УДК 621.391 DOI: 10.31673/2786-8362.2025.019950

Галаган Н.В., к.т.н.; **Гладка М.В.,** к.т.н.;
Борисенко І.І., к.т.н.; **Блаженний Н.В.,** PhD

ДОСЛІДЖЕННЯ ПРОБЛЕМ ФУНКЦІОНУВАННЯ ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖ З ЗАСТОСУВАННЯМ ІНТЕРНЕТУ РЕЧЕЙ

Halahan N.V., Gladka M.V., Borysenko I.I., Blazhennyi N.V. Research into the problems of functioning of intelligent networks using the Internet of Things. The article is devoted to the consideration of the Internet of Things technology, where it is necessary to first of all evaluate the basic principles, key tasks, as well as the most modern approaches and solutions.

The article proves that the Internet of Things is associated with a physical action or event. It forms a response to a real-world factor. At the same time, a single sensor can generate a huge amount of data, for example, an acoustic sensor for preventive equipment inspection. In other cases, a single bit of data is enough to convey important information about the state of the system. Sensor systems have evolved and, in accordance with Moore's law, have shrunk to sub-nanometer sizes and become significantly cheaper. This is what predicts that many devices will be connected to the Internet of Things, and this is why these predictions will come true.

Therefore, when considering the Internet of Things, it is necessary to consider microelectromechanical systems, sensors and other types of low-cost edge devices and their electrophysical properties. This also applies to the power systems needed to power the edge devices.

Keywords: sensors, differentiated privacy, Internet of Things, information system, privacy protection

Галаган Н.В., Гладка М.В., Борисенко І.І., Блаженний Н.В. Дослідження проблем функціонування інтелектуальних мереж з застосуванням інтернету речей. Стаття присвячена розгляду технології Інтернет речей, де потрібно насамперед оцінити базові принципи, ключові завдання, а також найсучасніші підходи та рішення.

В статті доведено, що Інтернет речей пов'язаний з фізичною дією або подією. Він формує реакцію на фактор реального світу. При цьому один-єдиний датчик може згенерувати величезний обсяг даних, наприклад, акустичний датчик для профілактичного огляду обладнання. В інших випадках одного біта даних достатньо, щоб передати важливі відомості про стан системи. Системи датчиків еволюціонували і, відповідно до закону Мура, зменшилися до субнанометрових розмірів і стали істотно дешевше. Саме це прогнозує, що до Інтернету речей будуть підключені безліч пристроїв, і саме тому ці прогнози виправдаються.

Тому, розглядаючи Інтернет речей, необхідно розглядати мікроелектромеханічні системи, датчики і інші типи недорогих граничних пристроїв і їх електрофізичні властивості. Це стосується і енергетичних систем, необхідних для живлення граничних пристроїв.

Ключові слова: датчики, диференційована конфіденційність, Інтернет речей, інформаційна система, захист конфіденційності

Вступ

З розвитком комунікаційних технологій та Інтернету взаємодія між суб’єктами спілкування поступово перейшло в кібернетичний простір віртуального світу. Проте взаємодія між суб’єктами в реальному світі не може бути повною мірою реалізована, що призводить до використання послуг в уявному просторі.

Сучасна технологія Інтернет речей використовується як платформа, яка покликана інтегрувати уявний простір до реального світу.

Аналіз останніх досліджень. Інтернет речей, як надсучасна складна система складається з великої кількості недорогих датчиків і бездротового зв'язку комунікацій з використанням технологій сенсорних мереж. Робота підприємств, надання медичних послуг, спілкування, придбання товарів відбувається у віртуальному просторі за допомогою телекомунікаційних мереж [1].

Використання Інтернет-технологій принесло зміни в суспільство, сприяло побудові нових бізнес процесів, засобів безпеки та створило проблеми конфіденційності [2-3] на різних рівнях функціонування комунікаційних мереж. При цьому один-єдиний датчик може згенерувати ве-

личезний обсяг даних, наприклад, акустичний датчик для профілактичного огляду обладнання [4]. В інших випадках одного біта даних достатньо, щоб передати важливі відомості про стан системи. Тому, розглядаючи Інтернет речей, необхідно розглядати мікроелектромеханічні системи, датчики і інші типи недорогих граничних пристроїв і їх електрофізичні властивості [5]. Це стосується і енергетичних систем, необхідних для живлення граничних пристроїв. Високі швидкості протікання технологічних процесів висувають вимоги до швидкодії технічних засобів [6].

