

ІНТЕРНЕТ РЕЧЕЙ: МОЖЛИВОСТІ І ЗАГРОЗИ

Розвиток Інтернет спричинив зміни у соціальному розвитку суспільства, відбулися зміни у тому, як люди взаємодіють, працюють, відпочивають, живуть. Інтернет створив нові галузі і нові ринки для багатьох напрямів діяльності, заклав підвалини для цифрової трансформації суспільства і бізнесу. В першу чергу це дозволяє ефективно здійснювати комунікацію людей між собою і навколишнім світом. Але в 21 столітті за допомогою Інтернет речей між собою можуть здійснювати комунікацію не тільки люди, але й речі. Тобто пристрої також можуть взаємодіяти між собою без втручання людини, збираючи і обмінюючись даними [1]. Ці дані надсилаються в хмару для аналізу або аналізуються локально. Пристрої можуть діяти на основі інформації, яку вони отримують один від одного. Більша частина роботи пристроїв відбувається без втручання людини, але люди можуть взаємодіяти з ними, наприклад, налаштовувати їх, давати інструкції або отримувати доступ до даних.

Таким чином, Інтернет речей (IoT) – це система взаємопов'язаних обчислювальних пристроїв, механічних і цифрових машин, об'єктів, тварин або людей, яким надано унікальні ідентифікатори (UID) і які мають здатність передавати дані через мережу від людини до людини або від людини до комп'ютера і навпаки [2]. Промисловий інтернет речей (IIoT) – це система об'єднаних комп'ютерних мереж і підключених до них промислових (виробничих) об'єктів з вбудованими датчиками і програмним забезпеченням для збору та обміну даними, з можливістю віддаленого контролю і управління в автоматизованому режимі, без участі людини [3].

Сьогодні кількість підключених до Інтернет пристроїв перевищила кількість населення світу. Річчю в IoT може бути людина з серцевим імплантатом, сільськогосподарська тварина з ін'єкційним ідентифікаційним чіпом, автомобіль із вбудованими датчиками, які сповіщають водія про низький тиск у шинах, або будь-який інший природний або штучний об'єкт, якому можна призначити адресу Інтернет-протоколу (IP) і який може передавати дані через мережу.

Основними характеристиками пристроїв IoT є те, що вони здатні підключатися до Інтернету та взаємодіяти з його середовищем шляхом збору й обміну даними. Ці пристрої сьогодні настільки різноманітні що існує незліченна кількість способів використання IoT у різних сферах діяльності. Ці розумні, постійно підключені пристрої надають контекстну інформацію в реальному часі з низькими накладними витратами для оптимізації процесів життєдіяльності людей і життєздатності компаній.

Багато підприємств пов'язали можливості розвитку свого бізнесу з Інтернет. Вони все частіше використовують IoT, щоб працювати ефективніше, краще розуміти клієнтів, надавати їм покращене обслуговування, покращувати процес прийняття рішень і підвищувати цінність бізнесу.

Найбільш поширеними видами використання IIoT є такі: розумне виробництво; підключені пристрої, профілактичне та прогнозне обслуговування; розумні електромережі; розумні міста; підключена логістика; розумні цифрові ланцюги поставок тощо. Вигодами, які підприємство може отримати від використання цих технологій є: отримання інформації на основі даних IoT для кращого управління всіма бізнес-процесами; підвищення продуктивності та ефективності господарських операцій; створення нових бізнес-моделей і джерел доходу; економія часу у виробництві, обслуговуванні, прийнятті рішень. Використання Інтернету речей у промисловості дозволяє провести моніторинг виробничої лінії, щоб забезпечити проактивне технічне обслуговування обладнання у разі виявлення датчиками загрозливої несправності. Це дозволяє компаніям зменшити операційні витрати, збільшити час безвідмовної роботи та покращити управління продуктивністю основних засобів. Датчики на виробництві також допоможуть швидко та ефективно здійснювати контроль якості і визначати загрози екології.

Споживач отримує перевагу від використання IoT в автомобілях, так як датчики можуть виявляти загрозливу несправність в транспортних засобах, які вже знаходяться в дорозі, і можуть попереджати водія детальною інформацією та рекомендаціями. Таким чином, виробники та користувачі автомобілів можуть дізнатися більше про те, як підтримувати автомобілі в робочому стані. Вже зараз люди користуються машинами зі штучним інтелектом, які обладнані купою сенсорних кнопок та автоматично під'єднуються до інтернету. Також безпілотні автомобілі з технологією штучного інтелекту вже не виглядають фантастично, а стають реальністю.

Транспортні та логістичні системи отримують переваги від різноманітних додатків IoT. Маршрути вантажівок, кораблів і поїздів, які перевозять вантаж, можуть бути змінені залежно від погодних умов, наявності транспортних засобів або водіїв. Сам вантаж також може бути оснащений датчиками для відстеження та контролю температури. В харчовій і фармацевтичній промисловості, у виробництві напоїв, квітів запаси продукції і сировини особливо чутливі до температури, у цьому разі контролювання температурного режиму зберігання може бути особливо корисним і ефективним.

