DataProEU

Національний університет Львівська політехніка

Co-funded by the
Erasmus+ Programme
of the European Union

Анастасія Дорошенко

Промисловий Інтернет речей та захист персональних даних

Навчальний посібник

Промисловий інтернет речей та захист персональних даних: навчальний посібник для магістрів за спеціальністю «Комп'ютерні науки» / Анастасія Дорошенко. – Національний університет «Львівська політехніка». – Львів, 2023.

Розглянуто архітектуру та принципи побудови систем Інтернету речей, описано сфери та приклади їх використання. Висвітлено актуальні проблеми захисту персональних даних в IoT із дотриманням вимог Загального регламенту захисту персональних даних ЄС (Regulation (EU) 2016/679 General Data Protection Regulation, GDPR).

Навчальний посібник написано в межах виконання проекту Жан Моне Кафедра «Захист персональних даних в ЄС» в Національному університеті «Львівська політехніка» (*101085612 — DataProEU — ERASMUS-JMO-2022-HEI-TCH-RSCH* «Data Protection in the EU».

Зміст

Вступ

Інтернет речей швидко змінив XXI століття, покращивши процеси прийняття рішень і запровадивши інноваційні споживчі послуги, такі як моделі оплати за користування. Інтеграція інтелектуальних пристроїв і технологій автоматизації революціонізували всі аспекти нашого життя – від медичних послуг до обробної промисловості, від сільського господарства до видобутку корисних копалин. Однак окрім позитивних аспектів, важливо також визнати серйозні проблеми безпеки, надійності та довіри до цього технологічного середовища.

Цей посібник буде корисним для ознайомлення із доменом Інтернету речей (Internet of Things, IoT), забезпечуючи основу для майбутнього глибокого вивчення. Зокрема, розглянемо історію виникнення Інтернету речей та його історичну еволюцію, ключові характеристики, переваги, архітектури, систематизуємо технології та існуючі програми в основних доменах IoT. Розглянемо поширені проблеми та виклики при розробці та розгортанні додатків IoT щодо загрози безпеці на різних архітектурних рівнях, етичні міркування, проблеми конфіденційності користувачів і проблеми, пов'язані з довірою. Це обговорення дасть чітке розуміння різноманітних аспектів Інтернету речей, забезпечуючи повне розуміння технології Інтернету речей, а також уявлення про великий потенціал і вплив цієї трансформаційної сфери.

Поява Інтернету суттєво вплинула на формування та розвиток існуючого цифрового світу та призвела, зокрема, до початку ери IoT. Інноваційний винахід останніх десятиліть – IoT – революціонізує взаємодію між фізичною та цифровою сферами [1]. У цьому взаємопов'язаному ландшафті цифровий світ взаємодіє з фізичним через низку датчиків і приводів. Якщо розглядати Інтернет речей як парадигму, то її можна характеризувати як комбінацію обчислень та мережі, що бездоганно інтегруються практично в будь-який об'єкт, надаючи можливості для віддаленого запиту та модифікації.

У широкому сенсі термін «Інтернет речей» описує трансформаційну сферу, де майже будь-який побутовий пристрій підключено до мережі, що дозволяє спільно використовувати для інтелектуальних і автоматизованих завдань. Концепцію IoT вперше представив Пітер Т. Льюїс у 1985 році [2], визначивши її як злиття людей, процесів і технологій із взаємопов'язаними пристроями та датчиками. Це полегшує віддалений моніторинг, оцінку стану, маніпуляції та аналіз трендів цих пристроїв [3]. Розвиток Інтернету речей ще далекий від завершення, але обіцяє майбутнє, де різноманітні пристрої безперебійно підключатимуться до Інтернету, змінюючи людське існування безпрецедентним чином. IoT – це мережа взаємопов'язаних пристроїв із датчиками, виконавчими механізмами, процесорами та різними комунікаційними технологіями. Датчики збирають дані в реальному часі як про

внутрішній стан, так і про зовнішнє оточення, починаючи від мобільних телефонів і закінчуючи мікрохвильовими печами. Актуатори, своєю чергою, реагують на дані або команди, забезпечуючи автоматизацію та дистанційне керування фізичними пристроями. Дані, зібрані датчиками, обробляються або на межі мережі, або на центральних серверах, при цьому деяка попередня обробка відбувається безпосередньо в датчиках або кінцевих пристроях. Потім оброблені дані передаються на віддалені сервери для подальшого аналізу, зберігання та обробки. Ці дані формують основу для аналізу, прийняття рішень і подальших дій, які можуть бути фізичними (наприклад, налаштування розумного термостата) або віртуальними (наприклад, надсилання сповіщень) [4]. Можливості застосування IoT є широкими та різноманітними, такими, що впливають на різні аспекти нашого життя. Від особистої зручності в розумних будинках до інновацій у галузі охорони здоров'я та фітнесу, IoT має потенціал для впливу на особисті, фінансові, фізичні, освітні, професійні та розумові аспекти життя людей. У розумних будинках IoT дає змогу дистанційно керувати електроприладами, освітленням, варити каву, регулювати термостат і навіть працювати без використання рук за допомогою голосових команд [5]. У сфері охорони здоров'я портативні пристрої IoT пропонують віддалений моніторинг, що дозволяє опікунам і медичним працівникам надавати своєчасну допомогу в надзвичайних ситуаціях. Крім того, люди можуть використовувати переносні пристрої для відстеження режиму сну, фізичної активності та загальної фізичної форми [6]. Це окремі приклади в широкій сфері застосування IoT, що підтверджують значні можливості та виклики, які дослідники досліджуватимуть у майбутньому.

Однією з найпоширеніших областей застосування інтернету речей є виробничі середовища для яких використовується термін "промисловий Інтернет речей" (IIoT, Industrial IoT). Термін IIoT часто розглядають як синонім Індустрії 4.0, одним з ключових елементів якої він є [7]. Тобто можна сказати, що IIoT веде до Індустрії 4.0, короткий огляд якої ми також наведемо в цьому посібнику. У 2015 році інтернет речей був оголошений однією з найактуальніших технологій. Його промислове застосування, тобто IIoT, було навіть у центрі уваги Всесвітнього економічного форуму 2016 під гаслом "Освоєння четвертої промислової революції" [8]. Однак існує і критичне сприйняття застосування інтернету речей у промисловому виробництві. Багато дослідників стверджують, що очікуване зростання продуктивності в результаті оцифрування є не настільки значним порівняно з попередніми промисловими революціями. У світлі цих критичних голосів ще важливіше проаналізувати, де можна отримати реальну цінність від промислового інтернету речей з погляду часу, гнучкості, надійності, вартості та якості. Тому в цьому посібнику представлені деякі матеріали, присвячені конкретним виробничим додаткам та варіантам їх використання.

1. Історія та перспективи розвитку Інтернету речей

За своєю суттю, IoT грунтується на концепції підключення повсякденних об’єктів і пристроїв до Інтернету, що дає їм змогу спілкуватися, збирати дані та виконувати дії автономно або у відповідь на команди. Ця базова концепція містить три ключові елементи: датчики та виконавчі механізми, які збирають і взаємодіють з даними, мережеву інфраструктуру для передавання даних і хмарні платформи для зберігання, обробки та аналізу даних. Поєднуючи ці елементи, IoT дає нам змогу підвищувати ефективність, отримувати інформацію в режимі реального часу та створювати розумні системи, що швидко реагують, які впливають на різні аспекти нашого життя: від розумних будинків і міст до промисловості та сфери охорони здоров’я. Еволюція IoT, яка розгорталася протягом кількох десятиліть, почалася з концепції розумних об’єктів. З того часу IoT зазнав числених новаторських змін, які вразили світ своїми унікальними і зручними характеристиками. Переваги, які приносить ця технологія, неможливо підрахувати, оскільки вона стосується майже всіх аспектів життя людей, спрощуючи та покращуючи його. У цьому розділі розглянуто фундаментальні концепції IoT, охоплюючи такі теми: історія виникнення, компоненти та характеристики IoT.

1.1. Історичний розвиток IoT

З моменту винаходу першої стаціонарної лінії зв'язку – телеграфу – у 1830-40-х рр., машини відігравали важливу роль у полегшенні прямого зв'язку. Значний поступ у напрямку IoT стався 3 червня 1900 року з першою передачею голосу по радіо, яку часто називають «бездротовою телеграфією». Це відкрило шлях для IoT. Розвиток комп’ютерів, що почався в 1950-ті рр., є ще одним важливим аспектом IoT. У 1962 році Інтернет, фундаментальний компонент IoT, розпочався як проект DARPA1.

Група відомих дослідників ініціювала спроби з’єднати комп’ютери та системи. До 1969 року DARPA перетворилася на ARPANET2, - попередника сучасного Інтернету [9]. Хоча термін «Інтернет речей» є відносно новим, концепція інтеграції комп’ютерів і мереж для моніторингу та керування пристроями має багату історію, що охоплює десятиліття.

Наприкінці 1970-х років різні зацікавлені сторони, включаючи підприємства, уряди та споживачів, почали досліджувати способи підключення персональних комп’ютерів (ПК) та іншого обладнання. Це призвело до практичного використання систем дистанційного моніторингу лічильників електричної мережі через телефонні лінії в ту епоху.

У 1980-ті рр. зростає інтерес до вдосконалення фізичних об’єктів сенсорами та інтелектом. У цей час комерційні постачальники послуг почали підтримувати публічний доступ до ARPANET – раннього попередника сучасного Інтернету. Супутники та стаціонарні телефони відіграли ключову роль у створенні базової комунікаційної інфраструктури для IoT, що розвивається. Концепцію мережі розумних пристроїв було досліджено ще в 1982 році, коли торговий автомат Coca-Cola в Університеті Карнегі-Меллона був модифікований для підключення до ARPANET. Це дозволило місцевим програмістам дистанційно контролювати вміст торгового автомата, гарантуючи наявність і охолодження напоїв перед здійсненням покупки. Однак керувати технологією було складно, і прогрес у цій галузі був обмеженим у той період.

Водночас протягом 1980-х років локальні мережі (LAN) набули популярності та виявилися ефективними для спілкування в реальному часі та обміну документами між групами ПК.

У 1990-ті рр. прогрес у бездротових технологіях заклав основу для широкого впровадження рішень «машина-машина» (M2M) у корпоративному та промисловому контексті, зокрема для моніторингу та експлуатації обладнання. Однак багато з цих перших рішень M2M покладалися на закриті, спеціально створені мережі та приватні або галузеві стандарти, а не використовували мережі на основі Інтернет-протоколу (IP) та стандарти Інтернету [10].

До середини 1990-х років Інтернет розширив своє глобальне охоплення, пропонуючи дослідникам і технологам нові можливості дослідження шляхів покращення зв’язків між людьми та машинами. Важливою віхою на цьому шляху стало створення Джоном Ромкі першого «пристрою» з підключенням до Інтернету — тостера з підтримкою IP, яким можна було керувати через Інтернет. Цей інноваційний тостер був представлений на Інтернет-конференції в 1990 році, ставши першим прикладом IoT в дії.

У 1991 році стаття Марка Вайзера «Комп’ютер 21-го століття» та наукові заходи, такі як UbiComp і PerCom, сформували сучасне бачення IoT [11]. Глобальна система позиціонування (GPS) стала реальністю на початку 1993 року, коли Міністерство оборони створило стабільну систему з 24 супутників [12]. Невдовзі з’явилися приватні комерційні супутники, які розширили функціональність IIoT. На початку 1994 року Реза Раджі представив концепцію IoT в IEEE Spectrum, описавши її як «переміщення невеликих пакетів даних для інтеграції та автоматизації з побутової техніки на цілі заводи». Пізніше того ж року Стів Манн винайшов камеру WearCam, що працює майже в реальному часі, на базі 64-процесорної установки. Між 1993 і 1997 роками компанії пропонували рішення IoT, у тому числі «at Work» від Microsoft і NEST від Novell. Імпульс зріс, коли Білл Джой на Всесвітньому економічному форумі 1999 року представив зв’язок між пристроями у своїй системі «Six Web».

Термін «Інтернет речей» був введений Пітером Т. Льюїсом у промові 1985 року під час 15-го щорічного законодавчого вихідного дня Black Caucus Foundation у

Вашингтоні, округ Колумбія. Льюїс визначив IoT як інтеграцію людей, процесів і технологій із підключеними пристроями та датчиками. для дистанційного моніторингу, оцінки стану, маніпуляції та оцінки трендів, пов'язаних із цими пристроями [13]. У 1997 році Пол Саффо описав датчики та їхні майбутні ролі.

Британський технолог Кевін Ештон – виконавчий директор Auto-ID Center в Массачусетському технологічному інституті – вперше ввів термін «Інтернет речей». Під час роботи в Procter and Gamble він досліджував радіочастотну ідентифікацію (RFID), технологічну структуру, яка дозволяє фізичним пристроям підключатися через мікрочіпи та бездротові сигнали. У тому ж році він розробив глобальну систему ідентифікації предметів на основі RFID [14]. У 1999 році Кевін Ештон був першим, хто описав IoT і запропонував назву «Інтернет речей» під час презентації для Procter and Gamble. Він вважав, що технологія RFID, призначена в основному для відстеження запасів, є важливою передумовою для IoT, що дозволяє комп'ютерам ефективно керувати окремими об'єктами та контролювати їх. Концепція тегування об'єктів була реалізована за допомогою таких технологій, як цифрові водяні знаки, штрих-коди та QR-коди, які використовуються для ідентифікації та відстеження.

Подальший технологічний прогрес, включаючи поширення смартфонів, хмарні обчислення, покращену обчислювальну потужність і вдосконалені алгоритми програмного забезпечення, а також наявність складних датчиків, здатних вимірювати різні параметри, заклали основу для надійного збирання, зберігання та обробки даних для IoT зростання. У 2000 році як значний крок вперед у комерціалізації IoT компанія LG оголосила про плани випустити розумний холодильник, здатний автономно керувати своїм вмістом. Walmart і Міністерство оборони США започаткували відстеження запасів за допомогою RFID та IoT у 2002–2003 рр. RFID набув популярності в програмі Savi армії США в 2003 році, і того ж року Walmart розширив використання RFID по всьому світу. У 2004 році Корнеліус «Піт» Петерсон, генеральний директор NetSilicon, передбачив, що пристрої IoT домінуватимуть в таких сферах інформаційних технологій, як медичні пристрої та промислове керування [15].

У 2005 році в числених статтях таких газета, як The Guardian, Scientific American і The Boston Globe, обговорювали майбутній напрямок IoT. Альянс IPSO був заснований у 2008 році для сприяння використанню IP у мережах «розумних об'єктів», тоді як FCC дозволив використання «білої» мітки в 2008 році. Google ініціював розробку автономних автомобілів у 2009 році, а в 2011 році вийшов на ринок розумний термостат Google Nest, що давав змогу дистанційно керувати опаленням. У червні 2012 року основні інтернет-провайдери та веб-компанії погодилися розширити глобальний адресний простір Інтернету та почали використовувати IPv6 для своїх послуг і продуктів, що стало значним кроком до життєздатного IoT. Це призвело до значного посилення інтересу до цієї галузі. Такі IT-гіганти, як Cisco, IBM і Ericsson пізніше виступили з численними освітніми та комерційними ініціативами, пов'язаними з IoT. Cisco Systems підрахувала, що IoT «народився» між 2008 і 2009 роками, коли співвідношення речей/людей зросло від

0,08 у 2003 році до 1,84 у 2010 році. Зараз у світі налічується близько 21,5 мільярда підключених пристроїв, що майже втричі перевищує кількість людей на планеті (рис. 1.1.) [16].

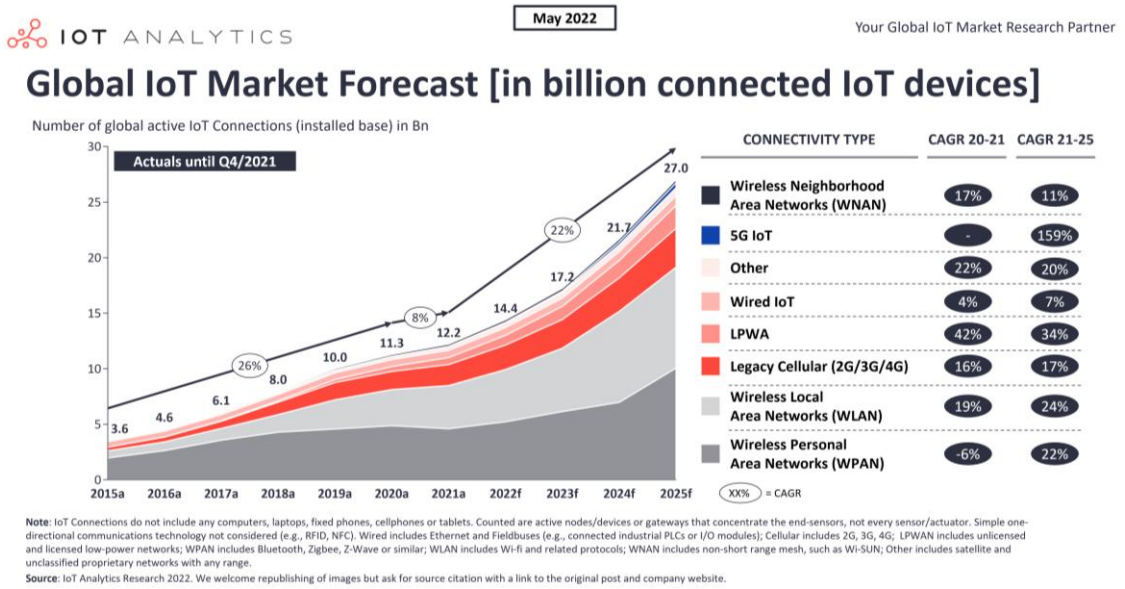

Рис. 1.1. Прогноз кількості підключених IoT пристроїв до 2025 року за версією IoT Analytics (Source: IoT Analytics Research, 2022)

У 2011 році Gartner, дослідницька компанія, яка винайшла знаменитий «цикл ажіотажу для нових технологій», включила «Інтернет речей» до свого списку, в якому вже у 2015 році Інтернет речей був на піку очікувань із прогнозом того, що через 5–10 років технологія перейде на плато ефективності (рис. 1.2.) [17].