Постановка завдання. Актуальним науковим завданням є визначення та дослідження проблем функціонування сучасних інтелектуальних мереж з застосуванням Інтернету речей (IoT).

Інтернет речей пов'язаний з фізичною дією або подією. Він формує реакцію на фактор реального світу. Системи датчиків еволюціонували і, відповідно до закону Мура, зменшилися до субнанометрових розмірів і стали істотно дешевше. Саме це прогнозує, що до Інтернету речей будуть підключені безліч пристроїв, і саме тому ці прогнози виправдаються.

Метою роботи є дослідження проблем функціонування інтелектуальних мереж з застосуванням Інтернету речей. Інтернет речей представляє собою концепцію мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами. Це відбувається за допомогою використання стандартних протоколів зв'язку. Крім датчиків, в мережах можуть використовуватись виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через бездротові або дротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів. При цьому набуває поширення всеосяжний або всеохоплюючий Інтернет, що спричиняє занепокоєння стосовно конфіденційності інформації.

Рух в майбутнє, яке сформоване даними, цифровою трансформацією та швидким розвитком штучного інтелекту потребує захисту конфіденційності і тому займає центральне місце в сфері безпеки.

При цьому заходи конфіденційності, які колись вважалися недоцільними, мають стати невід’ємною частиною будь-якого збору даних.

Виклад основного матеріалу дослідження

Значне розширення складу програмно-реалізованих або програмно-підтримуючих функцій в інформаційних системах, системах управляння та Інтернеті речей залежало від розвитку елементної бази та обумовлено виникненням доступних для використання програмованих мікропроцесорних контролерів та застосуванням технологій віртуалізації.

При цьому паралельно з удосконаленням основної (центральної) частини системи все більшу роль в забезпеченні швидкодії грають динамічні властивості периферійного обладнання – у першу чергу датчиків, які використовуються в системах Інтернету речей. Ці датчики мають свої особливості та певні динамічні характеристики (рис.1, 2).

Динамічні характеристики дозволяють оцінювати зміни вихідного сигналу датчика під час переходу від одного сталого режиму до іншого.

За допомогою повних динамічних характеристик можна проводити таку оцінку при будь-якому заданому законі зміни вхідної величини датчика. Як правило динамічну характеристику датчика визначають експериментально, змінюючи певним чином вхідний параметр і контролюють відповідні зміни вихідного сигналу. При цьому найбільш зручним (а для деяких датчиків єдино можливим) є одинична поетапна зміна вхідного параметра [7].

Відповідна йому зміна вихідного сигналу визначає перехідну характеристику датчика (рис. 2), з якої відомими методами можуть бути отримані, при необхідності, інші повні динамічні характеристики.

При цьому характеристики датчиків описуються наступними величинами:

P – вхідна величина;

$P_{\min}, P_{\max}$ – номінальні граничні значення вхідної величини (нижня і верхня, відповідно);

$\Delta(P_{\max})$ – значення основної похибки при верхньому граничному значенні вхідної величини;

I – вихідний сигнал датчика;

$I_{\min}, I_{\max}$ – номінальні граничні значення інформативного параметра (початкове і максимальне, відповідно);

$I_{вик}$ – максимальне значення інформативного параметра (викид);

$I_{\gamma\%}$ – заданий рівень інформативного параметра (у відсотках від $I_{\max}$);

ε – ширина заданої зони допустимої похибки в усталеному стані;

t – поточний час;

t_0 – початковий момент часу;

$t_{зап}$ – час «чистого» запізнювання;

$t_{вик}$ – час викиду;

$t_{\gamma\%}$ – процентний показник часу;

$t_{\text{уст}}$ – час установлення.

