АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Кисиленко В.К., студент (гр. РС-42, РТФ НТУУ «КПІ ім. Ігоря Сікорського»)

Вступ. Інтернет речей (англ. Internet of Things, IoT) – це мережі, що складаються із сукупності фізичних об'єктів (речей) або пристроїв, які мають вбудовані сенсори, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даних між об’єктами і комп'ютерними системами. Крім сенсорів, мережі Інтернету речей можуть мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові і бездротові мережі. Ці взаємопов'язані об'єкти виконують функції зчитування, приведення в дію, програмування та ідентифікації, та дозволяють виключити необхідність участі людини у багатьох процесах.

Протягом останнього десятиліття Інтернет речей плавно увійшов в наше життя завдяки появі систем бездротового зв'язку, таких як RFID, Wi-Fi, 4G, IEEE 802.15.x, які найчастіше використовуються в основі додатків моніторингу та контролю. Сьогодні системи Інтернету речей використовують не тільки для приватних мереж, а й на виробництвах, фабриках, заводах, підприємствах та навіть в державних установах. Основна проблема використання мереж IoT полягає в тому, що вони не мають захисту від впливів зі сторони зловмисника. Це може призвести, в ліпшому випадку, до заподіяння шкоди майну користувача, а в гіршому – його здоров’ю та життю.

Наприклад, пристрої контролю та управління електричною мережею можуть бути захоплені зловмисником за допомогою будь-якого девайсу, що має доступ до мережі Інтернет, та відповідного програмного забезпечення. Отримавши повний чи частковий контроль над пристроєм зловмисник може спричинити вимкнення або псування електричних приладів, в тому числі критично-необхідних приладів (систем життєзабезпечення в лікарнях, систем моніторингу на виробництві, охоронних систем, тощо), створити коротке замикання в мережі та навіть спричинити пожежу або аварію, якщо мова йде про виробництво. Саме тому постає актуальна проблема дослідження безпеки Інтернету речей та, зокрема, безпеки користувача, його майна та особистої інформації, що передається, обробляється та зберігається в мережах IoT.

Предметом дослідження є загальна оцінка небезпек для Інтернету речей на основних структурних рівнях, проблеми захисту персональних даних людини та забезпечення конфіденційності її інформації, основні ризики, пов’язані з інтеграцією Інтернету речей в життя людини, вплив незахищеності Інтернету речей на життєдіяльність людини.

Аналіз публікацій. Високий рівень неоднорідності в поєднанні з широкою гамою систем Інтернету речей, як очікується, підвищить існуючий рівень загроз безпеки в глобальній мережі, яка все частіше використовується для взаємодії людей, машин і роботів. Зокрема, традиційні заходи дотримання конфіденційності і протидії загрозам не можуть бути безпосередньо застосовані до технологій IoT через їх обмежені обчислювальні потужності. Крім того,

велика кількість з'єднаних пристроїв створюють проблему масштабованості. В роботі [1] приведено інформацію про ринок IoT, його перспективи, темпи розвитку, а також аніліз можливих ризиків, що з’являться з повною інтеграцією IoT в життя людини. В статті [2] приведений аналіз основних проблем безпеки Інтернету речей.

Для досягнення повного визнання з боку користувачів визначення і досягнення необхідного рівня безпеки та захищеності для Інтернету речей є обов'язковими. Крім цього, повинні бути гарантовані безпека та анонімність даних користувача, їх конфіденційність і цілісність, а також надійність механізмів аутентифікації і авторизації. Це необхідно для запобігання несанкціонованого доступу неавторизованих користувачів до системи. В статті [3] наведені основні криптографічні методи захисту інформації, забезпечення її конфіденційності та цілістності для мереж Інтернету речей.

Оскільки недосконаліть, незахищеність Інтернету речей може призвести до негативних впливів на життєдіяльність людини, зокрема до завдання шкоди фізичному та психологічному здоров’ю з боку зловмисника, ці проблеми будуть розглянуті в нашій роботі.

Основні результати дослідження. Для Інтернету речей визначені три основні характеристики – комплексні знання, надійність передачі інформації та інтелектуальна обробка. Відповідно до цих характеристик структура Інтернету речей може бути розділена на три рівні – рівень сприйнятті, мережевий рівень і прикладний рівень [4].