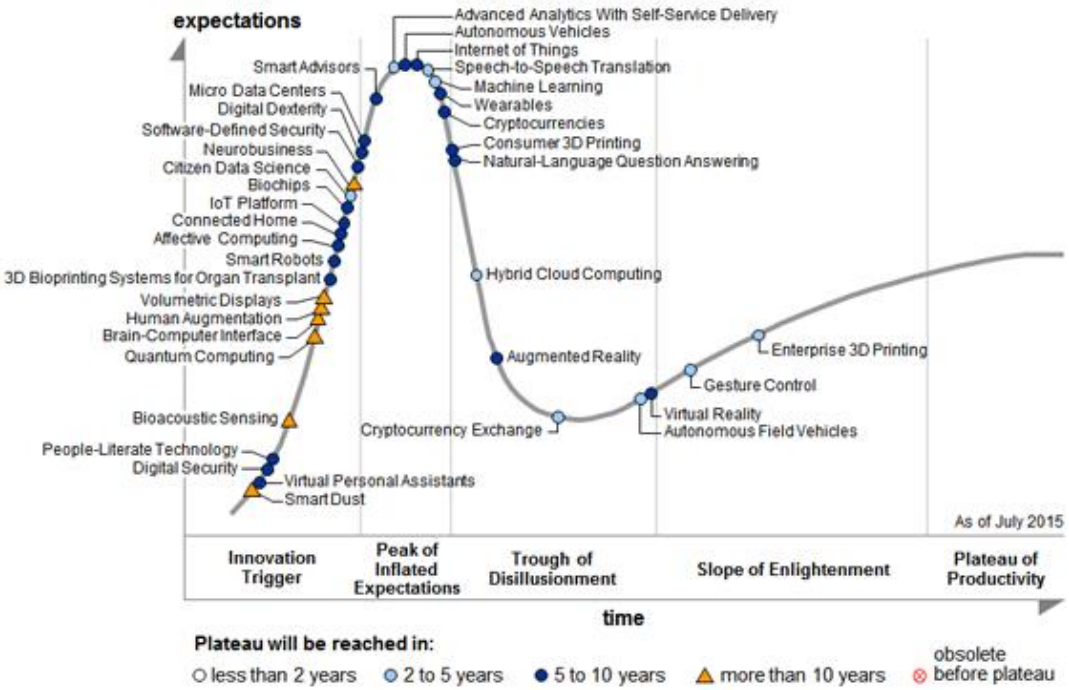

Рис. 1.2. Крива «хайпу» компанії GARTNER для Інтернету речей розглядає зміни уваги до технології у 2015 році [18]

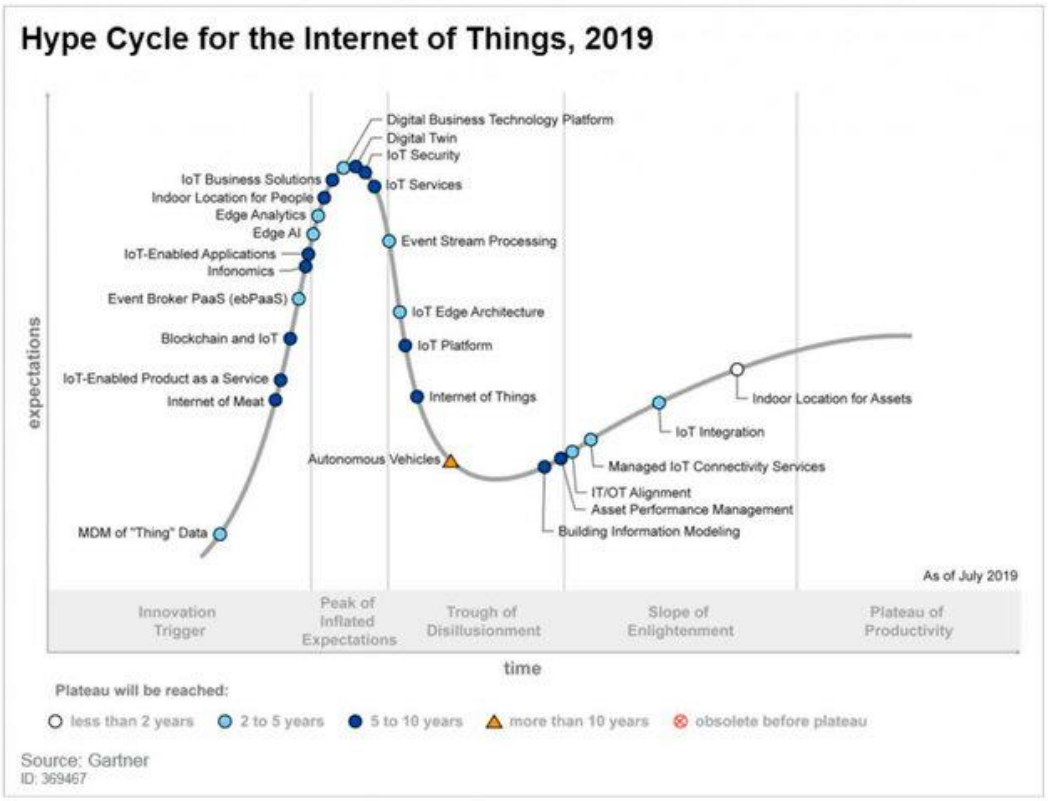

Рис. 1.3. Крива «хайпу» компанії GARTNER для Інтернету речей розглядає зміни уваги до технології у 2019 році [18]

Протягом наступних років цікавість до Інтернету речей збільшувалась, розвивалися такі напрями, як створення IoT платформ та IoT сервісів, виникає розуміння надзвичайної важливості розвитку IoT Security – напряму, який разом з поняттям цифрового двійника очолив криву хайпу Gartner у 2019 році (рис 1.3.). Сьогодні Інтернет речей вже впевнено прямує до досягнення плато ефективності, широко використовується у різних сферах економіки та людського життя.

1.2. Основні характеристики IoT

Розглянемо детальніше основні характеристики Інтернету речей:

1. *Зв'язок*: Підключення є найбільш важливою вимогою IoT. Основним аспектом IoT є мережа з мільйонами пристроїв, підключених один до одного. Зв'язокзалишається постійним, що дозволяє будь-кому з будь-якої точки світу підключитися до мережі IoT у будь-який момент.
2. *Інтелектуальна здатність приймати рішення*: Видобування знань з отриманих даних є дуже важливим. Розглянемо датчик, який виробляє дані; однак, справжня цінність цих даних полягає в їх правильній інтерпретації. Це найважливіший аспект Інтернету речей, в якому пристрої Інтернету речей мають здатність перетворювати необроблені

дані, зібрані датчиками, в значущу інформацію і приймати рішення на її основі.

3. *Динамічність та самоадаптація*: Пристрої Інтернету речей повинні мати можливість адаптуватися до змін контексту, навколишнього середовища та ситуації, що склалася. Наприклад, в системі відеоспостереження камери можуть перемикатися з денного на нічний режим або регулювати роздільну здатність у відповідь на виявлення руху, демонструючи свою адаптивність.

4. *Унікальна ідентичність*: Кожен пристрій Інтернету речей повинен мати унікальну ідентичність та унікальний ідентифікатор. Інтерфейси пристроїв IoT дозволяють користувачам запитувати інформацію про пристрої, відстежувати їхній стан та дистанційно керувати ними. Наявність чіткої ідентичності необхідна для того, щоб користувачі могли захистити свої пристрої за допомогою захисту паролем або альтернативних заходів безпеки.

5. *Самоконфігурація*: Пристрої Інтернету речей здатні самостійно оновлювати свої системи відповідно до ситуації, усуваючи необхідність втручання користувача. Крім того, вони демонструють гнучкість в управлінні мережею, дозволяючи новим пристроям безперешкодно приєднуватися до мережі і дозволяючи будь- якому пристрою вийти з мережі в будь-який час.

Рис. 1.4. Характеристики IoT

6. *Масштабованість* : мережа IoT переживає постійне зростання кількості підключених пристроїв, що призводить до значного і безперервного генерування даних. Відповідно, масштабованість стає головною особливістю будь-якої системи IoT.

7. *Інтероперабельність*: Пристрої Інтернету речей покладаються на стандартизовані протоколи і технології для забезпечення безперебійного зв'язку між собою та з іншими системами. Інтероперабельність є фундаментальним блоком IoT, що означає здатність різних пристроїв і систем IoT взаємодіяти і обмінюватися даними, незалежно від технології, що лежить в їх основі, або від виробника. Отже, пристрої IoT використовують стандартизовані протоколи, формати даних і технології для підтримки інтероперабельності.

8. *Гетерогенність*: Пристрої в мережі IoT демонструють гетерогенність, демонструючи здатність мережі вміщувати різноманітні елементи.

9. *Енергоефективність*: Енергоефективність є важливою характеристикою IoT. Численні пристрої Інтернету речей цілеспрямовано розробляються для мінімізації споживання енергії та створення пристроїв з низьким енергоспоживанням. Крім того, різні підходи IoT розроблені для оптимізації енергоспоживання, наприклад, вибір туманних/граничних обчислень замість хмарних, щоб зменшити вимоги до пропускної здатності і знизити енергоспоживання при побудові системи IoT.

10. *Безпека*: Наявність мільйонів пристроїв, підключених до Інтернету, і величезна кількість даних, що генеруються, підкреслюють вразливість мережі IoT до загроз безпеці. Тобто, безпека і захищеність стають ключовими характеристиками Інтернету речей. Забезпечення безпеки має першорядне значення для збереження ефективності переваг Інтернету речей, включаючи ефективність і новий досвід.

1.2.1. Переваги Інтернету речей

Кількість переваг, які IoT пропонує для життя людей, є основною причиною того, що IoT стає все більш популярним кожного дня. Рішення Інтернету речей розробляються і винаходяться для того, щоб зробити життя людей простішим і зручнішим. Технологія Інтернету речей впливає майже на кожну сферу, включаючи охорону здоров'я, освіту та бізнес. У цьому розділі розглядаються найбільш помітні переваги Інтернету речей у повсякденному житті людей.

1. *Ефективне збирання даних*: Збір даних на основі Інтернету речей був особливо корисним у таких секторах, як охорона здоров'я та фінанси. Наочною ілюстрацією ефективного збору даних є інтеграція Інтернету речей у сектор роздрібної торгівлі. Підключені до Інтернету мітки можуть

надавати дані про рішення про покупку і тенденції продажів – як щотижневі, так і щомісячні. Таке розширення збирання даних може покращити управління запасами та надати цінну інформацію про поведінку клієнтів, що зрештою сприятиме процвітанню бізнесу.

2. *Контроль та автоматизація*: IoT забезпечив своїм користувачам більш комфортний спосіб життя і дозволяє їм контролювати свою повсякденну діяльність одним натисканням кнопки. Одним з простих, але чудових прикладів є "розумна" лампочка, якою можна керувати, навіть не торкаючись вимикачів; користувач може просто вимкнути або увімкнути світло дистанційно. Лампочкою, кавоваркою чи будь-яким іншим електричним пристроєм у домі можна керувати не лише вимикачем пристрою, але й за допомогою голосових команд, якщо вони підключені до голосових асистентів Google або Amazon.

3. *Доступ до інформації в режимі реального часу*: Пристрої Інтернету речей пропонують миттєвий доступ до інформації, що є безцінним у сфері охорони здоров'я, бізнесу та повсякденного використання. Яскравою ілюстрацією переваг доступу до даних у режимі реального часу є сектор охорони здоров'я. Лікарі можуть отримувати доступ до даних про пацієнтів у режимі реального часу, що дає змогу здійснювати безперервний моніторинг стану здоров'я. Ця можливість стає особливо важливою для швидкого надання невідкладної медичної допомоги при виникненні несподіваних проблем зі здоров'ям.

4. *Підвищення ефективності*: Системи Інтернету речей працюють автономно, що є цінною перевагою в різних сферах. Зменшення втручання людини призводить до підвищення ефективності та зменшення залежності від робочої сили. Наприклад, компанія з автопарком транспортних засобів доставки може без зусиль відстежувати їхнє місцезнаходження в режимі реального часу, усуваючи потребу в безпосередній участі працівників у виконанні цього завдання.

5. *Покращення якості життя*: Поява Інтернету речей значно покращила життя користувачів у багатьох аспектах. Моніторинг здоров'я в режимі реального часу, включаючи такі пристрої, як тонометри та фітнес-трекери, дає користувачам можливість ефективно підтримувати своє самопочуття. Розумні будинки пропонують спосіб життя без стресу та зусиль. Ці переваги виходять за межі окремих людей і можуть принести користь цілим галузям або громадам. Розумні пристрої, пов'язані не лише з інтелектуальними світлофорами, але й з моніторами безпеки дорожнього руху та пунктами оплати за проїзд, можуть надавати водіям інформацію про дорожні умови на їхньому маршруті в реальному часі.

6. *Економія коштів та часу*: Інтернет речей мінімізує людські зусилля і значною мірою покладається на передачу даних у режимі реального часу, що призводить до економії часу. Наприклад, моніторинг пацієнтів у режимі реального часу приносить користь як пацієнтам, так і лікарям, усуваючи необхідність фізичних зустрічей, тим самим заощаджуючи час для обох сторін. IoT допомагає підприємствам оптимізувати свої робочі процеси, пропонуючи цінні ідеї та інформацію в режимі реального часу, що призводить до зниження витрат. Окрім оптимізації бізнес-процесів компаній, приватні особи можуть скоротити свої повсякденні витрати завдяки використанню Інтернету речей.

7. *Відстеження активів*: Цей процес передбачає відстеження продуктів у межах бізнес-системи або системи управління логістикою. Ручне відстеження активів є трудомістким і займає багато часу, але його можна спростити завдяки застосуванню технологій Інтернету речей, таких як штрих-коди і RFID-мітки. Ці технології дозволяють здійснювати віддалений моніторинг товарів і надавати зацікавленим сторонам інформацію про будь-які несправності або проблеми в режимі реального часу.

8. *Аналіз даних з дослідницькою метою*: Величезна кількість даних, зібраних з пристроїв Інтернету речей, відкрила великі можливості для дослідників у різних галузях, таких як охорона здоров'я, освіта, бізнес тощо. Дослідники в галузі охорони здоров'я можуть використовувати дані, зібрані за допомогою біосенсорів, для винаходу ліків і вакцин від хвороб; фінансова індустрія може використовувати дані для розуміння тенденцій і поліпшення клієнтського досвіду; супермаркети можуть аналізувати поведінку клієнтів і покращувати свій бізнес тощо.

9. *Великі дані та предиктивний аналіз*: Великі дані були широко визнаним терміном у світі задовго до появи IoT. Він передбачає збирання та аналіз величезних обсягів даних. Однією з основних цілей Інтернету речей є накопичення даних з різних джерел і передача цієї інформації назад в системи для аналізу. Ефективний аналіз великих даних може дати цінну інформацію, починаючи від прогнозів фондового ринку і закінчуючи розумінням поведінки клієнтів, тим самим покращуючи бізнес-ландшафт.

10. *Підвищення продуктивності*: Використання IoT як у промисловості, так і в побуті має потенціал для значного підвищення продуктивності. Наприклад, у розумному будинку користувачі можуть впорядковувати різні домашні завдання за допомогою голосових команд, забезпечуючи ефективну багатозадачність. Аналогічно, в бізнес-середовищі аналіз поведінки клієнтів може підвищити їхню задоволеність, що зрештою сприятиме процвітанню підприємства. Наприклад, 46% підприємств, які впровадили стратегії Інтернету речей, побачили підвищення

ефективності, хоча лише 29% з них спочатку очікували такого покращення [19]. У секторі охорони здоров'я лікарі можуть запропонувати своїм пацієнтам ширший спектр послуг, якщо їм не потрібно фізично відвідувати кожного пацієнта окремо.