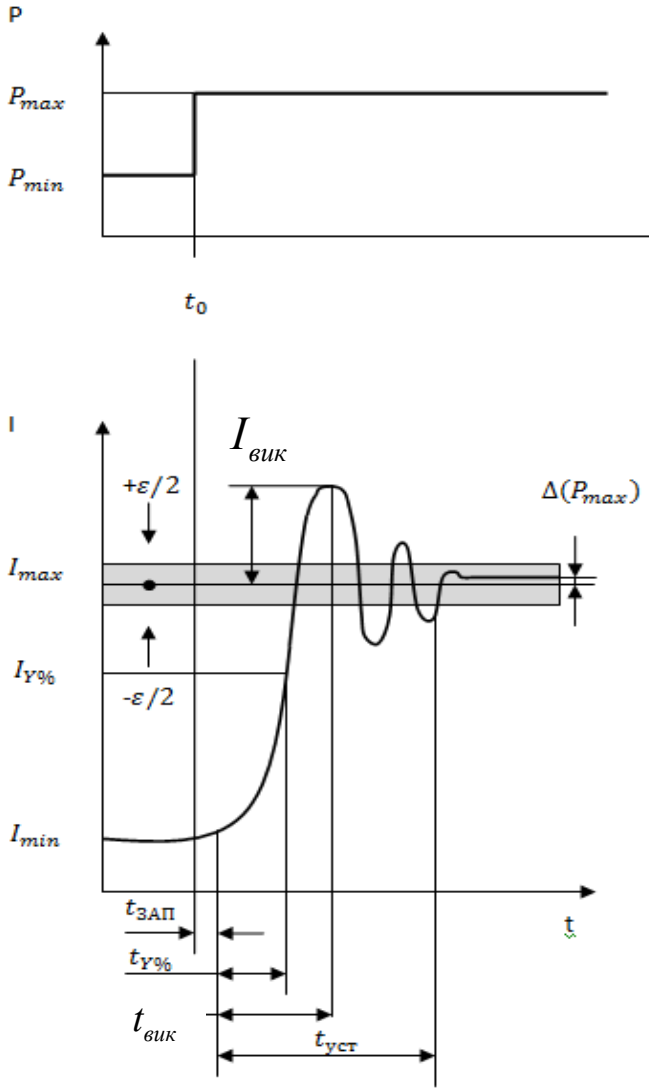

Рис. 1. Графіки, які демонструють зміну характеристик в датчиках з коливальним характером перехідних процесів

Для практичного застосування замість повної динамічної характеристики датчика використовують сукупність характеристик, що характеризують його параметри, та проводять кількісну оцінку.

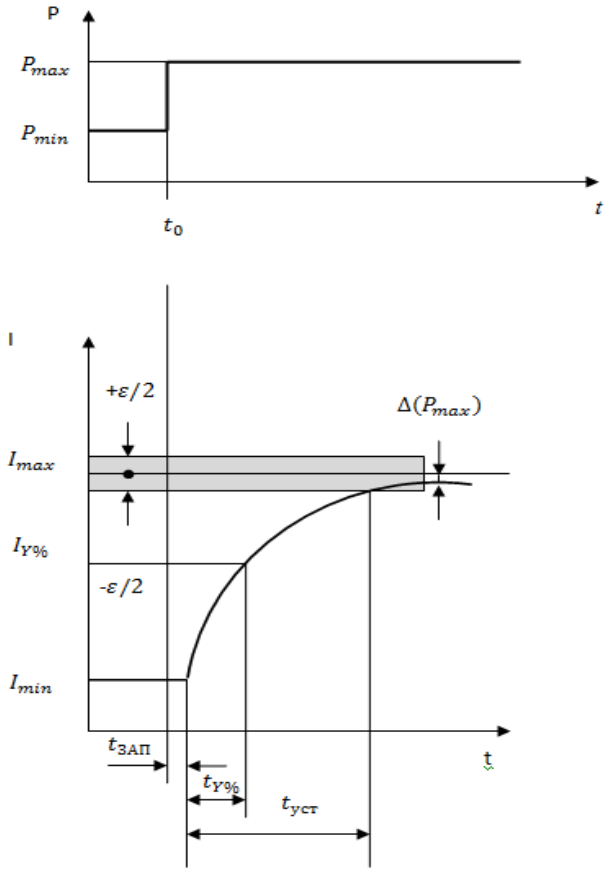

Рис. 2. Графіки, які демонструють зміну характеристик в датчиках з аперіодичним характером перехідних процесів

Такі характеристики розглядають як приватні динамічні характеристики. Наприклад, на рис. 1 показані приватні динамічні характеристики, що визначаються по перехідній характеристиці датчика, при цьому:

час чистого запізнювання $t_{зап}$ – інтервал між моментом стрибкоподібної зміни вхідної величини і початком викликаний їм зміни інформативного параметра вихідного сигналу;

час встановлення $t_{уст}$ – інтервал між початком зміни інформативного параметра сигналу і моментом, починаючи з якого інформативний параметр входить і залишається в деякому діапазоні ($\pm\varepsilon\%$) близько до сталого значення;

процентний показник часу $t_{\gamma\%}$ – інтервал між початком зміни інформативного параметра сигналу і моментом, коли цей параметр досягає $\gamma\%$ від сталого значення.

