. За оцінками спеціалістів компанії ТрендМікро, світового лідеру в області рішень для захисту корпоративних даних і кібербезпеки для бізнесу, переважна більшість всіх зафіксованих атак в 2018 році були або спрямовані на гаджети, або виконані з їх допомогою.

Сьогодні існує велика кількість інтернет-ресурсів для пошуку вразливих гаджетів підключених до інтернету, і пошук та використання таких вразливостей набуває все більшої популярності між зловмисників які спеціалізуються на злочинах у кіберпросторі та в сфері високих технологій. Більшість людей навіть гадки не має яку загрозу можуть нести сучасні гаджети. Дуже велика частина гаджетів, особливо бюджетних гаджетів китайського виробництва, вже на етапі завантаження на них базового програмного забезпечення мають або серйозні «діри» в безпеці, або містять потенційно небезпечний програмний код. Необхідно доносити до пересічних громадян інформацію про зазначену небезпеку. Потрібно запроваджувати інформаційні програми державного рівня для донесення до населення інформації про потенційні загрози. Водночас з тим вже пройшли ті часи коли відносна безпека досягалась встановленням антивірусу на конкретний пристрій. В теперішніх умовах неможливо досягти успіху в забезпеченні безпеки локальним програмним забезпеченням, адже для більшості гаджетів воно не існує, а самі гаджети переважно не передбачають можливість його встановлення взагалі. Досягти безпеки у світі гаджетів та в інтернеті речей можна тільки використовуючи глобальні програмно-технічні комплекси захисту, які досить коштовні, та можуть бути встановлені переважно на телекомунікаційних вузлах. Звісно великі корпорації можуть дозволити собі встановлення корпоративних систем захисту. Захист від атак на гаджети пересічних громадян та відслідковування підозрілої активності таких гаджетів повинні здійснюватися на рівні операторів та провайдерів телекомунікаційних послуг. Законодавчо досить важ-

ко врегулювати такі відносини, однак існує можливість проводити заохочувальну політику в сфері захисту інформації і кібербезпеки, та надавати певні пільги чи преференції компаніям, які будуть встановлювати такі системи безпеки. В подальшому, в процесі підвищення обізнаності населення в сфері загроз в інтернеті речей та неминучому зростанні кількості гаджетів в кожному окремому домогосподарстві, наявність функцій програмно-технічного захисту на рівні оператора/провайдера буде напряму впливати на конкурентоспроможність його послуг серед населення, водночас підвищуючи безпеку в сфері захисту і кібербезпеки в цілому в Україні.

Список бібліографічних посилань

1. Мірошнікова А. Чому безграмотність стає нормою? Освіторія : сайт. URL: https://osvitoria.media/experience/chomu-bezgramotnist-staye-normoyu/?fbclid=IwAR2dTgAczAcVHUOfTo1ZtvHYahp-HDVEc132M8YA8diVrD9A0joUCMMkav8 (дата звернення: 22.10.2019).
2. Коптюг Н. Эпоха гаджетов // Учительская газета : сайт. 30.05.2017. URL: http://www.ug.ru/method_article/1165 (дата звернення: 22.10.2019).
3. Shnayyer B. Click Here to Kill Everybody : Security and Survival in a Hyper-connected World. W. W. Norton & Company, 2018. 288 p.
4. Manjoo F. A Future Where Everything Becomes a Computer Is as Creepy as You Feared// The New York Times. Oct 10, 2018. URL: https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html (дата звернення: 22.10.2019).

Одержано 23.10.2019