11. *Безпека та захист*: Впровадження Інтернету речей пропонує користувачам засоби безпеки не лише в їхніх домівках, але й на підприємствах, у школах, офісах і практично будь-де. Люди можуть віддалено контролювати свої цінні активи, такі як транспортні засоби тощо. Батьки навіть можуть відстежувати місцезнаходження своїх дітей зі своїх робочих місць, забезпечуючи собі душевний спокій. IoT дозволяє відстежувати транспортні засоби та налаштовувати системи оповіщення в разі незвичайних інцидентів. Фінансові компанії та банки можуть підвищити безпеку своїх конфіденційних приміщень або транспортних засобів, використовуючи IoT [20].
12. *Підвищення* рівня залученості *клієнтів*: Інтернет речей пропонує кілька способів підвищити рівень залученості клієнтів. Цього досягають завдяки використанню цінних даних про клієнтів, персоналізації досвіду, підвищенню зручності та забезпеченню взаємодії в режимі реального часу.
13. *Ефективне використання ресурсів*: Інтернет речей сприяє ефективному використанню ресурсів за допомогою різних механізмів і можливостей. Його здатність збирати і відстежувати інформацію в режимі реального часу дає змогу організаціям відстежувати стан своїх ресурсів, таких як обладнання та машини, що дає змогу виявляти неефективність. Прогнозоване технічне обслуговування на основі Інтернету речей у промисловому секторі може передбачити збої в роботі обладнання, скорочуючи час простою і оптимізуючи розподіл ресурсів на технічне обслуговування.
14. *Вдосконалена* технологія: інновації, спричинені Інтернетом речей, призводять до створення нових і більш досконалих технологій на ринку. Наприклад, розглянемо сценарій кондиціонера, яким спочатку керували вручну за допомогою пульта дистанційного керування. З появою Інтернету речей користувачі тепер можуть керувати ним за допомогою голосових команд або контролювати його віддалено. Коли такі інновації з'являються на ринку, вони викликають конкуренцію, стимулюючи розробку вдосконалених рішень на основі відгуків користувачів. Цей цикл інновацій у відповідь на розвиток Інтернету речей сприяє безперервному прогресу технології.

1.3. Особливості промислового Інтернету речей

1.3.1. Індустрія 4.0 і промисловий Інтернет речей

Інтернет речей є однією з ключових технологій, які покладено у основу такого поняття, як четверта промислова революція, або Індустрія 4.0.

Що таке Індустрія 4.0?

Четверта промислова революція (Індустрія 4.0) передбачає новий підхід до виробництва, що грунтується на масовому впровадженні інформаційних технологій у промисловість, масштабній автоматизації бізнес-процесів та поширенні штучного інтелекту.

Переваги Четвертої промислової революції очевидні: підвищення продуктивності, велика безпека працівників завдяки скороченню робочих місць у небезпечних умовах праці, підвищення конкурентоспроможності, принципово нові продукти та багато іншого [21].

Відповідно до загальновідомої класифікації розвиток промисловості можна поділити на чотири періоди:

Таблиця 1.1.

Характерні особливості промислових революцій

Індустрія 1.0	Промислова революція, яка була переходом у Європі та Сполучених Штатах від переважно аграрної економіки до нової економіки, заснованої на виробництві. Цю революцію, яка почалася приблизно в 1760 році, значною мірою спричинив винахід парової машини.
Індустрія 2.0	Друга промислова революція, що почалася приблизно в 1840 році, характеризувалася переходом від парової енергії до електрифікації для конвеєрних методів і зосередженням на продуктивності.
Індустрія 3.0	Третя промислова революція, або цифрова революція, характеризувалася впровадженням комп'ютерів та електроніки для автоматизації, починаючи з кінця 1950-х років.
Індустрія 4.0	Сьогодні світ переживає Четверту промислову революцію, яка характеризується розвитком цифрового штучного інтелекту (ШІ) і процесів, керованих даними.

«Світ перебуває на роздоріжжі. Соціальні та політичні системи, які врятували мільйони людей від злиднів та півстоліття спрямовували нашу державну та глобальну політику, тепер працюють проти нас». З цього тривожного твердження починається книга «Технології Четвертої промислової революції», яку написав

засновник та незмінний президент Всесвітнього економічного форуму у Давосі Клаус Шваб. У 2016 році він ввів у масове вживання термін «Індустрія 4.0» (він з'явився у 2011 році в Німеччині та позначав технології «розумних» заводів), який став синонімом Четвертої промислової революції [8].

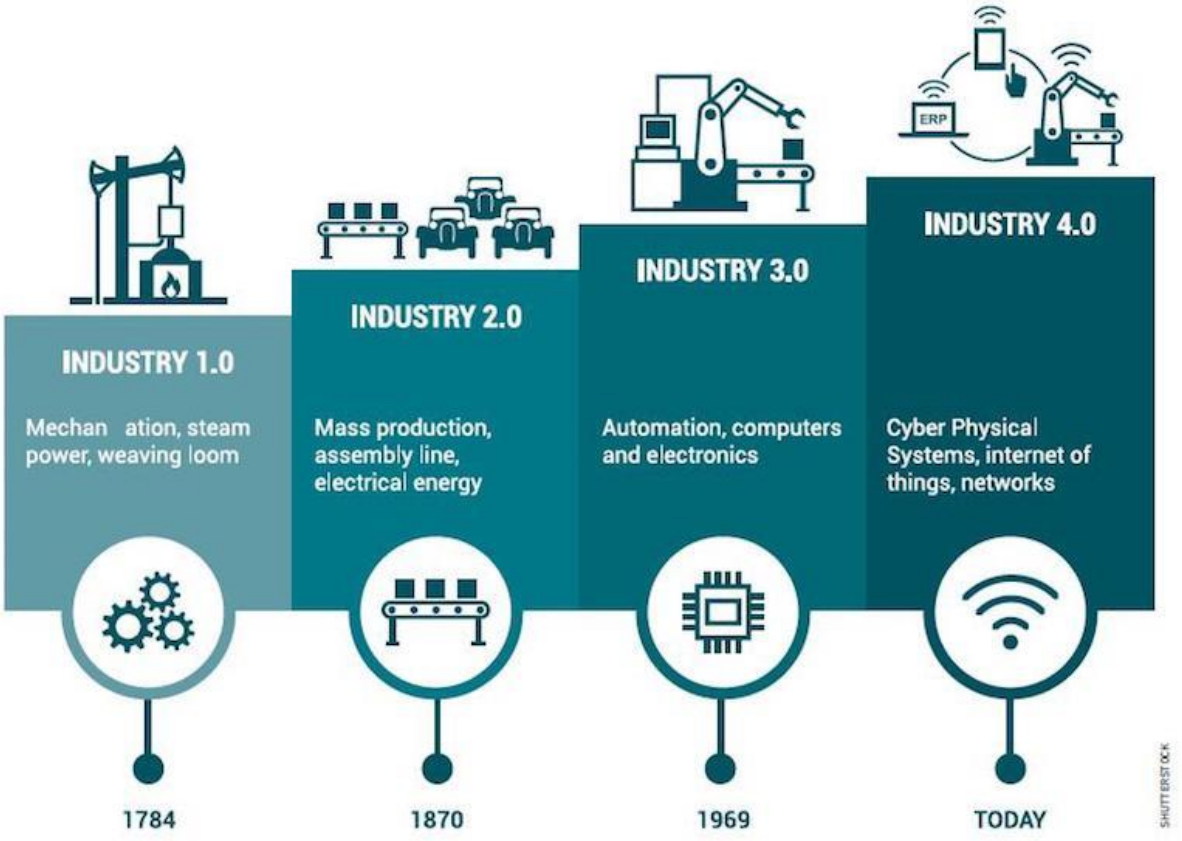

Рис. 1.5. Розвиток промисловості через індустріальні революції [22]

Подібно до всіх попередніх промислових революцій, Четверта змінює не лише виробництво, а й усе наше життя: економіку, відносини між людьми, навіть певною мірою саме розуміння того, що це означає — бути людиною. Штучний інтелект і роботизація, інтернет речей (IoT) та 3D-друк, віртуальна та доповнена реальність, біо- та нейротехнології – ці новітні методи на очах стають частиною нашого повсякденного існування.

Велика перспектива Індустрії 4.0 полягає в тому, що список розумних ініціатив, який швидко розширюється, включає не лише розумні заводи, а й такі напрями (рис.1.6), як:

- Розумні автомобілі
- Розумні будинки
- Розумні будівлі
- Розумні міста

Четверта промислова революція створює бачення майбутнього, яке залежить від вирішення низки сміливих проблем розвитку технологій та інтеграції.

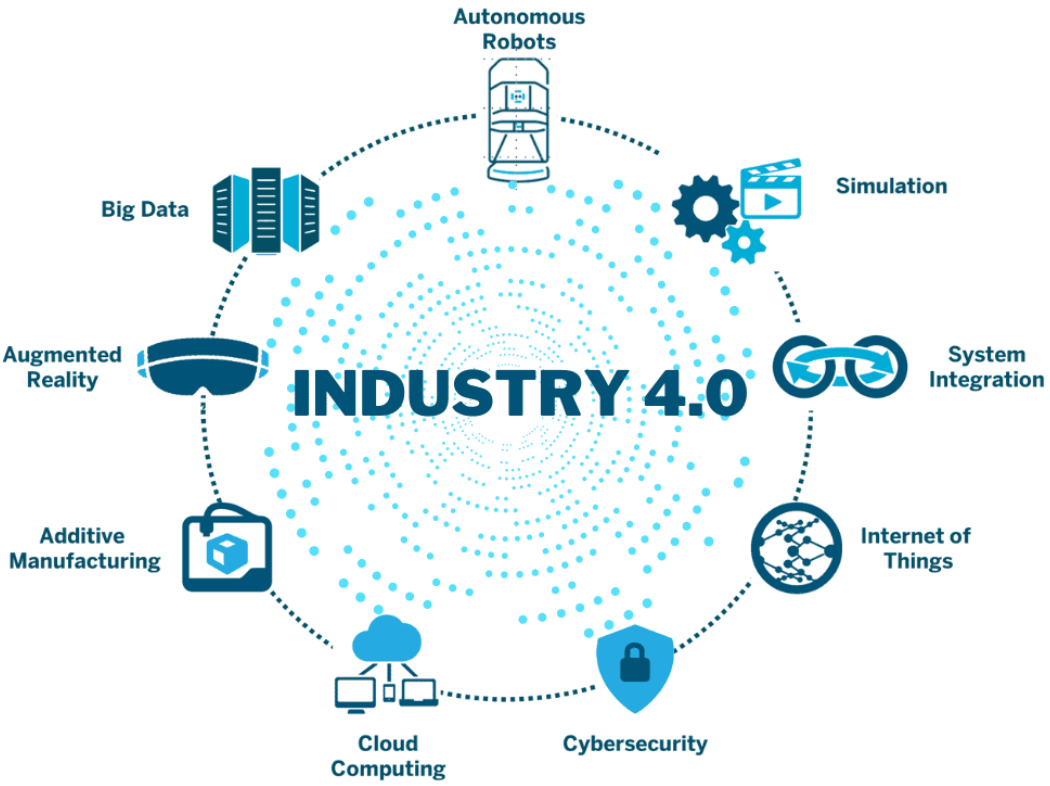

Рис. 1.6. Ключові технології Індустрії 4.0 [23]

Реалізація бачення Industry 4.0 передбачає як мінімум виконання таких етапів:

- Інтеграцію нового інтелектуального обладнання із вбудованими можливостями цифрової обробки, власним збиранням даних телеметрії та легкою інтеграцією в структуру існуючих мереж і старих технологій.
- Розроблення та розгортання датчиків і підключення до мережі, які працівники операційних технологій (OT) можуть легко розгортати та керувати ними для традиційного фізичного обладнання, якому бракує інтелектуальних технологій.
- Удосконалення існуючих архітектур для об'єднання людей і активів у центрі обробки даних (IT) з людьми, технологіями та даними на периферії (OT).
- Створення програмних додатків з використанням вбудованих моделей даних, які застосовуються до проблемної області Індустрії 4.0, міждисциплінарними командами професіоналів галузі та дослідників даних.
- Встановлення показників ROI для того, коли і як інвестувати в нові можливості Industry 4.0, які включали невизначеність і ризик.

Прогрес в обох ініціативах 1 і 2, перерахованих вище, був вражаючим. Кількість розгорнутих інтелектуальних машин, додаткових датчиків для збору даних і автоматизованих процесів підвищили продуктивність і безпеку майже в кожному

промисловому середовищі. Ця тенденція продовжується та розширюється, оскільки переваги рентабельності інвестицій підтверджуються документально, а старе обладнання та обладнання замінюється.

Постійний прогрес у створенні нових програмних додатків, які використовують моделі, керовані даними, потребує економічно ефективного способу передавання даних у центр обробки даних. Центр обробки даних – це місце, де дані доступні для спеціалізованого персоналу та інструментів. Більшість промислових об'єктів можуть доставити віртуальне цунамі даних. Однак регулярно використовується лише частина доступних потоків телеметрії. Необхідні інвестиції, спрямовані на покращення управління даними між периферією та ядром або хмарою, перш ніж ініціатива 4 може бути реалізована.

Індустрія комерційного програмного забезпечення та спільноти програмного забезпечення з відкритим кодом досягли величезного прогресу в рішеннях для зберігання великих даних та інструментах обробки даних для розроблення моделей. Переміщення даних від джерела до підприємства обробки та переміщення додатків, розроблених на центральному заводі, назад до периферії є складними проблемами для більшості організацій, які розробляють можливості Індустрії 4.0. Інструменти та методи, які використовують технологічні компанії масштабу Інтернету, такі як Uber, Facebook, Google і Microsoft, тепер доступні піонерам Індустрії 4.0. Найбільшою проблемою, що залишилася, є побудова кращих мостів між виробниками даних на периферії та технологією великих даних у центрі обробки даних.

Зростання ролі програмного забезпечення в індустрії 3.0 і 4.0

Понад 250 років минуло між винаходами парової машини та першого сучасного цифрового комп'ютера – визначальними технологіями для Індустрії 1.0 та Індустрії 3.0. Успіхи в дизайні фізичних запасів, які використовуються в промисловості, сприяли значному підвищенню продуктивності протягом тих ранніх періодів.

З появою Industry 3.0 програмне забезпечення стало новим джерелом керування автоматизацією та підвищення продуктивності. Важливість програмованого логічного контролера, який з'явився в цифрову еру, залишається надзвичайною і сьогодні. Доступні сотні нових моделей із десятками мов програмування, доступними книгами та навчальними посібниками.

1.3.2. Кіберфізичні системи (КФС)

Індустрія 4.0 ще більше керується програмним забезпеченням, але тепер у центрі уваги – інтерфейс кіберсистем до фізичного обладнання – кіберфізичних систем. Уся технологія, необхідна для перетворення фабрик на розумні фабрики, вже доступна. Точна вартість і рентабельність інвестицій у трансформацію промислових об'єктів невідомі. Отже, вартість широкомасштабної заміни традиційних систем програмного забезпечення системами Industry 4.0, безумовно, буде надто великою та руйнівною. Перехід до Industry 4.0 буде поступовим. Будь-які нові системи повинні

взаємодіяти з багатьма програмними системами, що забезпечують функціональність у відповідь на вимоги, визначені приблизно 20–40 років тому. Промислові підприємства будь-якого віку, які намагаються підтримувати тривалий час безвідмовної роботи та низькі експлуатаційні витрати, повинні визначити, чи ці витрати варті рентабельності інвестицій [24].

Кіберфізичні системи (КФС) є інтегрованими варіантами кіберсистем (що складаються з обчислювальних, комунікаційних та керуючих елементів) та фізичних систем (що складаються з матеріальних елементів). Майже всі продукти у сучасному суспільстві є тією чи іншою мірою кіберфізичними системами. Майже всі сучасні виробничі системи для цих продуктів також КФС (рис.1.7).