Зокрема, для датчиків з аперіодичним характером перехідних процесів процентний показник часу при γ = 63 % від I_{max} можна інтерпретувати як постійну часу;

час наростання - інтервал між початком зміни вихідного сигналу і моментом, коли цей сигнал наблизиться в перший раз до свого сталого значення. Час наростання можна визначити, наприклад, як процентний показник часу при γ = 90 % від I_{max}.

По перехідній характеристиці датчиків з коливальним характером перехідних процесів можуть бути визначені й інші приватні динамічні характеристики : перехідний викид $I_{вик}$, час викиду $t_{вик}$, коефіцієнт коливань, коефіцієнт загасання.

Динамічні похибки датчика визначаються як відхилення дійсної (оціненої) повної динамічної характеристики від номінальної (призначеної для всіх виробів даного виду).

Динамічні характеристики повинні враховуватися при оцінці результатів перетворення змін за розміром вхідної величини в вихідний сигнал датчика. Як правило, для цього досить використовувати номінальні, а не дійсні динамічні характеристики (при цьому не приймають до уваги динамічні похибки датчика).

Для наочності розглянемо діаграму причинно-наслідкових зв'язків – графічне зображення причино-наслідкових зв'язків між елементами, складовими модельованої системи.

Вважатимемо, що причинно-наслідковий зв'язок відображає відношення між окремими елементами системи як між причиною і наслідком. Даний зв'язок позначатимемо стрілкою, направленою від причини до слідства.

Зв'язок може бути позитивним (коли зміну причини викликає аналогічна зміна слідства) і негативним (зміну причини викликає протилежна зміна слідства). Полярність зв'язку позначається знаком «+» або «–». Два послідовно сполучені негативні зв'язки утворюють у результаті позитивний зв'язок, тобто $A \to -B \to -\mathrm{C}$ аналогічно (у сенсі зв'язку між *A* і *C*) $A \to +C$, а зв'язок $A \to +B \to -C$ аналогічно $A \to -C$.

Причинно-наслідкові зв'язки можуть утворювати замкнуті однонаправлені контури – контури позитивного або негативного зворотного зв'язку, як показано на рис. 3.

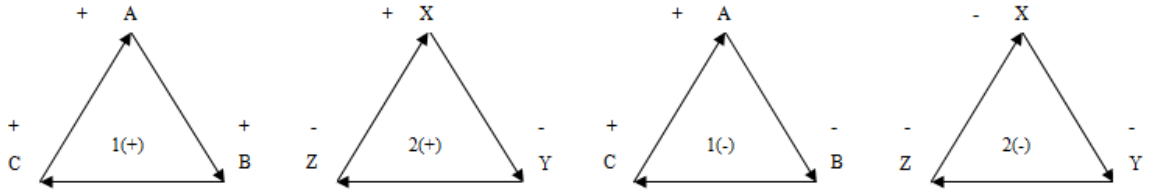

Рис. 3. Графічні зображення, що пояснюють причинно-наслідкові зв'язки модельованої системи

Збільшення *X* викликає зменшення *Y*. Це, у свою чергу, викликає збільшення *Z*, оскільки зв'язок *YZ* негативний, а зростання *2* викликає подальше збільшення *X*. Полярність контура позначена знаком « + » у дужках усередині контура. Приклади контурів негативного зворотного зв'язку наведені на рис. 3.

У контурі *1* збільшення *A* викликає зменшення *B*. Зменшення *Y* викликає зменшення *3*, оскільки вони зв'язані позитивним зв'язком, при якому зміна (зменшення) в причині *(B)* викликає аналогічну зміну (зменшення) в слідстві *(C)*. Аналогічне зменшення *3* викликає зменшення *A*, тобто реакція контура направлена на те, щоб компенсувати початкове збільшення A. Подібним же чином прослідкується поведінка другого контура.