Завдання рівня сприйняття – отримати надійне, цілісне та вірогідне зчитування інформації з сенсорів, RFID-міток, тощо.

Мережевий рівень забезпечує доступ, передачу інформації, її обробку та зберігання. Він складається з рівня доступу (мобільні мережі зв'язку) і основного рівня обміну (Інтернет, NGN, віртуальні приватні мережі). Більшість сенсорних мереж використовують бездротові мережі зв'язку: персональні мережі (WPAN), локальні мережі (WLAN), міські мережі (WMAN), глобальні мережі (WWAN), а також супутникову мережу. Сенсорні мережі в IoT використовують протоколи зв'язку на основі IP [1].

Прикладний рівень аналізує і обробляє прийняту інформацію для визначення оптимального рішення і контролю за управлінням, додатками і послугами. На прикладному рівні виконуються функції зі збору та зберігання даних, забезпечення ефективності енергозабезпечення і логістики.

Основна проблема безпеки на рівні сприйняття полягає у фізичній безпеці приладів сприйняття і безпеці збору інформації. Для більшості вузлів сприйняття характерна відсутність стандартів, різноманітність, простота, обмежене енергозабезпечення та слабка здатність до забезпечення безпеки. Тому Інтернет речей не може забезпечити уніфіковану систему захисту безпеки і є вразливою для зловмисника, який хоче завдати шкоди користувачу. Так як бездротова сенсорна мережа на рівні сприйняття є джерелом інформації, то інформаційна безпека на цьому рівні дуже важлива. Вона включає фізичне захоплення сенсорних вузлів, захоплення вузлів шлюзу, витік інформації

сенсора, загрози цілісності даних, порушення енергозабезпечення, загрози перевантаження, атаки типу DoS, загрози маршрутизації встановленням в мережу нелегітимних сенсорів і загрози копіювання вузла.

Загрози для безпеки існуючих мереж зв'язку поширюються і на Інтернет речей, який побудований на них. До них відносяться: несанкціонований доступ, перехоплення даних користувача, порушення конфіденційності, цілісності інформації, DoS-атаки, віруси, експлойтери, мережеві черв'яки, тощо. Крім того, існують міжмережеві проблеми аутентифікації, які можуть бути причиною DDoS та DoS-атак [2,3].

Для Інтернету речей стоять ще більш складні проблеми забезпечення безпеки в порівнянні з тими, які характерні 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, і т.д.[1].

Іноземні фахівці приділяють велику увагу науковим і експериментальним дослідженням в забезпеченні інформаційної безпеки Інтернету речей. Найбільший ризик для безпеки знаходиться на нижньому рівні архітектури – рівні сприйняття. При цьому не можна ігнорувати ризики для безпеки на інших рівнях архітектури IoT, для яких також характерний високий рівень ризику [4].

Висновки. Стрімкий розвиток кількості систем та мереж Інтернету речей викликаний широким поширенням бездротових технологій і міжмашинного обміну, розвитком технологій хмарних обчислень і початком переходу на IPv6. Однак, використання IoT в багатьох областях обмежено складними проблемами в частині забезпечення інформаційної безпеки, конфіденційності та безпеки інформації.

Прийняття обґрунтованих заходів безпеки, що протистоять виявленим недолікам, а також впровадження різних систем виявлення вторгнень, криптографічних заходів безпеки в процесі обміну інформацією та використання ефективних методів комунікації призведе до створення більш безпечної і надійної інфраструктури Інтернету речей, що зможе гарантувати безпеку здоров’я, інформації та майна користувача.

Науковий керівник: Гусєв А.М., к.б.н., доцент (каф. ОПЦБ НТУУ «КПІ ім. Ігоря Сікорського»)

Література

1. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. СПб.: БХВ-Петербург. — 2015. — 160с.

2. Соколов М.Н., Смолянинова К.А., Якушина Н.А. Проблемы безопасности интернета вещей: обзор. — Вопросы кибербезопасности : журнал. — 2015. — № 5(13). — 34с.

3. Лукацкий А.С. Криптография в "Интернете вещей" // www.slideshare.net : сайт. — 2016. — 23 марта.

4. Khan, R. [and others], Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, Frontiers of Information Technology (FIT), 2012 10th International Conference on. — 2012. — 257-260 с.