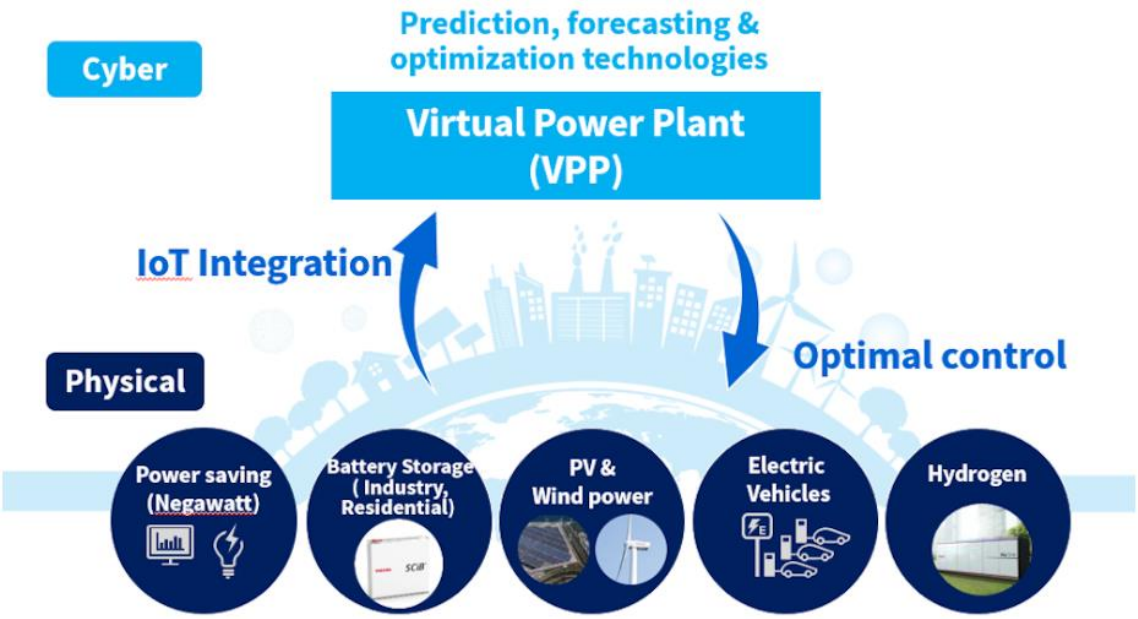

Рис. 1.7. Схема віртуальної електростанції Toshiba [25]

Розробка такої складної системи, як КФС, вдихнула нове життя в галузь системного проектування, яке поступово відходило від сфери професійної діяльності, основаної на кресленнях, до дисципліни, основаної на моделях. Фактично, успіх у кіберфізичній системній інженерії сильно залежить від правильного застосування системної інженерії на основі моделей (MBSE). Виробництво є національним пріоритетом у кількох країнах, зокрема в США, Китаї, Німеччині, Японії. Ці країни вкладають значні кошти у партнерські відносини між державним та приватним секторами, які вони вважають стратегічними, виробничо-технологічними сферами [26].

Наприклад, Національний інститут стандартів і технологій США (NIST) бере активну участь у кількох дослідницьких проектах у галузі інтелектуальних виробничих систем, спрямованих на вирішення проблем стандартів та наукових вимірів у виробничих системах. У цих проектах NIST також застосовує досягнення у галузі кіберфізичних систем для виробництва [27].

Кіберфізичні системи є прямим наслідком інформаційної революції. Обчислення, інтернет-комунікації та цифрове управління, що вбудовуються, стали невід'ємною частиною сучасних інженерних продуктів і процесів їх виробництва. Такі продукти та процеси і є кіберфізичними системами.

Національний науковий фонд (NSF) США є великим інвестором у фундаментальні дослідження в КФС з 2010 року, і він визначає та пояснює КФС наступним чином: «*Кіберфізичні системи* – це інженерні системи, які побудовані на безшовній інтеграції обчислювальних систем та залежать від їх алгоритмів та фізичних компонентів. Прогрес у КФС забезпечить можливості адаптивності, масштабованості, відмовостійкості, безпеки та зручність використання, які набагато перевершать прості вбудовані системи сьогодення. Технологія КФС змінить спосіб взаємодії людей із створеними системами так само, як і Інтернет змінив спосіб взаємодії людей із інформацією. Нова інтелектуальна КФС стимулюватиме інновації та конкуренцію в таких секторах, як сільське господарство, енергетика, транспорт, проектування та автоматизація будівель, охорона здоров'я та виробництво» [28].

1.3.3. Цифрові двійники (Digital Twins)

Ще однією важливою складовою кіберфізичних систем є цифрові двійники, використання яких забезпечує значне підвищення ефективності виробництва, збільшення прибутків компаній та підвищує безпеку в багатьох сферах економіки.

Дослідницька та консалтингова компанія Gartner дає дуже коротке визначення:

Цифровий двійник — це цифрове уявлення реального об'єкта або системи.

Розширене визначення може бути таким:

Цифровий двійник (Digital Twin) – це програмний аналог фізичного пристрою, що моделює внутрішні процеси, технічні характеристики та поведінку реального об'єкта в умовах впливу перешкод та навколишнього середовища.

За визначенням стандарту ISO 23247-1:2021 «Automation systems and integration. Digital twin framework for manufacturing»: «*Цифровий двійник* – це цифрова модель конкретного фізичного елемента або процесу з підключенням до даних, що забезпечує конвергенцію між фізичним і віртуальним станами з відповідною швидкістю синхронізації» [29].

Вперше концепцію цифрового двійника описав 2002 року Майкл Грівс, професор університету Мічігана. У своїй книзі "Походження цифрових двійників" він розклав їх на три основні частини [30]:

- Фізичний продукт у реальному просторі.
- Віртуальний продукт у віртуальному просторі.
- Дані та інформація, що поєднують віртуальний та фізичний продукт.

На думку Грівса, «в ідеальних умовах всю інформацію, яку можна отримати від виробу, можна отримати від його цифрового двійника» [30].

Офіційно термін «Цифровий двійник» уперше згадано у звіті NASA про моделювання та симуляцію за 2010 рік. У ньому йдеться про надреалістичну віртуальну копію космічного корабля, яка відтворювала б етапи будівництва, випробувань та польотів [31].

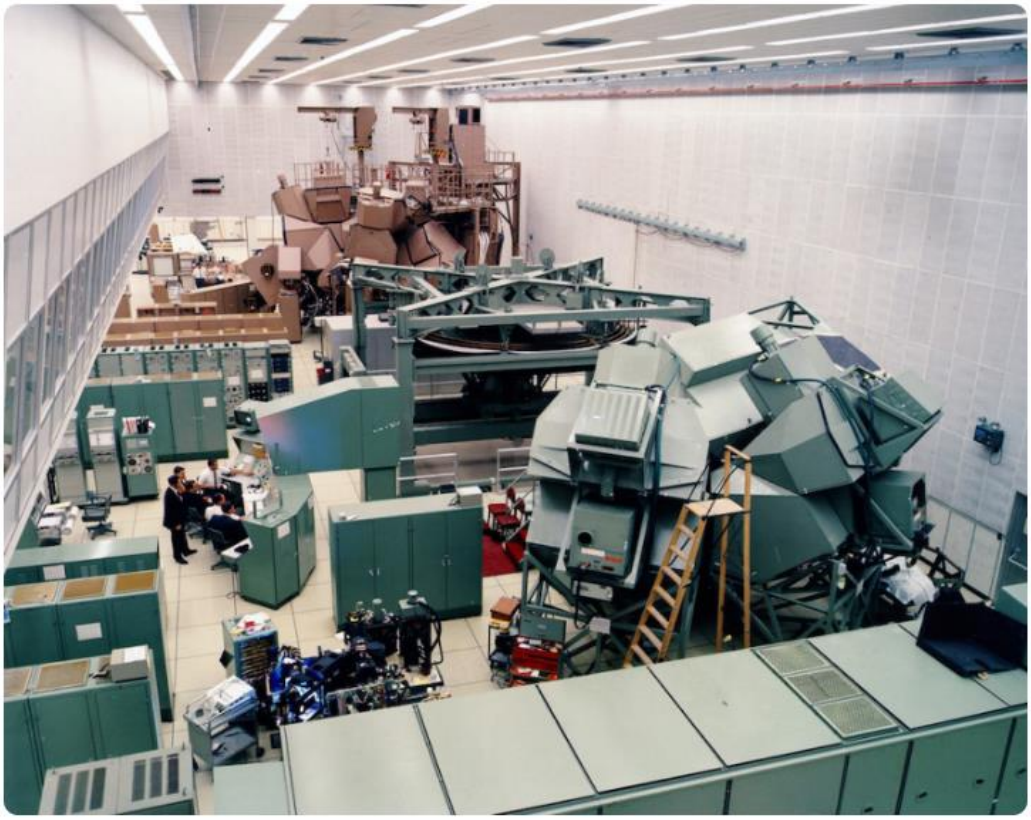

Рис. 1.8. Центр зі створення цифрових двійників у NASA

Потужний поштовх у розвитку цифрових двійників стався завдяки розвитку штучного інтелекту та інтернету речей. Згідно з дослідженням Gartner Hype Cycle, що описує цикли зрілості технологій, це сталося у 2015 році. 2016-го цифрові двійники і самі увійшли до Gartner Hype Cycle, а до 2018 року опинилися на піку (рис. 1.3.) [32].

Важливою особливістю цифрового двійника є те, що як його вхідні параметри використовується інформація з датчиків реального пристрою, що працює паралельно. Робота можлива як в онлайн, так і в офлайн-режимі. Далі можливе порівняння інформації віртуальних датчиків цифрового двійника з датчиками реального пристрою, виявлення аномалій та причин їх виникнення [33].

Датчики на реальний пристрій встановлюють у процесі впровадження на підприємстві технологій промислового Інтернету речей (IIoT). Без створення цифрових двійників виробів неможливе впровадження сучасної технології PLM (Product Lifecycle Management, управління життєвим циклом виробу).

IIoT і PLM — невід'ємні атрибути "розумної фабрики" (Smart Factory). Її характерна риса — формування та використання цифрової моделі матеріальних потоків, тобто Цифрового двійника вже не окремого виробу, а виробничої системи.

Усі названі вище технології теж є підходами до реалізації концепції Четвертої індустріальної революції (Industry 4.0). Якщо в традиційній промисловості досягають необхідні характеристики виробу численими натурними випробуваннями, то в Індустрії 4.0 ставиться завдання проводити багаторазові випробування за допомогою цифрового двійника, а натурні випробування проходити з першого разу.

Відповідно, цифровий двійник можна розглядати як віртуальну модель фізичного об'єкта. Він охоплює життєвий цикл об'єкта та використовує дані в реальному часі, відправлені з датчиків об'єкта, для моделювання поведінки та моніторингу операцій. Цифрові двійники можуть відтворювати безліч реальних предметів від окремих одиниць обладнання на заводі до повноцінних установок, таких як вітряні турбіни і навіть цілі міста. Технологія цифрових двійників дозволяє контролювати роботу об'єкта, виявляти потенційні несправності та приймати більш обґрунтовані рішення про обслуговування та життєвий цикл [34].

Цифрові двійники забезпечують користувачам безліч переваг:

- Підвищення продуктивності

  Інформація та аналітика в реальному часі, що надаються цифровими двійниками, дозволяють оптимізувати продуктивність обладнання, заводу або об'єктів. Проблеми можна усувати у міру їх виникнення, забезпечуючи максимальну роботу систем та скорочуючи час простою.

- Можливості прогнозування

  За допомогою цифрових двійників можна забезпечити повне візуальне та цифрове представлення виробничого підприємства, комерційної будівлі або об'єкта, навіть якщо воно складається з тисяч одиниць обладнання. Інтелектуальні датчики відстежують вихід кожного компонента, відзначаючи проблеми чи несправності у міру їх виникнення. Відповідно можна вжити необхідні заходи за перших ознак проблеми, а не чекати, поки обладнання повністю вийде з ладу.

- Віддалений моніторинг

  Віртуальна природа цифрових двійників означає, що ви можете віддалено контролювати об'єкти та керувати ними. Віддалений моніторинг також означає, що для перевірки потенційно небезпечного промислового обладнання потрібно менше людей.

- Скорочений час виробництва

  Створюючи цифрові репліки, можна прискорити виробництво продуктів і об'єктів Виконуючи сценарії, ви можете побачити, як ваш продукт чи об'єкт реагує на збої та вносити необхідні зміни до початку виробництва.

Цифрова модель, цифрова тінь або цифровий двійник?

Цифровий двійник є надзвичайно популярним терміном, який часто використовують у сьогоднішніх дискусіях про цифровізацію, розумне виробництво та індустрію 4.0. Однак автори не завжди достатньо уточнюють особливості цієї термінології для кожного випадку використання, адже залежно від ступеня деталізації та принципу взаємодії між фізичними та цифровими об'єктами, розрізняють цифрову модель, цифрову тінь та безпосередньо цифровий двійник (рис. 1.9). Розглянемо детальніше кожен з цих типів.

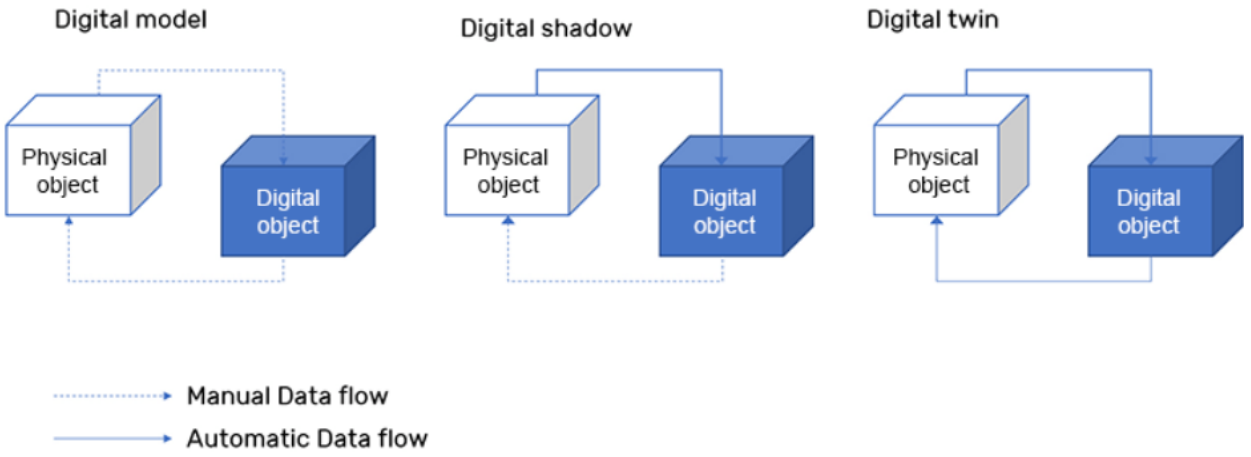

Рис. 1.9. Діаграми потоків в цифровій моделі, цифровій тіні та цифровому двійнику [35]

Цифрова модель

Цифрова модель – це віртуальне представлення фізичного об'єкта, системи або процесу. Він може мати різні форми, як-от 3D-моделі, файли систем автоматизованого проектування (САПР), симуляції або математичні алгоритми. Цифрові моделі дозволяють візуалізувати, аналізувати та маніпулювати об'єктами чи системами в цифровому середовищі, допомагаючи при проектуванні, оптимізації та тестуванні. Зазвичай модель представляє прогноз або припущення щодо того, як фізичний об'єкт, система чи процес можуть працювати в майбутньому чи в певному середовищі.

САПР традиційно використовується для створення цифрової моделі для представлення концептуальної ідеї, детального проекту об'єкта в цифровому середовищі, а також для створення виробничої та будівельної документації. Це спосіб оцінювання варіантів дизайну та розгляду різних можливостей без необхідності фізично реалізовувати об'єкт. Перед початком роботи в майстернях і на будівельних майданчиках можна моделювати обладнання, будівельні елементи та системи трубопроводів, перевіряти тривимірні макети на готовність до складання та етапу будівництва та оцінювати вартість.

У цьому процесі інформація надходить від цифрової моделі до фізичного об'єкта в одному напрямку. Тривимірна модель може бути спрощеною апроксимацією або детальною моделлю 1-1, яка містить значну кількість метаданих.

Зазвичай призначення такої моделі визначає використовувані інструменти та рівень деталізації. Іноді для розрахунків і оцінювання стабільності достатньо навіть 2D-презентації, оскільки на цьому етапі проекту деталі 3D-об'єктів не важливі. У цих випадках мета цифрової моделі визначає рівень точності. Як правило, для CAD-моделей це означає спрощену 3D-модель для базового проекту, яка пізніше використовується для детального проектування та проектування виробництва.

Цифрові моделі знаходять застосування в різних галузях промисловості та дисциплінах. Їх переважно використовують в архітектурі, інженерії, виробництві та розвагах для проектування, створення прототипів і візуалізації. У наукових дослідженнях цифрові моделі корисні для моделювання, аналізу даних і перевірки гіпотез.

Цифрова тінь

Цифрова тінь – це цифрове представлення, що розвивається, яке відображає поточний стан і поведінку фізичної сутності або системи. Вона збирає дані з активу (це може бути база даних, залізнична система або банківська платформа) за допомогою датчиків, пристроїв Інтернету речей або інших джерел і подає інформацію в модель. Це означає, що цифрова тінь актуальна для фізичної сутності. Вона представляє актив із достатнім рівнем деталізації, тому корисно добре її зрозуміти.

Як правило, цифрові тіні є математичними моделями, але вони також можуть бути тривимірними представленнями та часто зосереджені на конкретних аспектах (таких як показники продуктивності, робочі умови або фактори середовища). Вони забезпечують моніторинг, прогнозний аналіз і прийняття рішень.

Наприклад, виробнича компанія може створити цифрову тінь своєї виробничої лінії. Цифрова тінь дозволяє компанії відстежувати та аналізувати виробничі процеси, виявляти вузькі місця та приймати керовані даними рішення для оптимізації процесів і покращення якості. У разі будь-яких несподіваних збоїв або втрати даних цифрову тінь можна використовувати для відновлення останнього робочого стану та мінімізації часу простою.