Можна запропонувати наступне правило визначення полярності контурів зворотного зв'язку. Якщо в контур входить парне число негативних причинно-наслідкових зв'язків або їх взагалі немає в нім, то це контур позитивного зворотного зв'язку; якщо в контур входить непарне число негативних причинно-наслідкових зв'язків, то це контур негативного зворотного зв'язку. При цьому полярність причинно-наслідкового зв'язку між двома елементами контура визначається реакцією елемента–наслідку на зміну елемента–причини, незалежно від їх зв'язків з іншими елементами.

На основі діаграми причинно-наслідкових зв'язків модельованої системи будується діаграма потоків і рівнів – графічне зображення динамічної моделі у вигляді рівнів і потоків, що зв'язують їх.

Для управління безпекою та надійним захистом інтелектуальних мереж з застосуванням IoT, які стають все більш вразливими, застосовують метод стохастичного інформаційного аналізу. Це розширює традиційні моделі , які фокусуються на окремих відмовах компонентів або ланцюжках безпосередньо пов'язаних між собою відмов, до більш складних процесів і небезпечних взаємодій між компонентами системи. Інформаційний підхід до аналізу безпеки та надійності складних систем принципово відрізняється від звично логіко-ймовірнісного підходу та методу станів.

Стохастичний інформаційний аналіз надійності систем дає змогу здійснити перехід від класичних методів аналізу систем без надлишку до імовірнісного аналізу надійності та безпеки інтелектуальних мереж із застосуванням IoT як складних систем.

Завдання інформаційного аналізу полягає в побудові такої моделі системи, у якій враховується інформаційний зв'язок її частин (підсистем). Спрямований із входу на вихід і з виходу на вхід системи ланцюжок залежностей інформаційних змінних дає змогу трактувати цей ланцюжок як передачу інформації із входу на вихід і з виходу на вхід (рис. 4).

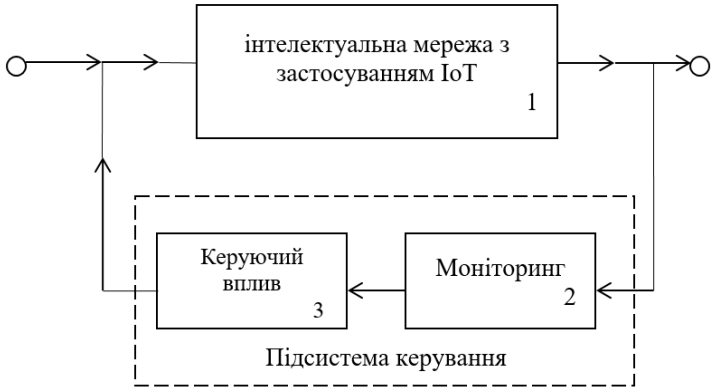

Рис. 4. Контур управління безпекою

Процеси управління здебільшого відбуваються на межі двох рівнів ієрархії, і завжди пов'язані з накладанням обмежень. Метод стохастичного інформаційного аналізу використовує концепцію накладання обмежень на поведінку системи, щоб уникнути небезпечних подій або умов, а не зосереджуватися на уникнення відмов окремих компонентів [8-9].

Між ієрархічними рівнями кожної структури контролю безпеки необхідні ефективні канали зв'язку, потрібні ефективні канали комунікації під час процесів контролю. Контур керування представляє собою замкнуту систему, що складається з об'єкта та його підсистеми керування. Підсистема управління може складатися з моніторингу (підсистеми контролю або діагностики) та органу управління, який впливає на об'єкт.