Для підприємств роздрібною торгівлі технології IoT можуть бути у нагоді для керування запасами, покращення взаємодії з клієнтами, оптимізації ланцюгів поставок і скорочення операційних витрат. Наприклад, розумні полиці, оснащені датчиками ваги, можуть збирати інформацію на основі RFID і надсилати дані на платформу IoT для автоматичного моніторингу запасів і ініціювання сповіщень, якщо товари закінчуються. Спеціальні сповіщення в соціальних мережах можуть надавати цільові пропозиції та рекламні акції клієнтам, що підвищить ефективність постачання найпопулярніших товарів. Також сюди можна віднести безконтактну оплату та спеціальні додатки для здійснення покупок через інтернет.

У державному секторі IoT може використовуватись для розумного управління містами та урядування з метою кращого виявлення та попередження вирішення громадських проблем. Наприклад, державні комунальні підприємства можуть використовувати додатки на основі Інтернету речей, щоб сповіщати своїх користувачів про перебої з водопостачанням, електроенергією чи каналізацією. Програми IoT можуть збирати дані про масштаби збоїв і розгортати ресурси, щоб допомогти комунальним службам швидше відновлюватися після збоїв. До IoT-технологій міста відносяться розумне паркування, карти шуму, забруднення повітря, розумне освітлення та трафік на дорогах. Сьогодні більшість із цієї сукупності пристроїв знаходиться на стадії планування та розробки, але вони в перспективі мають широкий діапазон їх використання. За допомогою IoT-технологій можна збільшити безпеку на міських дорогах, краще контролювати рух міського транспорту та контролювати забруднення великих індустріальних населених пунктів.

Завдяки IoT лікарі можуть допомагати людям через Інтернет. Медичні дрони готові забезпечити хворого потрібними ліками. IoT завдяки відкриттям в генетиці дозволяє знайти підхід до кожного пацієнта окремо, проаналізувати стан його здоров'я та розробити індивідуальну схему лікування. Медичне обладнання лікарень можна відстежувати таким чином, щоб забезпечити його ефективне використання. Оснащені датчиками інвалідні візки можна відстежувати за допомогою програми моніторингу ресурсів IoT, щоб швидко знайти найближчий доступний інвалідний візок.

Серед IoT-пристроїв у аграрній сфері можна виокремити дрони та різноманітні пристрої для перевірки складу ґрунту, стану здоров'я домашніх тварин, відстеження їх місцезнаходження, прогнозу кліматичних змін.

Використання IoT-пристроїв в будинку дозволяє зробити життя людини більш комфортним. Зокрема, це розумні термостати, кондиціонери, пилососи, колонки, навіть годівниці для тварин та багато інших повсякденних пристроїв, які виконують звичайні домашні функції.

Окрім переваг, які можна отримати від використання технологій Інтернету речей, є певні загрози і ризики. З огляду на те, що через пристрої IoT та IIoT проходить так багато важливих для бізнесу даних, організації повинні вжити заходів для захисту своїх технологій. При цьому ризики потрібно розглядати не окремо і ізольовано для напрямку IoT, а як загальну загрозу і ризики всього бізнесу. При використанні IoT загрози в першу чергу пов'язані із питаннями безпеки і конфіденційності даних. Пристрої, які погано захищені, можуть стати уразливими і доступними для шахраїв. Крім того пристрої тісно пов'язані між собою і створюють мережу, в якій використовуються вбудовані системи, такі як процесори, датчики та комунікаційне обладнання, для збору, надсилання та обробки даних, котрі вони отримують із свого середовища. Таким чином, уразливість одного пристрою зробить можливим для хакера дістатись до всіх даних. Порушення конфіденційності також є серйозною проблемою використання технологій IoT. Компанії, які професійно займаються просуванням на ринок цієї інтелектуальної технології, можуть мати доступ до особистих даних користувачів. Несумлінні постачальники технологій можуть використовувати цю інформацію для продажу особистих даних або маніпулювання користувачами. Не менш важливим ризиком може стати використання Інтернету речей для критичної інфраструктури. При використанні IoT в управлінні електроенергією, транспортною інфраструктурою, фінансовими послугами, соціальними медіа відбувається генерація величезної кількості даних, які тісно пов'язані між собою і із існуючими системами управління. Тут має бути розроблена політика безпеки і шифрування з метою забезпечення захисту даних і активів.

Література:

1.Парамонов В. Інтернет речей. «Розумна» електроніка URL: <https://www.turkaramamotoru.com/uk/Інтернетречей-20010.html> (дата звернення: 17.10.2022).

2.Definition Internet-of-Things-IoT. URL: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>. (the date of access: 17.10.2022).

3.Industrial Internet of Things, IIoT. URL: <https://www.it.ua/knowledge-base/technology-innovation/promyshlennyj-internet-veschej> (the date of access: 17.10.2022).