Цифрові тіні є цінними в ситуаціях, коли моніторинг і аналіз є критичними. Вони зазвичай працюють у таких галузях, як логістика, управління ланцюгами поставок, енергетика та транспорт. Збираючи й аналізуючи дані з датчиків і пристроїв Інтернету речей, цифрові тіні полегшують прогнозне технічне обслуговування, виявлення відхилень і оптимізацію процесів і операцій.

Цифрові двійники

Цифрові двійники об'єднують віртуальну та фізичну сфери, створюючи зв'язок у реальному часі між фізичною сутністю та її цифровим аналогом, де фізичний об'єкт передає інформацію цифровій копії та навпаки. Цифрові двійники моделюють та контролюють фізичні об'єкти або системи, полегшуючи аналіз, оптимізацію та прогнозне технічне обслуговування. Вони забезпечують живий цикл зворотного зв'язку та сприяють підвищенню продуктивності, ефективності та надійності.

Інакше кажучи, існує двостороння взаємодія між фізичним і цифровим середовищем, де цифрова репліка здатна змінити те, як працює фізична сутність. Наприклад, це має вирішальне значення, якщо ми говоримо про критично важливий актив, важливий з погляду доданої вартості, у сферах національного значення, таких як безпека чи конкурентна перевага. У цих випадках важливо забезпечити достатню стійкість до того, як актив реагуватиме на потенційні відхилення.

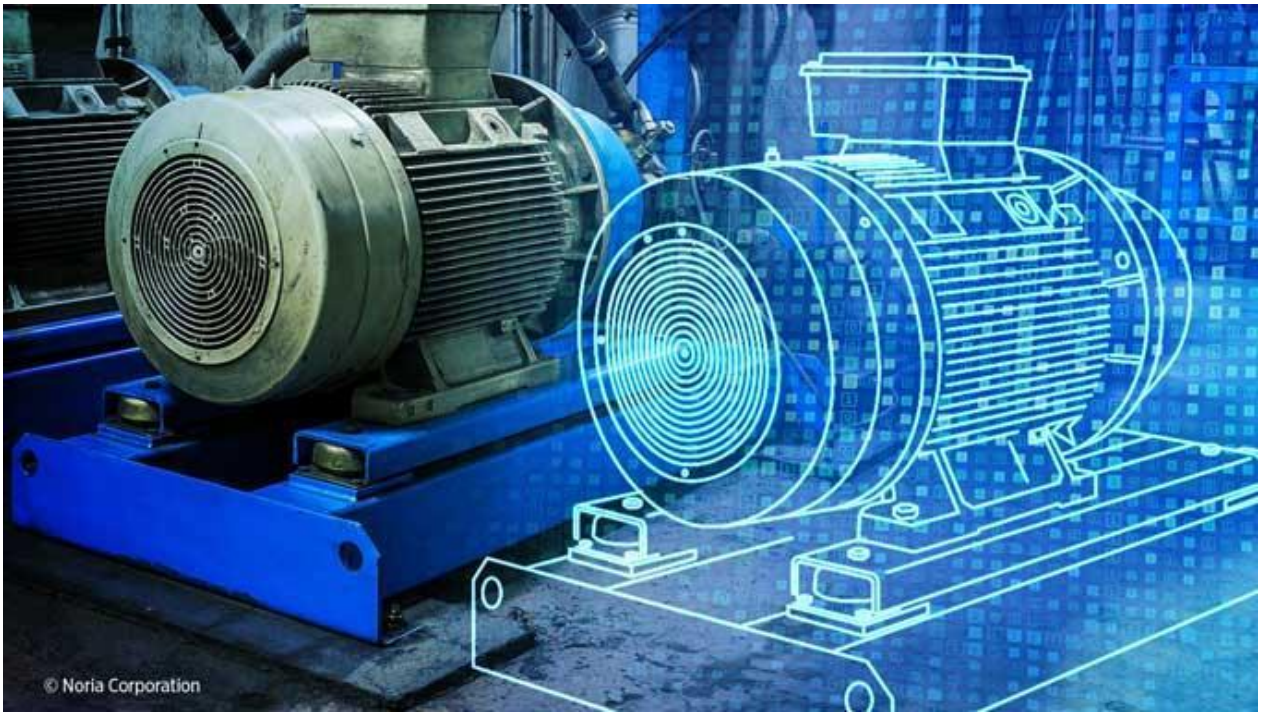

Рис. 1.10. Приклад цифрового двійника електродвигуна [36]

Цифрові двійники починають створюватись з цифрової моделі або цифрової тіні, щоб захопити або ініціювати їх. Простий сценарій – це коли цифрова модель поступово створюється на етапі базового проектування, розробляється потім в детальному проектуванні та використовується для надання необхідної інформації та моделювання змін у процесі будівництва. Це підтримує та полегшує процес виробництва, результатом якого є фізичний об’єкт. Після створення та завершення проекту цифрова модель може бути викинута або використана надалі для управління активами як цифровий двійник. Діапазон необхідних варіантів використання значно варіюється від проектів технічного обслуговування та модернізації до конкретних випадків моделювання сценаріїв для надзвичайних ситуацій або навчання персоналу.

Здається, незважаючи на стрибки вперед у розвитку програмного та апаратного забезпечення, існування універсального цифрового двійника залишається під питанням. У промислових проектах різні групи зацікавлених сторін вимагають різних областей для інформації. Те, що важливо і критично для дизайнерів, не стосується технічного обслуговування чи інших функцій.

Цифровий двійник підкреслює двонапрямлений підхід. Інформаційний потік іде не лише від цифрових активів до фізичного світу, а й повертається назад; інформація з будівництва та управління активами зливається з цифровою моделлю. Це найскладніша і складна ситуація, яка вимагає чіткого визначення потреб і ролей зацікавлених сторін.

Цифрові двійники використовуються в складних системах, таких як виробничі підприємства, інфраструктура, заклади охорони здоров'я та розумні міста. Вони забезпечують моніторинг і контроль у реальному часі, прогнозне технічне обслуговування та оптимізацію продуктивності. Цифрові близнюки також можуть відігравати важливу роль в оптимізації енергоспоживання, покращенні розробки продукту та забезпеченні дистанційного моніторингу та допомоги.

Області застосування цифрових двійників

Цифрові двійники знайшли своє застосування в різних областях. Одна з найважливіших функцій полягає у вдосконаленні виробничих процесів. Використовуючи цифрові двійники, компанії можуть у цифровому середовищі створювати копії своїх розумних підприємств, виявляти «вузькі місця» (у компонентах, системах, процесах та інших активах), тестувати потенційні рішення, моделювати результати взаємодій між компонентами та прогнозувати стохастичні зміни, які можуть виникнути при виконанні операцій. Така симуляція заощаджує організації час, ресурси та гроші, необхідні для тестування робочих гіпотез на практиці [37].

Цифрові двійники також знайшли своє місце у промисловому дизайні та випробуваннях виробів. Наприклад, виробництво реактивного двигуна, для одного з найпопулярніших літаків передбачає такі етапи: кілька тисяч окремих компонентів спочатку збираються воєдино, а потім проходять великі контрольні випробування перевірки безпеки роботи двигуна загалом. Але тепер виробнику не обов'язково збирати дорогий фізичний зразок авіаційного двигуна, він може замінити його на цифровий двійник – точну тривимірну копію. Саме її належним чином аналізують, оцінюють та використовують відповідно до чинних вимог. Більше того, цифровий двійник можна створити і для двигуна, що вже перебуває в експлуатації, щоб проаналізувати стан його компонентів та розрахувати прогнозне технічне обслуговування [38].

Найбільш ефективним застосування цифрових двійників є для продукції з такими критеріями:

- Супровід продукції кваліфікованим спеціалізованим сервісом (контроль стану, моніторинг, технічний супровід)
- Тривалий життєвий цикл виробу (5-70 років)
- Велика кількість примірників встановленого обладнання
- Широкий діапазон та різноманітність умов експлуатації
- Важкодоступність виробу для обслуговування

Під цей перелік критеріїв підпадає продукція з різних галузей промисловості, зокрема:

- енергетика;
- авіаційні двигуни та системи;
- складне промислове обладнання (насоси, приводи та ін.);
- залізничні та автомобільні транспортні системи;
- медичне обладнання.

Як виглядає процес створення цифрового двійника

Двійники можна створювати різними способами:

- графічна 3D-модель;
- модель на основі інтернету речей;
- інтегровані математичні моделі – такі, як CAE-системи (Computer-aided engineering, рішення для інженерного аналізу, розрахунків та симуляцій) для інженерних розрахунків;
- різні технології візуалізації, включаючи голограми, AR та VR.

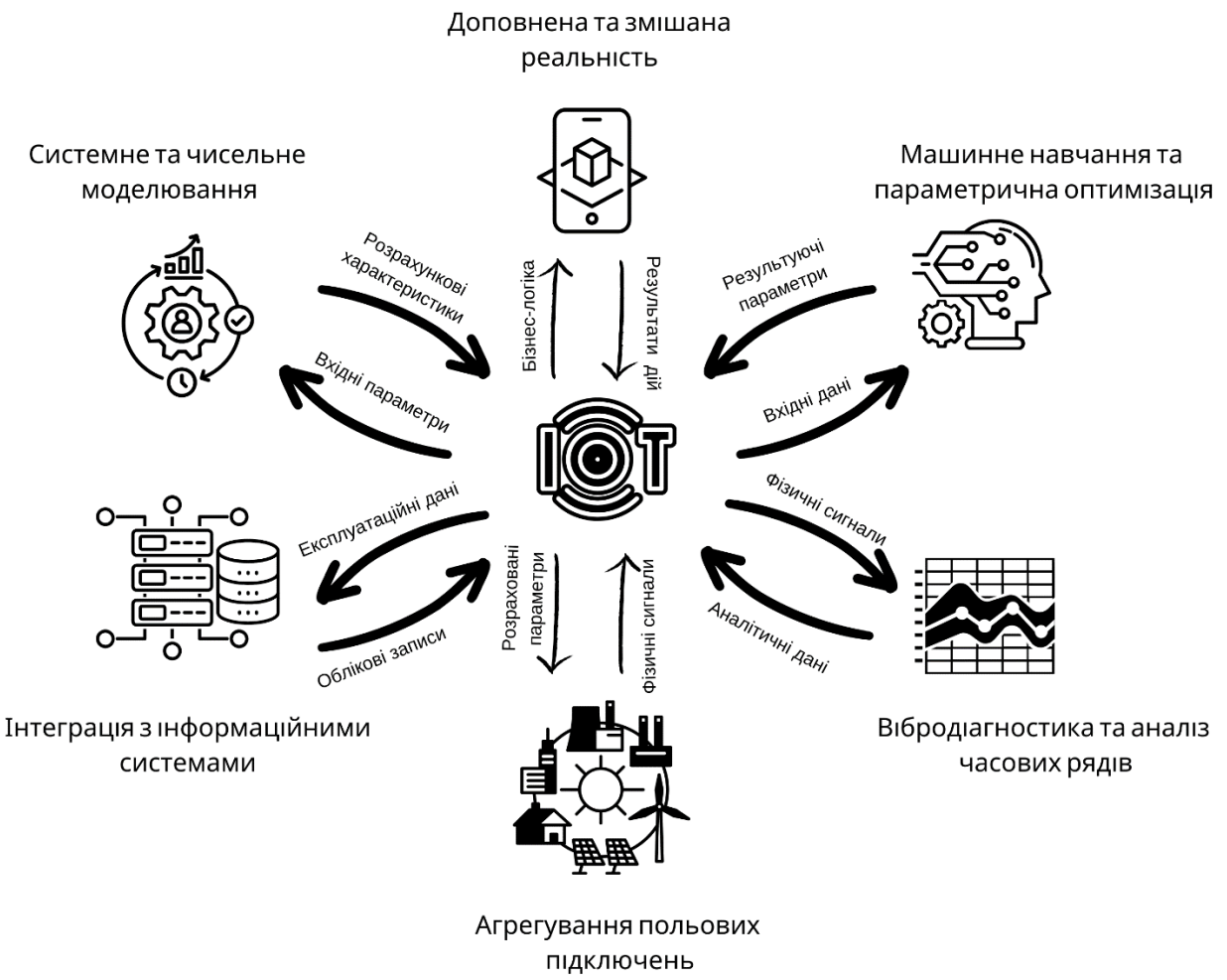

Рис. 1.11. Ідеологія комплексного цифрового двійника

Розглянемо етапи створення цифрового двійника:

- Дослідження об'єкта

Цей етап передує розробці тільки в тому випадку, якщо цифровий двійник має реальний прототип — наприклад, працююче підприємство або система комунікацій. Тоді розробники складають детальну карту прототипу, відтворюють усі процеси та характеристики. При цьому важливо вивчити об'єкт у різних умовах.

- Моделювання цифрової копії об'єкта

Цей етап може бути першим, якщо реального прототипу ще немає і створення цифрового двійника передує йому. Наприклад, у будівництві чи дизайні, коли спочатку створюється цифрова 3D-модель, а потім — оригінал будівлі чи іншого об'єкта.

Для побудови комплексної моделі використовують математичні методи обчислення та аналізу:

  - Метод кінцевих елементів (FEA - Finite Element Analysis), що дає змогу розрахувати експлуатаційне навантаження. Його застосовують, наприклад, для розрахунку механіки деформованого твердого тіла, теплообміну, гідродинаміки та електродинаміки.
  - FMEA-моделі (Failure Mode and Effects Analysis, аналіз видів та наслідків відмов) необхідні для аналізу надійності систем та виявлення найбільш критичних кроків виробничих процесів.
  - CAD-моделі (computer-aided design/drafting, засоби автоматизованого проектування) використовуються, щоб розрахувати зовнішні характеристики та структуру об'єктів, матеріалів та процесів.

- Реалізація моделі

Потім розраховану раніше архітектуру цифрового двійника переносять на спеціальні платформи, такі як Siemens або Dassault Systemes. Вони поєднують математичні моделі, дані та інтерфейс для управління цифровим двійником, перетворюючи його на динамічну систему. Цей етап можна порівняти з трансформацією програмного коду на програму або додаток з візуальним інтерфейсом, який зрозумілий будь-якому користувачеві.

- Тестування основних процесів роботи на цифровому двійнику

Головна мета цього етапу — спрогнозувати, як поводитиметься об'єкт чи система у звичайному режимі та при позаштатних ситуаціях, щоб уникнути поломок та перевантаження після запуску. Для цього до процесу підключають технічних аналітиків, які збирають великий масив даних під час випробувань, щоб прорахувати алгоритми для будь-яких можливих умов та ситуацій.

- Запуск та налагодження

Якщо попередній етап провели коректно, у процесі роботи реального прототипу можна уникнути до 90% збоїв та поломок. Однак частину ситуацій все ж таки не вдається спрогнозувати, і тоді їх відстежують вже на етапі запуску та налагодження цифрового двійника.

- Коригування та розвиток оригінального об'єкта або системи

Далі інженери продовжують працювати з цифровим двійником як із реальним фізичним об'єктом доти, доки не будуть налагоджені всі системи та процеси. За результатами цієї роботи в оригінальний об'єкт вносять зміни, щоб досягти його максимальної ефективності.

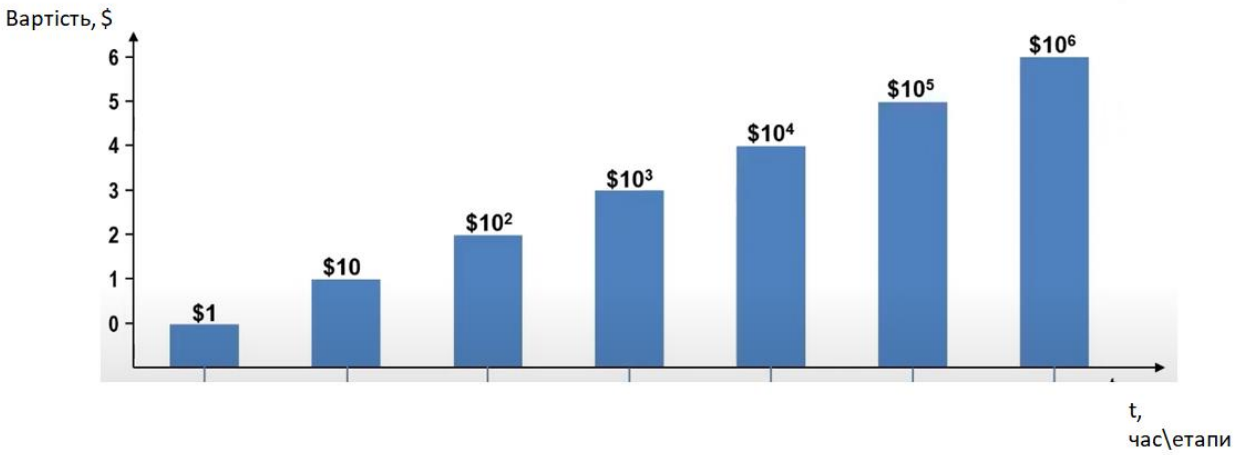

Рис. 1.12. Умовна вартість внесення змін в проект на різних етапах життєвого циклу розробки

Відповідно, цифровий двійник застосовується на всіх стадіях життєвого циклу виробу, включаючи проектування, виробництво, експлуатацію та утилізацію.

