DOI 10.34054/bdc006

Інтернет речей: проблеми безпеки та основні засади її забезпечення

Марія Диха[21]

Інтернет речей (Internet of Things, IoT) – «концепція мережі, що складається із взаємозв'язаних фізичних 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» (Інтернет речей, n.d.).

Аналізуючи підходи до визначення IoT вважаємо, що Інтернет речей – це взаємодія пристроїв й інших предметів в мережі, які збирають, обробляють, обмінюються даними завдяки електроніці, програмному забезпеченню з метою виконання визначених завдань та реалізації певних функцій.У найбільш поширеному розумінні IoT дозволяє фізичним об'єктам (речам), здійснювати взаємодію між собою або з зовнішнім світом, частково або повністю без участі людини.

Запровадив термін «інтернет речей» Кевін Ештон у своїй доповіді «Інтернет Речей» для «Procter & Gamble» в 1999 р. з ідеєю впровадження радіочастотної ідентифікації

[21] Професор кафедри економіки підприємства і підприємництва, доктор економічних наук, професор, Хмельницький національний університет, Україна

(RFID) в ланцюг поставок виробничих товарів чим привернув увагу до самої ідеї підключення до мережі нових типів пристроїв. На сьогодні розробками в сфері досліджень і стандартизації інтернету речей займаються багато країн як на рівні національних ініціатив, наприклад ANSI (США), BSI (Великобританія), так і на інтернаціональному рівні: ETSI, ITU, ISO, IEC.

Інтернет речей вже сьогодні приносить великі зміни у повсякденному житті. А за прогнозами Gartner, «до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпеченнята послуг становитиме 1,9 трлн дол» (Gartner says the Internet of Things, 2013).

Інтернет речей з'єднує мільярди нових пристроїв з інтернетом, але це також розширює можливості кібератак хакерів проти мереж та інформації. Широке включення «розумних» пристроїв у повсякденні об'єкти призводить до появи нових вразливих місць як в інфраструктурі, яку вони підтримують, на яку вони покладаються, так і на процеси, якими воникерують.

Кібератак зазнають державні інституції, бізнес структури, окремі сектори економіки (наприклад, енергетична мережа), а також і окремі особи.

Дослідники з безпеки продовжують розкривати вразливі місця у функціонуванні міжнародних і державних інституцій, у різних сферах ведення бізнесу і життєдіяльності людей. Зокрема, у промислових та комерційних програмах можемо навести такі приклади (Fisher, E. A., Liu, E. C., Rollins, J. W., Theohary, C. A., 2014; National Vulnerability Database, n.d.):

1) кібернападники атакували підприємство з метою отримання доступу до його ділової мережі. Кіберзловмис-

ники вразили металургійний комбінат у Німеччині, маніпулюючи та руйнуючи системи управління та запобігаючи зупиненню доменної печі регульованим способом, що призвело до «масових пошкоджень».

2) комерційна посудомийна машина, яка може бути підключена до інтернету, включає в себе вбудований веб-сервер, який «прослуховує порт 80 і схильний до атаки переходу по каталогу. Отже, зловмисник може використати цю проблему для доступу до конфіденційної інформації для атак» (National Vulnerability Database, n.d.).

Щоб протистояти загрозам IoT варто розуміти їх природу та технології їх поширення. В цьому контексті варто звернути увагу на доповідь дослідницьких служб (CRS) від 2014 року до Конгресу США, в якій визначено п'ять типів кіберзловмисників:

1. Кібертерористи: транснаціональні терористичні організації, бойовики та джихадисти, які використовують інтернет як інструмент планування атак, форму війни, радикалізації та вербування, метод розповсюдження пропаганди та засіб комунікації.

   Експеримент DHS Aurora передбачав комп'ютерну атаку на систему управління генератором енергії, яка призвела до припинення операцій та знищення обладнання.

2. Кібершпигуни: особи, які викрадають секретну або конфіденційну інформацію, якою користуються уряди або приватні корпорації, щоб отримати конкурентну стратегічну, безпечну, фінансову чи політичну перевагу. Зокрема, у звіті ФБР за 2011 рік зазначено: «Компанія стала жертвою вторгнення та втратила за добу 1 мільярд доларів досліджень і розробок, які розроблялися 10 років».

3. Кіберзахоплення: особи, які займаються незаконними кібератаками для отримання грошової вигоди. Важко оцінити, але щорічні глобальні витрати для приватних осіб складають сотні мільярдів доларів (і втрата довіри-клієнтів).

4. Кіберагенти: це агенти або квазіагенти національних держав, які розвивають свої можливості та здійснюють кібератаки для підтримки стратегічних цілей країни. У серпні 2012 року серія кібер-атак була спрямована проти Саудівської фірми Арамко, найбільшого у світі виробника нафтогазової промисловості. Напади спричинили спустошення 30 тисяч комп'ютерів компанії, а сам програмний код вірусу, мабуть, покликаний порушити або зупинити виробництво нафти. Деякі співробітники служби безпеки заявляють, що Іран, можливо, підтримав цю атаку.