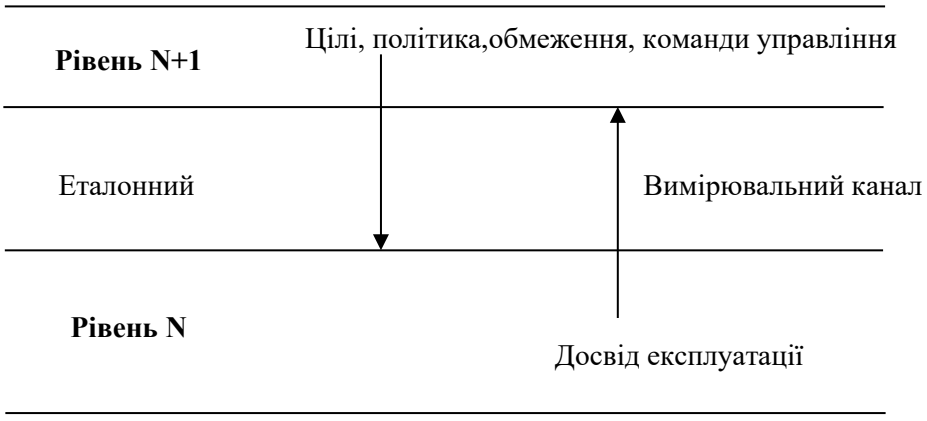

Рис. 5. Канали зв’язку між рівнями управління

На основі структурної схеми системи, вихідного потоку інформації та інформаційних змінних підсистем визначаються потоки інформації підсистем. Відповідно до цього, підсистеми вважаються з'єднаними паралельно, якщо загальний потік інформації з'єднання підсистем дорівнює сумі потоків, які проходять через кожну підсистему, і відмова однієї підсистеми призводить лише до часткової втрати загального вихідного потоку інформації,

який проходить через відмовлену підсистему. Якщо вихідний потік інформації однієї підсистеми є вхідним потоком інформації іншої, то ці підсистеми з'єднані послідовно.

Найважливішою умовою для підвищення надійності та безпеки є наявність моделі системи. Наявність моделі визначає, що будь-який контролер, незалежно від того, чи він суб'єкт, чи об'єкт автоматизації, потребує моделі процесу контролю, щоб ефективно ним керувати. Мета використання моделі процесу контролю є визначення того, які керуючі дії необхідні на основі знання поточного стану керованого процесу, а також оцінити вплив різних керуючих дій на цей стан.

Крім того відкрита проблема полягає в тому, як ще більше збільшити кількість підтримуваних пристроїв IoT, об'єднавши користувача стільникового зв'язку з декількома пристроями та реалізувавши одночасну передачу даних [8]. Хоча існує низка досліджень зв'язку зворотного розсіювання навколишнього середовища, результати цих досліджень не враховують спільний дизайн між передачею/виявленням даних зв'язку та Інтернету речей [8]. Це робить результати в існуючих системах неоптимальними з точки зору продуктивності передачі даних IoT (наприклад, пропускна здатність і кількість підтримуваних пристроїв IoT. Тому потрібні додаткові дослідження, щоб підвищити продуктивність в майбутньому.

Багато комерційних компаній займаються розробкою супутників для майбутнього IoT, наприклад, Iridium, GlobalStar та ORBCOMM. Таким чином, зв'язок IoT за допомогою супутника буде доступним.

Для передачі даних від пристроїв IoT до базових мереж супутники на великій висоті спочатку збирають дані з пристроїв IoT, а потім передають дані на супутникову антену, яка знаходиться на землі та підключена до базових мереж через дротове або бездротове з'єднання.

Однією з типових топологій для передачі даних між пристроями IoT і супутниками є прямий режим. У цьому режимі пристрої IoT безпосередньо передають дані на супутники. Основною особливістю прямого режиму є те, що оскільки відстань від пристроїв IoT до супутників велика, то потужність передачі пристроїв IoT повинна бути високою.

Зокрема, позначені дані можуть надходити або з ручних проектів, або з комп'ютерного моделювання залежно від практичних ситуацій.

Висновки

У статті досліджено проблеми функціонування інтелектуальних мереж з застосуванням Інтернету речей. Інтернет речей представляє собою концепцію мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами. Це відбувається за допомогою використання стандартних протоколів зв'язку. Крім датчиків, в мережах можуть використовуватись виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через бездротові або дротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів. При цьому набуває поширення всеосяжний або всеохоплюючий Інтернет, що спричиняє занепокоєння стосовно конфіденційності інформації.

