УДК 004.05(043.2)

Олена Дубчак, ст.викладач,
Євгенія Галич, Владислав Павленко
(Національний авіаційній університет, Україна)

Аналіз проблем інформатизації в сфері Інтернету речей

Ця стаття містить інформацію про Аналіз проблем інформатизації у сфері Інтернету речей та розподіл проблем інформатизації IoT.

Стрімкий розвиток інформаційних технологій став відправною точкою впровадження технологій збирання даних. З реалізацією цієї ідеї почали з'являтися та активно застосовуватися на практиці раніше невідомі технології, які зараз полегшують життя мільйонам людей. Інтернет речей (Internet of Things, IoT) знаходиться лише на початку свого шляху, тільки зароджується, проте швидко розвивається, збільшуючи щорічно обсяг міжмережевого трафіку. Але всі інноваційні технології, що впроваджуються, містять в собі серйозні виклики інформаційній безпеці.

IoT - концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають в собі вбудовані датчики, та програмного забезпечення (ПЗ). Ця технологія дозволяє здійснювати передачу і обмін даними за допомогою використання стандартних протоколів зв'язку. Мережі можуть з'єднувати виконавчі пристрої, вбудовані у фізичні об'єкти, за допомогою дротових або бездротових носіїв. Але IoT не тільки приєднує датчики до існуючих пристроїв, він створює ринок для нових підключень. Усі ці взаємопов'язані речі генерують майже неймовірну кількість даних і мають можливість зчитувати та аналізувати інформацію, приводити в дію механізми, програмувати та ідентифікувати, а використання інтелектуальних інтерфейсів робить втручання людини непотрібним.[1]

Хоча питання, пов'язані із захистом систем, в тому числі з використанням пристроїв IoT, вивчалися багатьма вченими та експертами в цій галузі, але не всі виробники в сучасному світі готові констатувати вразливість і загальну незахищеність своєї продукції. Існує ще багато проблем безпеки у всьому середовищі IoT, починаючи від виробників і закінчуючи користувачами.

Аналіз безпеки технології IoT є одним з ключових аспектів використання цієї технології, а основними проблемами безпеки IoT є несанкціонований доступ до мережі; пошкодження або викрадення даних; відсутність стандартизованої автентифікації та доступу до даних. Для вирішення цих проблем фахівці та експерти рекомендують використовувати такі заходи, як шифрування, автентифікація та мережева безпека. *Шифрування* необхідно використовувати для захисту даних від несанкціонованого доступу. *Автентифікація*, зазвичай, містить такі процедури, як ідентифікація та авторизація для перевірки особи користувачів і обмеження доступу до ресурсів та інформації. *Мережева безпека* може бути використана для забезпечення безпеки в Інтернеті та захисту даних від несанкціонованого доступу та

використання. Сюди слід віднести такі заходи, як моніторинг мережі та захист від атак шкідливого ПЗ.

Варто згадати основну проблему в сфері IoT – шкідливі програми. Наприклад, ботнет – ПЗ, розроблене для IoT. Бот-мережа це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами - автономним ПЗ. Зазвичай використовується для незаконних дій, таких як: розсилання спаму; перебирання паролів на віддалених системах; DoS – атаки - на відмову в обслуговуванні; несанкціоноване отримання персональних даних користувачів; викрадення номерів кредитних карток і паролів доступу.[2] Та, крім цих проблем, ботнет може завдати шкоду багатьом споживачам. Зловмисники можуть використовувати велику кількість споживчих пристроїв з низьким рівнем безпеки для здійснення атак, наприклад, на об'єкти критичної або громадської інфраструктури. Бот-мережа IoT може ініціювати величезні перебої з підключень датчиків, що може спричинити згубні сплески використання інфраструктури. Це може призвести до стрибків напруги та зниження доступності критично важливої інфраструктури. Існують певні рішення для пом'якшення дій таких атак, наприклад, більш розумне ПЗ, яке може відрізнити дані про надзвичайні ситуації від даних, що надходять від несправних датчиків. Таке ПЗ може встановлювати обмеження як на тип даних, які пристрій може надсилати, так і на частоту їх надсилання.

Відсотковий розподіл проблем інформатизації IoT може залежати від ряду факторів, таких як галузь використання і тип пристрою. Однак можна виділити загальні проблеми, які стосуються сектору IoT.

1. Безпека - ця проблема становить 47% від загальної кількості проблем, пов'язаних з IoT. Безпека може бути серйозною загрозою, оскільки пристрої IoT вразливі до кібератак та крадіжок особистої інформації.
2. Конфіденційність - 25% від загальної кількості проблем в IoT. Збір та обробка персональних даних користувачів, зібраних різними пристроями IoT, такими як домашні камери спостереження та медичні пристрої, є ключовим питанням проблеми інформатизації.
3. Стандартизація - становить 17%. Відсутність єдиних стандартів для пристроїв IoT може спричинити проблеми у їх взаємодії та розвитку.
4. Інші проблеми – 11% від усіх задач інформатизації пристроїв IoT.[3]

Проблеми інформатизації IoT можуть бути вирішені різними шляхами. Якщо висвітлити проблему *безпеки*, можна дійти до висновку, що необхідно використовувати захист пристроїв за допомогою відповідних шифрувальних технологій, використовувати сильні паролі та автентифікацію користувача. Також важливо постійно вдосконалювати програмне забезпечення пристроїв, щоб запобігти виявленим вразливостям. Для забезпечення *конфіденційності* персональних даних користувачів, які збираються за допомогою пристроїв IoT, необхідно забезпечити їх захист від несанкціонованого доступу. Один із способів - це використання механізмів шифрування та автентифікації, які дозволяють перевіряти ідентичність користувача та забезпечують конфіденційність передачі даних. Вирішення проблеми *стандартизації* може

бути досягнуто шляхом розробки єдиних стандартів та протоколів для пристроїв IoT. Це дозволить забезпечити сумісність різних пристроїв та спростить їх взаємодію між собою. Щодо *інших проблем*, які можуть виникнути в процесі інформатизації IoT, можна виділити такі варіанти вирішення проблем як вдосконалення аналітики даних та ефективне управління життєвим циклом пристроїв IoT. Аналітика даних може допомогти покращити ефективність використання пристроїв, підвищити якість обслуговування клієнтів, прогнозувати виникнення проблем з пристроями та забезпечити їх попередження а управління життєвим циклом пристроїв IoT має бути ефективним, щоб забезпечити їх надійність та довговічність.

Після проведення аналізу проблем інформатизації в сфері IoT можна зробити висновок, що хоча ця технологія дуже перспективна, вона все ще стикається зі значними викликами і проблемами. Тому її розвиток потребує вирішення ряду важливих проблем, таких як безпека, збір і захист даних, дотримання стандартів та енергоефективність.

Список літератури

1. Баранов О.А. "Інтернет речей" як правовий термін. Юридична Україна /О.А.Баранов // Київ: 2016. - № 5/6 (161/162).- 96 ст.
2. Чубенко А.Г. ТЕРМІНОЛОГІЧНИЙ СЛОВНИК з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / А.Г Чубенко та ін. // Київ:2018.- 118 ст.
3. Звіт компанії Thales, "2019 Global IoT Security & Privacy" [Електронний ресурс]:https://www.thalesgroup.com/en/markets/digital-identity-and-security/internet-things/white-paper/2019-global-iot-security-privacy