5. Кіберг-активісти: особи, які виконують кібер-атаки для задоволення, або за філософськими чи іншими не грошовими міркуваннями.

Серед основних загроз та недоліків IoTвважаємо за доцільне звернути увагу на такі:

1. Відсутність єдиної системи. Проблема інтеграції IoT – у відсутності загальних правил і стандартів. Поки не буде розуміння загальної картини, складно впровадити універсальне рішення.

2. Енерговитратність. Для повноцінної роботи IoT потрібно домогтися автономності мережі і отримувати енергію з навколишнього середовища.

3. Питання безпеки та приватності. Основний ризик – у відкритій базі даних. У шахраїв з'явиться можливість

зламувати не тільки рахунки і комп'ютери, але навіть холодильники.

4. Вартість. Техніка дорога, незважаючи на те, що її використання окупиться в майбутньому: система «розумний дім» допоможе заощадити на електриці і водопостачанні, обладнання на виробництві завчасно сповістить про ризик поломки, кухонна техніка дозволить уникнути псування продуктів.

Аналізуючи технологічний прогрес останніх десятиліть, можна впевнено сказати, що людство рухається до впровадження концепції IoT в життя.

Отже, необхідно проектувати системи для забезпечення безпеки. В цьому контексті важливо збалансувати витрати на захист та час на його забезпечення.

Захист рішень на базі IoT від тих, хто планує завдати шкоди, буде мати вирішальне значення для зростання IoT, а також для особистої та ділової безпеки.

Серед основних засад забезпечення безпеки вважаємо за необхідне виділити такі:

1. Комунікаційні технології. Шифрування – складний процес, має наслідки від апаратного забезпечення до ключового управління, але є ефективним рішенням для безпечного IoT.

2. Послуги, мови та інструменти. Слабкі сторони програмного забезпечення у системі та коді призводять до вразливої роботи IoT. Мова, стандарти дизайну та кодування, а також інструменти, які їх підтримують, утримання служб, пов'язаних із безпекою – потребують фінансування, але економія на таких складових може призведе до серйозних порушень, яких можна було б запобігти.

3. Сертифікація. Сертифікація безпеки може вимагатись для певного напрямку діяльності. Навіть якщо це не потрібно зараз, усвідомлюючи вимоги щодо сертифікації та включення корисних елементів у практику розробки, вже зараз потрібно створювати безпечні продукти та потенційно підготувати їх до вимог сертифікації в майбутньому.

4. Промислова кооперація. Боротьба з хакерами – це асиметрична війна. Співпраця щодо виявлення дефектів, відстеження та спільного використання розробок, навіть конкурентів, стала прийнятною практикою. Так NIST Cybersecurity Framework призвела до розробки основ для організації зусиль щодо впровадження та адаптації практик безпеки в організації.

Отже, для інтернету речей характерні ще більш складні проблеми забезпечення безпеки в порівнянні з тими, які властиві для мереж зв'язку. До них додаються можливі проблеми масштабованості мережі, викликані мало передбачуваним обсягом передачі даних від великого числа вузлів, ненадійність програмного забезпечення, тощо.

Широке застосування інтернету речей є результатом інтеграції комп'ютерних технологій, технологій зв'язку і різних областей промислових галузей. Крім порушення інформаційної безпеки традиційних мереж зв'язку (в результаті ризику підслуховування, спотворення інформації, розкриття інформації) пристрої та мережі інтернету речей стикаються з додатковими проблемами безпеки на прикладному рівні – при використанні хмарних обчисленнях, обробці інформації, забезпеченні прав на інтелектуальну власність, захист приватності тощо.

У найближчому майбутньому середовище IoT буде безпосередньо причетне до життя простих людей та до бізнесу

і державної діяльності. Отже, таку складну структуру необхідно будувати з урахуванням сучасних вимог до інформаційної безпеки. До питання забезпечення захищеності інформації в межах IoT необхідно підходити комплексно і особливо приділяти уваги таким аспектам як безпека кінцевих інформаційних систем і безпека їх взаємодії.

Список використаних джерел

Fisher, E. A., Liu, E. C., Rollins, J. W., Theohary, C. A. (Dec. 15, 2014). The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress. *Congressional Research Service.* Retrieved from https://fas.org/sgp/crs/misc/R42984.pdf

Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. (Dec 13, 2013). In Finyear. Retrieved from https://www.finyear.com/Gartner-Says-the-Internet-of-Things-Installed-Base-Will-Grow-to-26-Billion-Units-By-2020_a27901.html

National Vulnerability Database (n.d.). National Institute of Standards and Technology. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2017-7240

Інтернет речей. (n.d.). Вікіпедія. Retrieved June 1, 2019 from https://uk.wikipedia.org/wiki/Інтернет_речей