Для розгляду технології Інтернет речей потрібно насамперед оцінити базові принципи, ключові завдання, а також найсучасніші підходи та рішення. Інтернет речей пов'язаний з фізичною дією або подією. Він формує реакцію на фактор реального світу. При цьому один-єдиний датчик може згенерувати величезний обсяг даних, наприклад, акустичний датчик для профілактичного огляду обладнання. В інших випадках одного біта даних достатньо, щоб передати важливі відомості про стан системи. Системи датчиків еволюціонували і, відповідно до закону Мура, зменшилися до субнанометрових розмірів і стали істотно дешевше. Саме це прогнозує, що до Інтернету речей будуть підключені безліч пристроїв, і саме тому ці прогнози виправдаються.

Тому, розглядаючи Інтернет речей, необхідно розглядати мікроелектромеханічні системи, датчики і інші типи недорогих граничних пристроїв і їх електрофізичні властивості. Це стосується і енергетичних систем, необхідних для живлення граничних пристроїв.

При цьому подальшим напрямком досліджень може бути диференціальна конфіденційність, що представляє собою технологію підвищеної конфіденційності, яка дозволяє дослідникам шляхом обробки даних отримувати інформацію з дуже конфіденційних даних без завдання шкоди для загальної конфіденційності. Механізм диференціальної конфіденційності ґрунтується на математичних гарантіях, які захищають індивідуальну інформацію, водночас дозволяючи проводити цінний аналіз з баз даних, не розголошуючи особисту інформацію.

Список використаної літератури:

1. В. Б. Толубко, Л. Н. Беркман, Л. П. Крючкова, А. Ю. Ткачов. Підвищення показників якості системи управління послугами мережами майбутнього / В // Наукові записки Українського науково-дослідного інституту зв'язку. - 2018. - № 3. - С. 5-11.

2. Ambient Backscatter Communications: A Contemporary Survey / N. Van Huynh et al. IEEE Communications Surveys & Tutorials. 2018. Vol. 20, no. 4. P. 2889–2922. URL: https://doi.org/10.1109/comst.2018.2841964.

3. Mao Q., Hu F., Hao Q. Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. 2018. Vol. 20, no. 4. P. 2595–2621. URL: https://doi.org/10.1109/comst.2018.2846401.

4. G. Vougioukas and A. Bletsas, “Switching frequency techniques for universal ambient backscatter networking,” IEEE J. Select. Areas Commun., vol. 37, no. 2, pp. 464-477, Feb. 2019.

5. Zhang C., Patras P., Haddadi H. Deep Learning in Mobile and Wireless Networking: A Survey. IEEE Communications Surveys & Tutorials. 2019. Vol. 21, no. 3. P. 2224–2287. URL: https://doi.org/10.1109/comst.2019.2904897.

6. Modulation in the Air: Backscatter Communication Over Ambient OFDM Carrier / G. Yang et al. IEEE Transactions on Communications. 2018. Vol. 66, no. 3. P. 1219–1233. URL: https://doi.org/10.1109/tcomm.2017.2772261.

7. Yang G., Zhang Q., Liang Y.-C. Cooperative Ambient Backscatter Communications for Green Internet-of-Things. IEEE Internet of Things Journal. 2018. Vol. 5, no. 2. P. 1116–1130. URL: https://doi.org/10.1109/jiot.2018.2799848.

8. Hua S., Wang Q., Xu X. Application of machine learning in wireless communication. Theoretical and Natural Science. 2023. Vol. 12, no. 1. P. 130–135. URL: https://doi.org/10.54254/2753-8818/12/20230452.

9. X. Zhou, M. Sun, G. Y. Li, and B.-H. F. Juang, “Intelligent wireless communications enabled by cognitive radio and machine learning,” China Commun., vol. 15, no. 12, pp. 16-48, Dec. 2018.

Автори статті

Галаган Наталія – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0001-8582-3126

Гладка Мирослава – кандидат технічних наук, доцент, Київський національний університет імені Тараса Шевченка, Київ, Україна.

ORCID: 0000-0001-5233-2021

Борисенко Ірина – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0001-8645-3881

Блаженний Назарій – PhD, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-3826-7400

Authors of the article

Halahan Nataliia – Candidate of Sciences (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0001-8582-3126

Gladka Myroslava – Candidate of Sciences (technical), Associate Professor, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
ORCID: 0000-0001-5233-2021
Borysenko Iryna – Candidate of Sciences (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0009-0001-8645-3881
Blazhennyi Nazariy – PhD (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0000-0002-3826-7400