На етапі ескізного проектування: створюються варіанти комп'ютерної моделі виробу, що розробляється для оцінювання та вибору можливих технічних рішень.

На етапі технічного проектування: вибраний на попередньому етапі варіант доопрацьовується та уточнюється з використанням моделей елементів. Отримана в результаті модель виробу дозволяє врахувати та оптимізувати взаємодію всіх елементів з урахуванням режимів роботи та впливів навколишнього середовища, її вже можна називати цифровим двійником виробу, що розробляється.

На етапі виготовлення: розроблена модель допомагає визначити необхідні допуски при виготовленні для досягнення необхідних характеристик та забезпечення безвідмовної роботи виробу протягом усього терміну служби, а також дозволяє швидко виявляти причини несправностей у процесі тестування.

На етапі експлуатації: модель цифрового двійника може бути доопрацьована та використана для реалізації зворотного зв'язку з метою внесення коректив у розроблення та виготовлення виробів, діагностику та прогнозування несправностей, підвищення ефективності роботи, для виявлення нових запитів споживачів.

Варто зазначити, що вартість внесення змін в проєкт на різних етапах його реалізації є різною: якщо зміни на етапі ескізного проєктування становлять умовний 1 $ та можуть бути легко і швидко здійснені, то для тої самої зміни після етапи реалізації і введення в експлуатацію може знадобитись умовно 10^6 $, а також набагато довший час та зусилля.

Типи цифрових двійників

Існує кілька різних типів цифрових двійників, які часто можуть працювати одночасно в одній системі. Хоча деякі цифрові двійники реплікують лише окремі частини об'єкта, вони мають вирішальне значення задля забезпечення віртуального представлення.

Найбільш поширеними типами цифрових двійників є такі:

- Двійники компонентів

  Двійники компонентів, або двійники деталей – цифрове представлення окремої частини всієї системи. Вони є важливими для роботи об'єкта, такого як двигун вітряної турбіни.

- Двійники об'єктів

  У термінології цифрового двійника об'єкти – це два або більше компонентів, які працюють як частина більш комплексної системи. Двійники об'єктів віртуально представляють взаємодію компонентів та генерують дані про продуктивність, які можна аналізувати для прийняття обґрунтованих рішень.

- Двійники систем

  Вищий рівень абстракції двійників об'єктів – це двійники систем або двійники одиниць. Двійник системи показує, як різні об'єкти спільно працюють у рамках ширшої системи. Прозорість, що забезпечується технологією двійника системи, дозволяє приймати рішення щодо підвищення продуктивності чи ефективності.

- Двійники процесів

  Двійники процесів відображають цифрове середовище цілого об'єкта і дають уявлення про те, як різні його компоненти, об'єкти та одиниці працюють разом. Наприклад, цифровий технологічний двійник може у цифровому вигляді відтворити роботу всього виробничого підприємства, об'єднавши всі компоненти всередині нього.

Класифікація двійників виробу:

1. *Цифрові двійники-прототипи (DTP).* DTP-двійник містить інформацію, необхідну для опису та створення фізичних версій екземплярів виробу. Ця інформація включає геометричну та структурну моделі, технічні

вимоги та умови; вартісну модель, розрахункову (проектну) та технологічну моделі виробу. DTP-двійник можна вважати умовно-постійною віртуальною моделлю виробу.

2. *Цифрові двійники-примірники (Digital Twin Instance, DTI).* DTI-двійники виробу описують конкретний фізичний екземпляр виробу, з яким двійник залишається пов'язаним протягом усього терміну служби. Двійники цього типу створюються на базі DTP-двійника та додатково містять виробничу та експлуатаційну моделі, які включають історію виготовлення виробу, застосування матеріалів та комплектуючих, а також статистику відмов, ремонтів, заміни вузлів та агрегатів та ін. Тобто, DTI-двійник виробу піддається змінам відповідно до змін фізичного екземпляра під час його експлуатації.
3. *Агреговані двійники (Digital Twin Aggregate, DTA).* DTA-двійники виробу визначаються як інформаційна система управління фізичними екземплярами сімейства виробів, яка має доступ до всіх їх цифрових двійників.

Сфери застосування цифрових двійників

Глобальний ринок цифрових двійників у період від 2020 до 2022 рік зріс на 71%. При цьому майже дві третини підприємств (близько 63%) запроваджують такі рішення або планують їхнє розроблення. Про це йдеться у звіті IoT Analytics, опублікованому 7 березня 2023 року [39].

Оприлюднені дані базуються на аналізі 100 різних проектів у сфері IoT. Зазначається, що багато ініціатив з цифрової трансформації передбачають створення цифрових двійників — копій фізичних об'єктів чи процесів: такий підхід допомагає оптимізувати ефективність бізнесу та прискорити впровадження інновацій. Станом на кінець 2022 року приблизно 29% виробничих компаній у всьому світі повністю впровадили або впроваджували стратегію цифрових двійників для частини своїх операційних активів.

Загалом, IoT Analytics визначає концепцію цифрових двійників як віртуальну модель, яка відтворює поведінку існуючого чи потенційного реального активу, системи чи кількох систем. При цьому виділяються шість основних сфер застосування таких рішень: це системне прогнозування, моделювання систем, взаємосумісність активів, технічне обслуговування, візуалізація та моделювання продуктів. У деяких випадках цифрові двійники можуть вирішувати завдання у кількох напрямках.

1. Системне прогнозування

До цієї групи належать близько 30% проаналізованих проектів. У цьому випадку цифрові двійники використовуються для прогнозування цілих систем, наприклад, частини або всього заводу, будівлі, електростанції або навіть міста. Віртуальні копії об'єктів допомагають визначати поведінку та майбутній стан фізичної системи на основі поточних даних та записів про події у минулому.

2. Моделювання систем

Частка таких задач становила близько 28%. Моделювання складних систем дозволяє інженерам тестувати всілякі сценарії за схемою «що станеться, якщо». При цьому може враховуватися безліч найрізноманітніших параметрів і змінних. Приклади використання — моделювання підприємств перед відкриттям чи внесенням суттєвих змін, віртуальне розгортання залізничної мережі чи транспортної інфраструктури у мегаполісі.

3. Взаємосумісність активів

Критеріям цієї категорії задовольняє приблизно кожний четвертий (24%) проект. Ці цифрові двійники спрощують та раціоналізують загальні формати даних та дозволяють стандартизувати введення/виведення показників на етапі експлуатації або оптимізації об'єкта. Причому можна в режимі реального часу видобувати різні дані з активів.

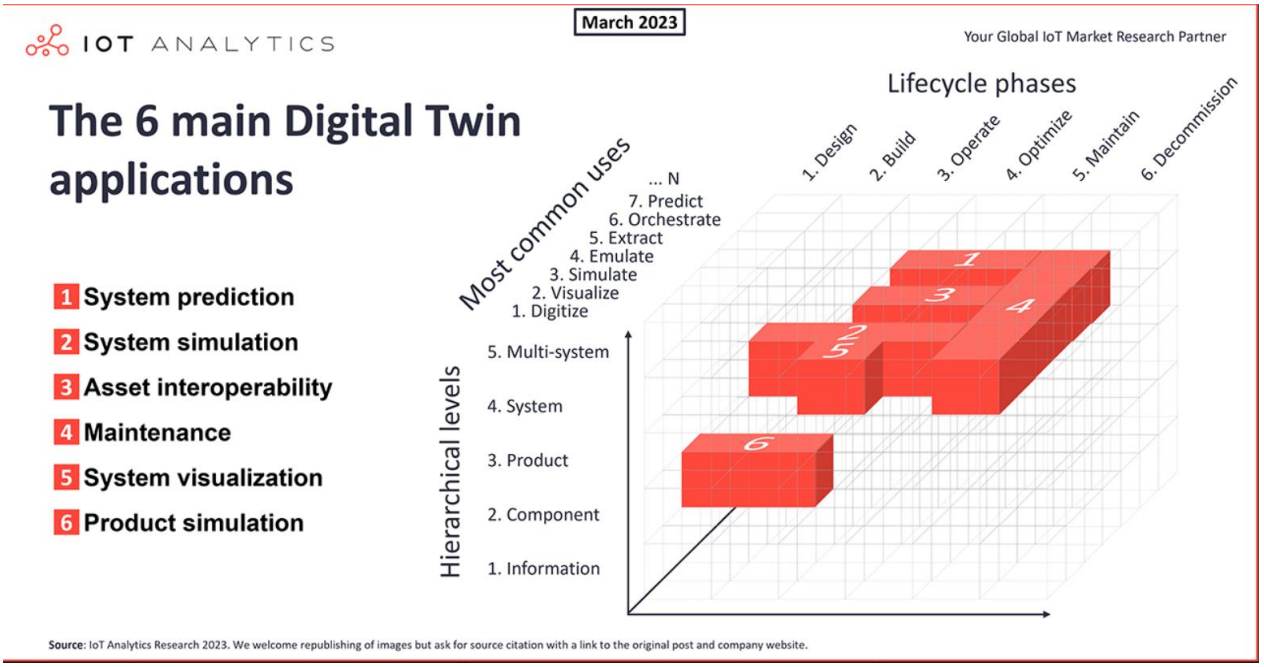

Рис. 1.13. Шість головних застосувань цифрових двійників за версією IoT Analytics

4. Технічне обслуговування

Основним завданням таких цифрових двійників, на які припадає 21%, є допомога системі на етапі обслуговування. Найчастіше такі моделі включають певні функції прогнозування. Подібні рішення переважно призначені для забезпечення експлуатаційної ефективності об'єкта.

5. Візуалізація

Приблизно 20% проаналізованих проектів цифрових двійників орієнтовані на візуалізацію системи на етапі її експлуатації. Серед найпоширеніших типів використовуваних візуалізацій — тривимірні елементи, що допомагають отримати уявлення про роботу того чи іншого об'єкта чи сервісу.

6. Моделювання продуктів

На ці рішення припало 9%. Цифрові двійники відіграють ключову роль у розробці нових та покращених продуктів. Основним варіантом використання є моделювання різних елементів і конструкцій у віртуальному просторі, що усуває необхідність створення дорогих прототипів і дозволяє швидко тестувати тисячі (а деяких випадках — мільйони) варіантів виробу.

2. Екосистема IoT

Сучасна концепція Інтернету речей передбачає, що всі сучасні пристрої, незалежно від платформи, повинні мати можливість спільно функціонувати з іншими пристроями та сервісами, утворюючи єдину взаємозалежну екосистему, а не існувати ізольовано.

Саме ця передумова є однією з основних причин трансформації ринку вбудовуваних систем. Сьогодні він рухається у напрямку розробки інтелектуальних систем (датчиків, машин, механізмів, приладів тощо), об'єднаних в єдину глобальну обчислювальну мережу з метою отримання та обробки даних для підвищення ефективності виробництва (у промисловій сфері) або комфорту та зручності користувача (на рівні споживача).

Розгортання таких інтелектуальних систем потребує злагодженої роботи одразу кількох учасників ринку, включаючи як постачальників комплектуючих (все тих же процесорів, мікропроцесорів, контролерів, датчиків тощо), так і виробників кінцевих продуктів (споживча електроніка, промислове обладнання, автомобілі, літаки тощо), виробників програмного забезпечення, здатних кастомізувати всі ці вбудовані системи для окремо взятих замовників, підключити їх до «хмар» та забезпечити їхню взаємодію з іншими системами в інфраструктурі замовника.

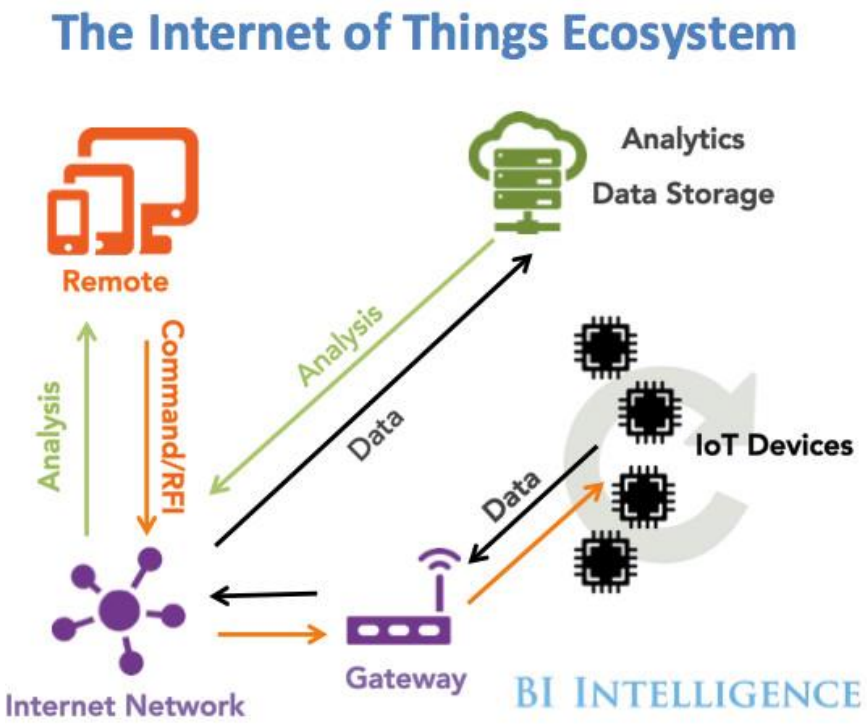

Рис. 2.1. Структурна схема екосистеми IoT [40]

Екосистема IoT складається з трьох ключових компонентів, які є основними будівельними блоками для побудови IoT системи:

1. Датчики/пристрої та виконавчі механізми;

2. Зберігання та аналітика даних;

3. Інструменти інтерпретації та візуалізації.

Розглянемо кожен з цих компонентів та їх типи.

2.1. Датчики/пристрої та виконавчі механізми

2.1.1. Датчики/пристрої

Датчики відіграють вирішальну та важливу роль у системі IoT. З огляду на те, що IoT працює шляхом збору даних із навколишнього середовища, для задоволення цієї потреби всі пристрої IoT повинні містити один або кілька датчиків. Визначальною характеристикою пристроїв IoT є їх усвідомлення контексту, що стає можливим завдяки використанню сенсорної технології. Датчики не тільки компактні та економічні, але й енергоефективні. Однак вони мають обмеження, такі як ємність батареї та легкість розгортання.

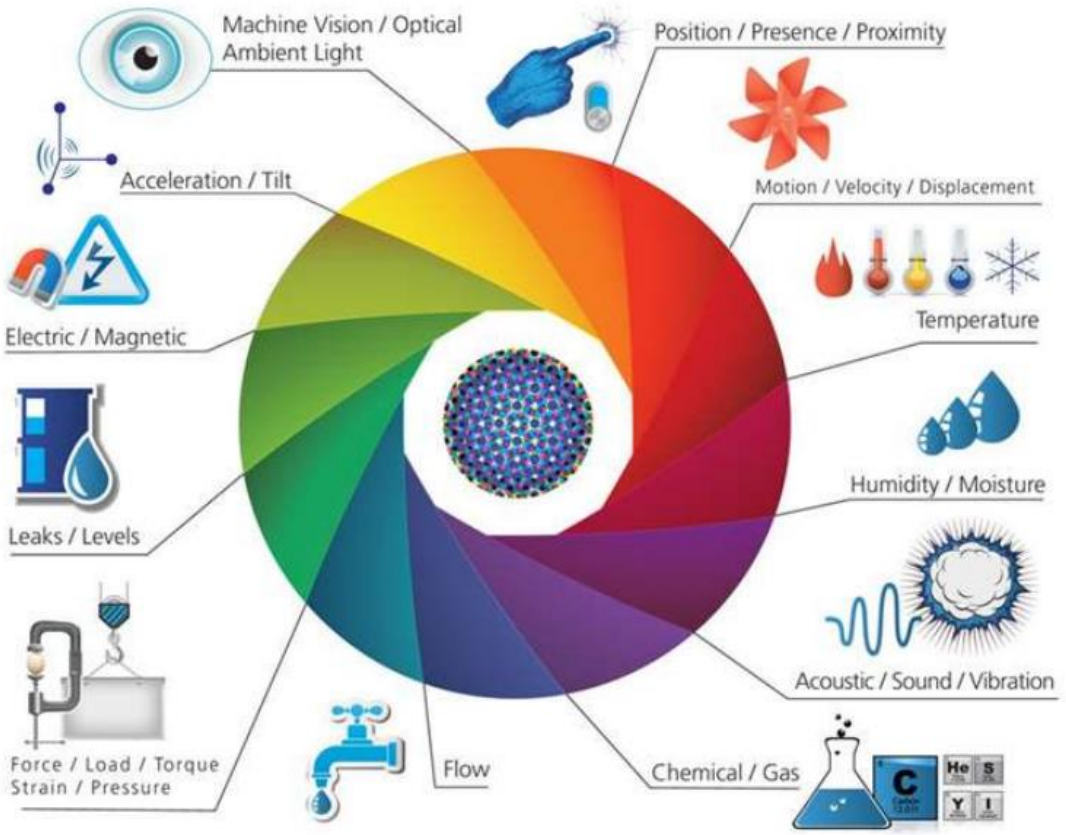

Рис. 2.2. Типи датчиків IoT

Розглянемо різні типи датчиків.

- Мобільні датчики.

  Смартфони, які дуже поширені та часто використовувані, оснащені різними датчиками. Враховуючи їх широке використання, дослідники вивчають потенціал використання смартфонів як невід'ємних компонентів у створенні розумних рішень IoT. Ці програми можуть використовувати дані датчиків зі смартфонів для отримання цінної інформації та результатів. Деякі з загальних датчиків, які є в смартфонах, містять акселерометр, гіроскоп, GPS, магнітометр, датчик світла та датчик наближення [19]. Деякі смартфони, наприклад Samsung Galaxy S4, оснащені додатковими датчиками, зокрема термометром, барометром і датчиком вологості [4].

- Медичні датчики

  Галузь охорони здоров'я є однією з найпоширеніших сфер, де розробляються інноваційні застосування Інтернету речей. Носимі пристрої та датчики полегшили віддалений моніторинг для лікарів і дозволили дослідникам постійно збирати дані в режимі реального часу. Ці пристрої бувають різних форм, наприклад, браслети, розумні годинники та пластирі (патчі) для моніторингу. Розумні годинники та фітнес-трекери, відомі своєю універсальністю, набули популярності серед споживачів. Також, пластирі для моніторингу стали цінним надбанням для сектору охорони здоров'я, оскільки вони дають змогу дистанційно лікувати пацієнтів.

- Нейронні датчики

  Нейронні датчики відіграють вирішальну роль у розумінні роботи нейронів людини, дозволяючи декодувати сигнали мозку, оцінювати поточний стан мозку та, за необхідності, оптимізувати його для покращення концентрації та уваги. Цю практику зазвичай називають нейрофідбеком.

- Екологічні та хімічні датчики

  Тоді як звичайні інструменти керують такими параметрами, як температура та тиск, спеціалізовані екологічні датчики відіграють вирішальну роль в оцінюванні якості повітря. Ці датчики виявляють гази та тверді частинки, а також вимірюють такі фактори, як температура, вологість, тиск і забруднення. Крім того, хімічні сенсори відіграють вирішальну роль у виявленні як хімічних, так і біохімічних речовин. Серед доступних інноваційних технологій – електронний ніс (e-nose) і електронний язик (e-tongue), які грунтуються на розпізнаванні образів,

щоб відчувати хімічні речовини на основі запаху та смаку. Ці датчики застосовують у розумних містах для моніторингу рівнів забруднення.

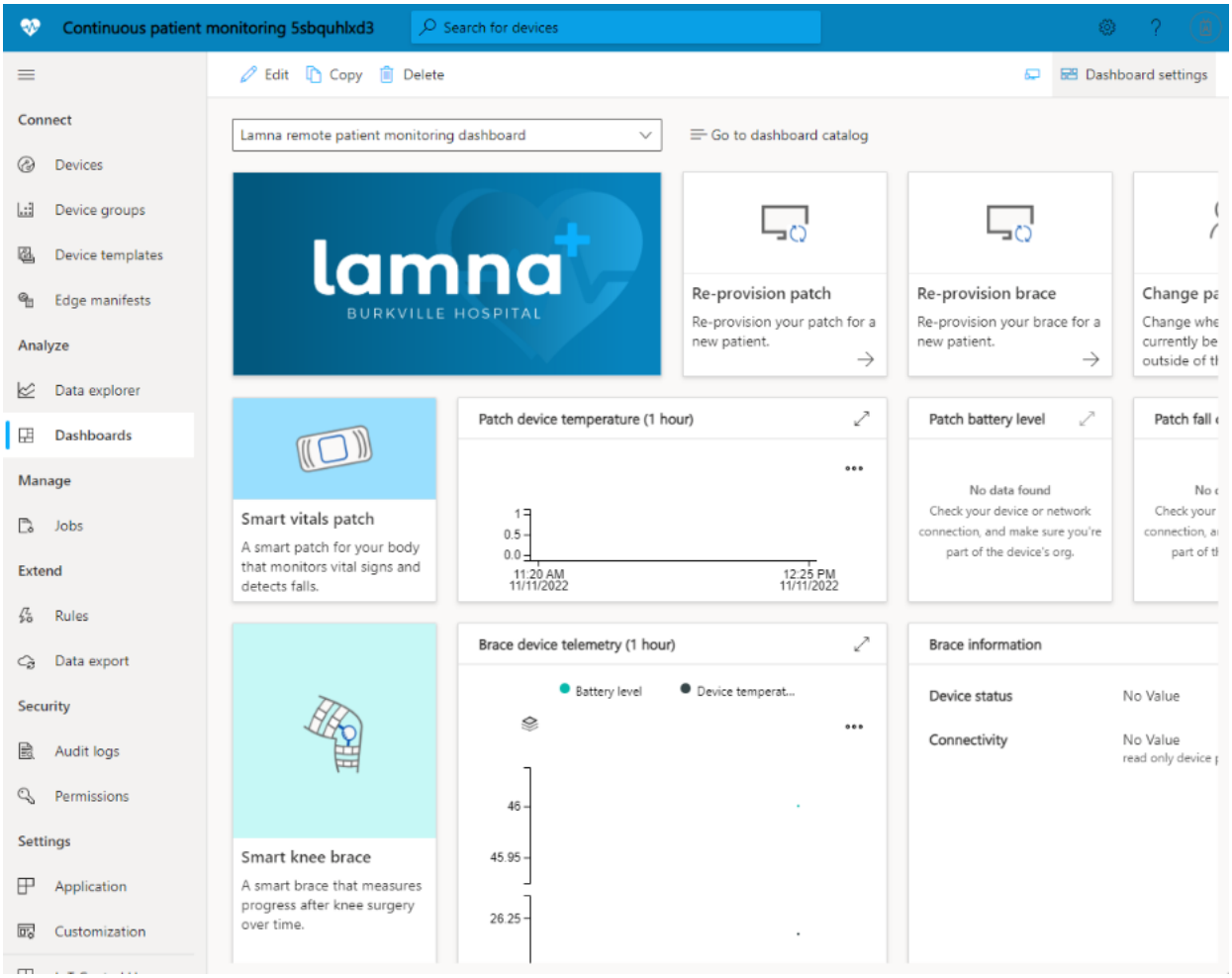

Рис. 2.3. Панель для віддаленого моніторингу пацієнтів Lamna лікарні Берквіля з використанням Azure IoT [41]

- Радіочастотна ідентифікація (RFID)

  Технологія RFID, яка виконує роль датчика, знаходить поширена в різних програмах IoT. Наприклад, її використовують для відстеження продуктів у великих запасах або моніторингу товарів у великих роздрібних магазинах.

2.1.2. Виконавчі механізми

Виконавчі механізми використовуються в IoT-пристроях для виконання певної дії. Вони перетворюють енергію на фізичний рух і зазвичай розташовані на зовнішній периферії системи. Візьмемо, наприклад, сценарій із системою «розумний дім», яка містить численні датчики та виконавчі механізми. У цьому налаштуванні виконавчі механізми отримують сигнали від датчиків і, залежно від контексту, виконують такі

дії, як замикання або відмикання дверей, увімкнення та вимкнення світла чи електричних пристроїв, регулювання температури в будинку або встановлення сигналів тривоги для надзвичайних ситуацій. По суті, приводи реагують на команди та виконують їх на основі сигналів, які вони отримують від датчиків або інших пристроїв.

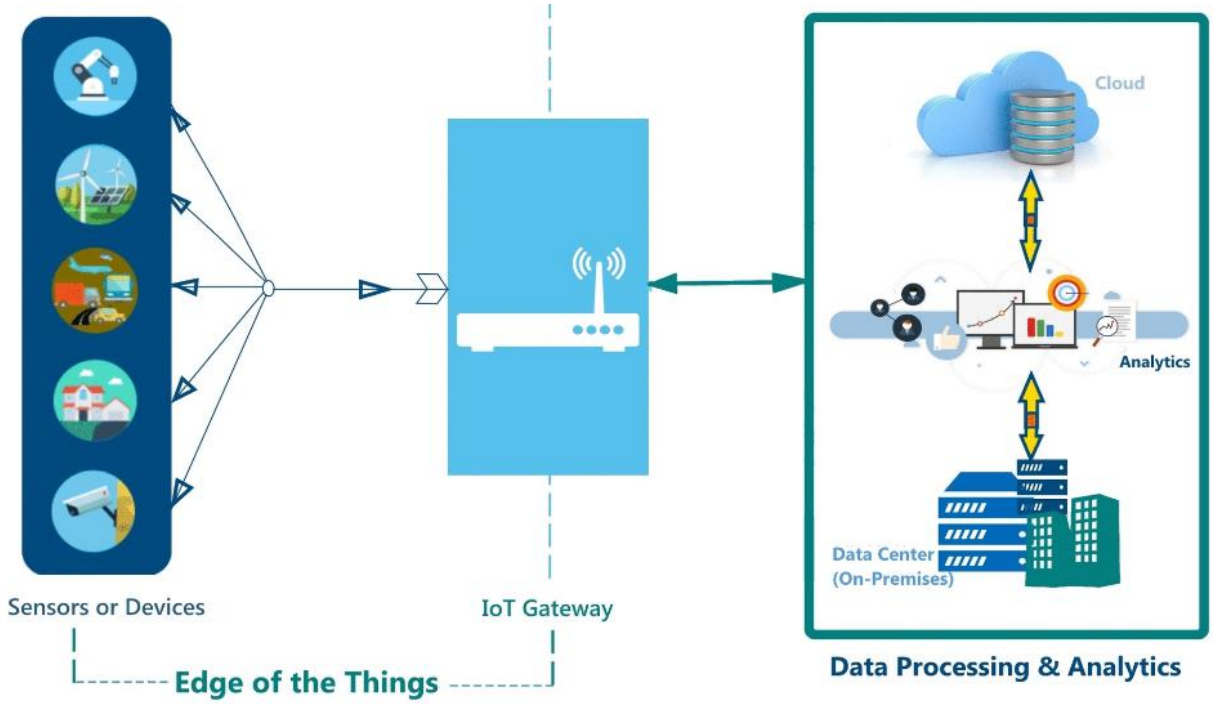

Рис. 2.4. Загальна екосистема Інтернету речей

Іншим важливим аспектом IoT є керування значним обсягом даних, які постійно генеруються та обмінюються між пристроями IoT. Зберігання цих даних є серйозною проблемою в мережах IoT. Крім того, дані, зібрані з цих пристроїв, повинні пройти фільтрацію, обробку та аналіз для забезпечення ефективного функціонування системи IoT. У цьому процесі шлюзи, хмарні служби та аналітика співпрацюють, щоб виконувати завдання зберігання та обробки даних.

2.2. Шлюз

Шлюзи, призначені для спрощення системи IoT, функціонують як проміжне середовище зв'язку між пристроями та центральною хмарною системою.

Основні функції шлюзів IoT перераховані нижче:

- Попередня обробка даних

  Шлюз IoT слугує посередником між сенсорними пристроями та центральною хмарою, проводячи базову аналітику даних перед тим, як передавати інформацію безпосередньо в хмару. Цей рівень виконує завдання локальної фільтрації даних, очищення, попередньої обробки

та перекладу протоколів. Під час цього процесу він також може агрегувати, видаляти дублікати або підсумовувати дані, щоб збільшити час відгуку та знизити витрати на передачу.

- Збирання даних

  На цьому рівні дані збираються з кількох джерел, перетворюються в потрібний формат, а потім передаються на рівні обробки. Роль шлюзу на цьому етапі полягає в забезпеченні безпечного зв'язку між пристроями IoT і структурами обробки.

- Пересилання даних і тимчасове зберігання

  Основна роль шлюзу полягає в забезпеченні безпечного передавання даних між сенсорним рівнем і центральною хмарою. Крім того, цей рівень слугує тимчасовим сховищем для зібраних даних.

- Керування пристроєм

  Цей рівень полегшує конфігурацію пристрою в режимі реального часу, дозволяючи коригувати статуси пристрою, режими роботи, підтвердження помилок тощо.

- Діагностика

  Шлюз IoT визначає помилки та несправності в межах усього технологічного рівня, включаючи самодіагностику для самого шлюзу IoT.

2.3. Зберігання та аналітика даних

2.3.1. Хмара

Хмара є центром мережі IoT, беручи на себе ключові ролі в обробці, зберіганні та управлінні даними. Ключові характеристики хмари включають здатність зберігати та обробляти велику кількість даних, створених пристроями, масштабованість для легкої роботи з тисячами пристроїв, гнучкість, що дозволяє додавати або видаляти пристрої за потреби, не вимагаючи повної реконфігурації системи, нагляду та керування з боку постачальника хмарних послуг і економічну ефективність.

Хоча хмарні послуги не є обов'язковими для IoT, останній перехід до периферійних і туманних обчислень розширює можливості локальної обробки даних. Тим не менш, хмару, як правило, включають в систему для її масштабованості, зберігання та економічно ефективного надання послуг [28]. Крім того, хмарні сервіси пропонують такі функції безпеки, як шифрування та автентифікація, одночасно забезпечуючи віддалений доступ і керування пристроями IoT.

2.3.2. Аналітика

Найбільш складним і важливим рівнем в IoT є аналітика. Він передбачає аналіз даних, отримання цінних ідей за допомогою різноманітних алгоритмів машинного навчання (ML) і методів статистичного аналізу. Численні застосування аналітики в IoT охоплюють виявлення аномалій, моніторинг навколишнього середовища, управління енергією, розумні міста та сільське господарство [29].

2.3.3. Інструменти інтерпретації та візуалізації

Цей сегмент по суті служить інтерфейсом користувача (UI). Інтерфейс користувача пропонує користувачам платформу для безпосередньої взаємодії з додатком або системою, полегшуючи спілкування. Інтерфейс користувача не завжди залежить від екрану. Наприклад, пульт дистанційного керування телевізором використовує інтерфейс користувача з кількома кнопками, тоді як такі пристрої, як Amazon Echo, реагують на голосові команди для керування. Отримання автоматичного сповіщення, профілактичний моніторинг інформації та дистанційне керування системою є деякими типовими прикладами інтерфейсів користувача в системах IoT.

3. Архітектура IoT

Архітектура – це структурована основа, що відображає матеріальні компоненти мережі, їх робоче розташування і налаштування, основні принципи і структури, а також спосіб організації та використання даних у процесі функціонування. Архітектура Інтернету речей складається з набору пристроїв, датчиків, виконавчих механізмів, кінцевих користувачів, хмарних сервісів і, найголовніше, різних рівнів зв'язку та протоколів Інтернету речей.

Всі системи IoT за своєю суттю дотримуються загальної трирівневої архітектури. Однак, виходячи з потреб або специфічних вимог застосування, загальна модель може бути модифікована додаванням додаткових шарів, утворюючи таким чином чотири- або п'ятишарові архітектури [42].

Архітектуру IoT можна поділити на два види: багаторівнева архітектура і архітектура для конкретної галузі. У цьому розділі ми навели загальну архітектуру IoT.

IoT має багаторівневу архітектуру, яка належить до структурованої основи, що використовується для проектування і організації різних компонентів і функцій системи IoT. Ця архітектура складається з декількох рівнів, кожен з яких має свою специфічну роль і обов'язки, що дозволяє забезпечити ефективний зв'язок, обробку даних і управління в екосистемі IoT. Типові шари в архітектурі IoT включають *рівень сприйняття, мережевий рівень і рівень застосування*. Ці рівні співпрацюють для забезпечення безперебійної роботи пристроїв IoT, передавання даних і надання послуг IoT кінцевим користувачам.

Відповідно до цієї узагальненої архітектури, також відомої як *трирівнева архітектура*, систему IoT поділяють на такі три рівні:

- прикладний рівень,
- мережевий рівень
- рівень сприйняття.

Кожному з цих рівнів притаманні певні проблеми з безпекою.

Візуальне представлення загальної трирівневої архітектури показано на рис. 3.1.

1. *Рівень сприйняття* (*Perception Layer:*) Рівень сприйняття, також відомий як сенсорний рівень, є фундаментальним рівнем архітектури IoT. Цей рівень взаємодіє з розумними пристроями, включаючи, але не обмежуючись розумними годинниками і розумними кільцями, використовуючи масив датчиків і виконавчих механізмів. Основними завданнями цього рівня є збирання даних з цих інтелектуальних пристроїв за допомогою датчиків і подальше передавання отриманих даних на верхній рівень, відомий як мережевий рівень.

2. *Мережевий рівень (Network Layer):* Мережевий рівень, також відомий як рівень передачі, є середнім рівнем архітектури IoT [63]. Цей рівень відповідає за отримання інформації з рівня сприйняття і визначення маршрутів для передавання оброблених даних до різних підключених пристроїв і додатків Інтернету речей за допомогою інтегрованих мереж, таких як дротові або бездротові захищені з'єднання. Мережевий рівень є основним рівнем трирівневої архітектури IoT, оскільки він використовує різні пристрої, такі як пристрої маршрутизації, шлюзи, комутатори і концентратори, і управляє ними за допомогою різних технологій зв'язку, таких як WiFi, Bluetooth, 3G, LTE, Zigbee тощо. Отже, мережевий рівень відповідає за передавання даних до і від декількох додатків через інтерфейси і шлюзи з використанням різних комунікаційних технологій і протоколів.

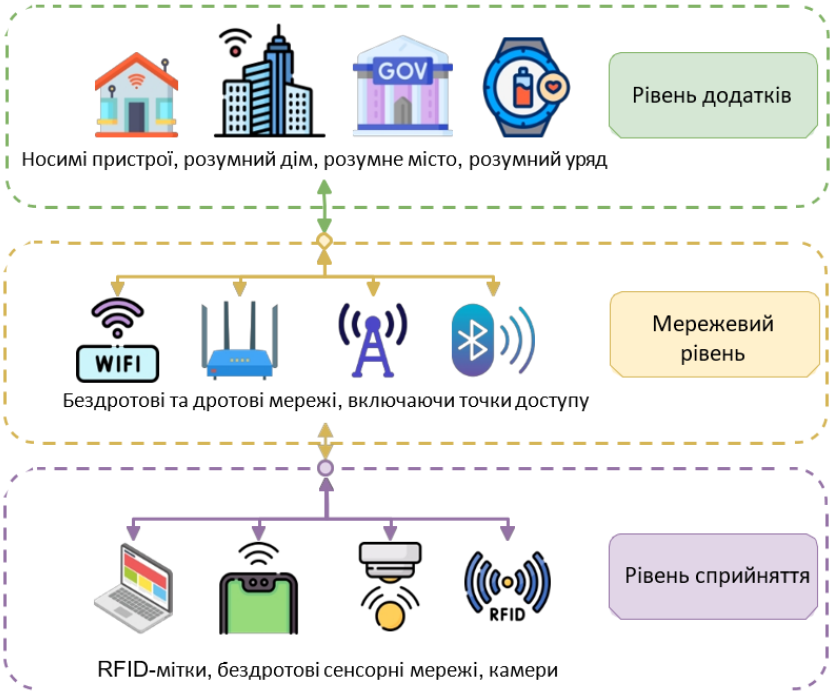

Рис. 3.1: Загальна архітектура Інтернету речей

3. *Рівень додатків (Application Layer):* В ерхнім рівнем в архітектурі IoT, є рівень додатків або бізнес-рівень. Цей рівень має завдання агрегувати дані з мережевого рівня, для створення розумного середовища – кінцевої мети парадигми IoT. Цей рівень вміщує різноманітний набір додатків, кожен з яких характеризується власними вимогами. Прикладами таких додатків є розумні мережі, розумні міста та розумний транспорт. Крім того, цей рівень бере на себе відповідальність за підтримку автентичності, цілісності та конфіденційності даних [64].

Трирівнева архітектура є узагальненою та найпоширенішою архітектурою. Однак, хоча вона й видається простою на перший погляд, функціональність мережевого та прикладного рівнів іноді може бути складною. Наприклад, мережевий рівень не лише відповідає за передавання даних, але й надає послуги з обробки даних, такі як агрегація та обробка даних тощо. З іншого боку, прикладний рівень не лише відповідає за надання послуг клієнтам і користувачам, але й забезпечує аналіз даних, проводить інтелектуальний аналіз даних тощо.

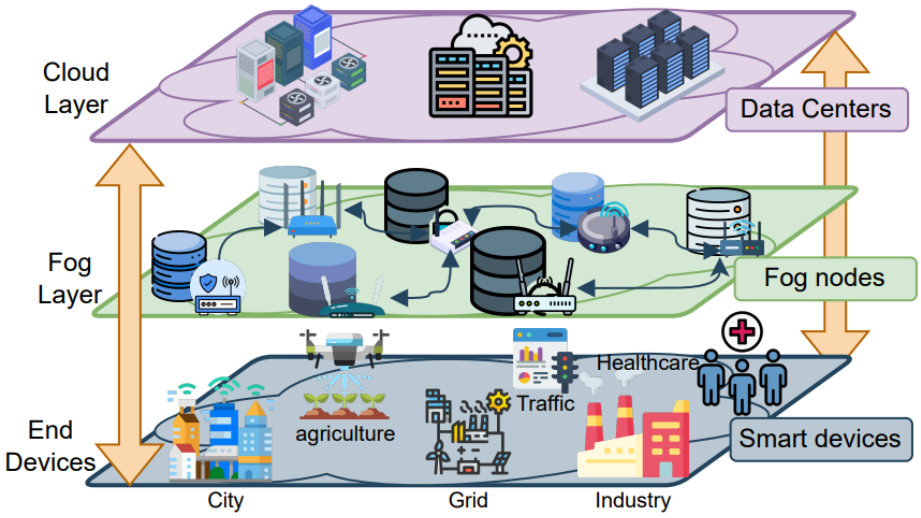

Рис. 3.2. Порівняння хмарної архітектури із архітектурою, що базується на туманних обчисленнях

Тому у відповідь на конкретні виклики були включені додаткові рівні, що ґрунтуються на фундаментальних рівнях. Наприклад, чотиришарові або п'ятишарові архітектури підвищують гнучкість системи. Тим не менш, тришарова архітектура є основою для всіх цих варіацій. Крім того, додатки нового покоління характеризуються коротшим часом відгуку і низьким споживанням енергії, оскільки пристрої Інтернету речей мають обмежену потужність. Тому дослідники використовували шари туману та хмари, які візуалізовані на рис. 3.2.

4. Ключові технології IoT

Для роботи IoT потрібні різноманітні технології, які розгортаються на різних рівнях архітектури IoT, і існує багато різних видів технологій, зокрема апаратні технології, програмні технології і, що найбільш важливо, комунікаційні технології. У цьому розділі розглядаються найважливіші технології IoT, які використовуються для забезпечення успішної роботи системи IoT. На рис.4.1 зображено таксономію технологій IoT.

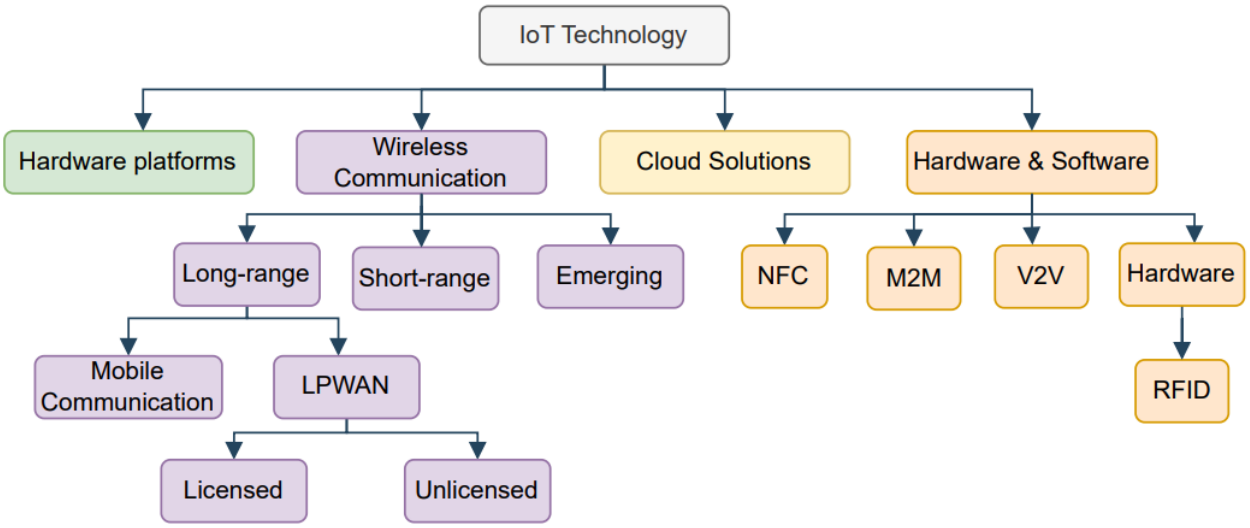

Рис. 4.1: Технологічна таксономія Інтернету речей

4.1. Апаратні платформи

Основними компонентами системи IoT є пристрої, прикріплені до датчиків або носимих пристроїв, які використовуються для збирання даних. Тому для побудови цих сенсорних пристроїв використовуються різні типи апаратних платформ. Перед вибором апаратної платформи необхідно врахувати кілька ключових моментів, такі як призначення пристрою Інтернету речей або тип підключення, якого він потребує.

Дві найбільш доступні та популярні апаратні платформи - це Raspberry Pi та Arduino. Обидві вони мають потужні можливості збирання, обробки та зберігання даних і забезпечують як бездротове, так і дротове підключення. Однак, з точки зору управління енергоспоживанням, Arduino перевершує Raspberry Pi, оскільки Raspberry Pi не містить режимів сну або призупинення для використання енергії, в той час як Arduino має такі режими [67]. Intel Galileo Gen та Intel Edison є прикладами використання IDE Arduino.

4.2. Технологія бездротового зв'язку

З огляду на величезну кількість пристроїв в існуючій мережі Інтернету речей і очікування ще більшої кількості різноманітних підключених пристроїв в майбутньому, існує потреба в розробці різних технологій для полегшення їх підключення. У цьому підрозділі розглядаються існуючі бездротові технології, призначені для підключення до Інтернету речей, і класифікуються на три групи.

4.2.1. Технології малого радіуса дії

Технології малого радіуса дії зазвичай використовують у системах Інтернету речей для забезпечення зв'язку між пристроями в межах обмеженої близькості. Ці технології добре підходять для сценаріїв, коли пристрої повинні обмінюватися даними в межах невеликої зони покриття, зазвичай від кількох метрів до кількох кілометрів. Існує кілька технологій малого радіуса дії, кожна з яких має унікальні характеристики та переваги, придатні для конкретних цілей. У Табл. 4.1 наведено всебічний огляд різних технологій малого радіуса дії, що використовуються в середовищі Інтернету речей, згрупованих за різними параметрами, такими як частотний діапазон, швидкість передачі даних, дальність передавання тощо. У таблиці наведено технічні характеристики Bluetooth, ZigBee, Wi-Fi, LR-WPAN, VLC і BS-ILC.

Таблиця 4.1

Порівняння популярних технологій малого радіуса дії на основі різних параметрів.

Параметри	Bluetooth	ZigBee	LR-WPAN	Wi-Fi	OWC	
					VLC	BS-ILC
Стандартний	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.11a/b/c/ d/g/n/ac/ah	IEEE 802.15.7m IEEE 802.15.13	LoRaWAN
Діапазон частот	1 МГц - 2,48 ГГц	В основному на 2,4 ГГц Опціонально 868 МГц або 915 МГц	868/915 МГц, 2,4 ГГц	a: 5 ГГц, b: 2,4 ГГц, g: 2,4 ГГц, n: 2,4 ГГц 802.11ah: 1/2/16 МГц	400-800 ТГц	Залежить від регіону, Європа: 868 МГц США: 915 МГц
Швидкість передачі даних	1 Мбіт/с - 3 Мбіт/с	20 кбіт/с до 250 кбіт/с	40-250 кбіт/с	a: 54 Мбіт/с, b: 11 Мбіт/с, g: 54 Мбіт/с, ah: 300 Мбіт/с n: 600 Мбіт/с, ac: 7 Гбіт/с	15.13: мультигігабітний Нещодавно: 100 Гбіт/с	100 Гбіт/с
Діапазон передачі	Класичний: 100м BLE: 240м	10-100 метрів	10-100 метрів	від 100 м до 1 км	Зазвичай, в межах кімнати 7м: 200 метрів 15.13: Кілька метрів	200 метрів
Споживання енергії	Класичний: високий BLE: Низький.	Низький	Низький	Від помірного до високого	Передавачі: Помірні Одержувачі: Мінімально	Дуже низький
Вартість	Економічно ефективний	Економічно ефективний	Економічно ефективний	Від помірного до високого	від помірного до високого	Економічно ефективний
Протокол RA	FHSS, FDMA Опитування на основі TDMA	CSMA/CA	CSMA/CA	CSMA/CD, CSMA/CA	CSMA/CA, TDMA/CDMA	LBT
Тип модуляції	GFSK, DQPSK, π/4-DQPSK	BPSK/O-QPSK	BPSK/O-QPSK	BPSK/QPSK/QAM	OOK/PPM/OFDM	CSS

Таблиця 4.2

Порівняння популярних технологій далекого радіуса дії за різними параметрами

Технології / Параметри	2G	Технологія мобільного зв'язку			WiMax	ТЕХНОЛОГІЇ LPWAN			
		3G	4G	5G		НЕЛІЦЕНЗІЙНИЙ LPWAN		ЛІЦЕНЗІЙНИЙ LPWAN	
						LoRa	Sigfox	LTE-M	NB-IoT
Стандартний	GSM, CDMA	UMTS, CDMA2000	LTE, LTE-A, IEEE 802.16	5G NR, Wi-Fi 6 (802.11ax)	IEEE 802.16	LoRaWAN R1.0	Власна технологія	3GPP LTE	3GPP LTE
Діапазон частот	850 МГц, 900 МГц, 1800 МГц, 1900 МГц	850 МГц, 1900 МГц, 2100 МГц	700 МГц, 1700/2100 МГц, 2500 МГц	60 МГц - 80 ГГц	2,3 ГГц, 2,5 ГГц, 3,5 ГГц	Неліцензійні діапазони ISM, 125 кГц, 250 кГц	Неліцензійні діапазони ISM, 100 Гц	Ліцензовані діапазони LTE, 1,4 МГц	Ліцензовані діапазони LTE, 200 кГц
Швидкість передачі даних	9Kbps - 384Kbps	384Kbps - кілька Мбіт/с	100 Мбіт/с - 1 Гбіт/с	1 Гбіт/с - 20 Гбіт/с або вище	16d: 75 Мбіт/с 16e: 1 Гбіт/с	0,3 Кбіт/с - 50 Кбіт/с	100bps - 600bps	300bps - 1Mbps	200 кбіт/с - 250 кбіт/с
Діапазон передачі	кілька кілометрів	кілька кілометрів	кілька кілометрів	кілька кілометрів	кілька кілометрів	До міста: 5 км Сільська місцевість: 20 км	До міста: 10 км Сільська місцевість: 50 км	До міста: 1 км Сільська місцевість: 10 км	кілька кілометрів
Енергоспоживання	низький	Помірний	Помірний до високого	Низький (Енергетичний) ефективний)	високий	Надзвичайно низький	Низький	Помірний	Низький
Протокол RA	TDMA/ CDMA/ FDMA	CDMA/ WCDMA	OFDMA / SC-FDMA	Масивний MIMO/ формування променя/ CP-OFDM	OFDMA/ TDD/FDD	ALOHA/ Щілинний - ALOHA	ALOHA	Щілинний - ALOHA	Щілинний - ALOHA
Тип модуляції	GMSK/QPSK	QPSK/16-QAM	OFDM/QPSK/ 16-QAM/64-QAM/ 256-QAM	256-QAM	OFDM, QPSK, 16-QAM, 64-QAM	CSS	GFSK/DBPSK	QPSK/QAM/ BPSK	QPSK/BPSK
Вартість	Економічно ефективний	Помірний	Високий	Високий	Високий	Економічно ефективний	Залежить від модель підписки	Від помірного до високого	Від помірного до високого

Bluetooth, ZigBee, LR-WPAN і BS-ILC пропонують економічно ефективні комунікаційні рішення, тоді як загальна вартість Wi-Fi і VLC може змінюватися залежно від використання. Що стосується частотних діапазонів, то більшість технологій працюють у діапазоні 2,4 ГГц, за винятком VLC, який використовує набагато ширший діапазон частот. Частота BS-ILC залежить від регіону. VLC і BS-ILC надають пріоритет досягненню високих швидкостей передачі приблизно 100 Гбіт/с, в той час як швидкість передачі Wi-Fi може відрізнятися в різних стандартах. Примітно, що VLC і BS-ILC демонструють дуже низьке споживання енергії, як показано в Табл. 4.2.

4.2.2. Технології далекого радіуса дії

Технології далекого радіуса дії, призначені для передавання даних або сигналів на значні відстані, як правило, діють набагато далі, ніж технології ближнього радіуса дії, такі як Bluetooth або Wi-Fi. Технології далекого радіуса дії широко використовуються в різних сферах, таких як бездротовий зв'язок на великі відстані, віддалений моніторинг, відстеження тощо, і є важливими для сценаріїв, коли необхідно надійно передавати дані на великі географічні території.

Ці технології можна розділити на дві основні категорії: технології мобільного зв'язку та технології LPWAN. У Табл. 4.3 представлено детальний огляд різних технологій далекого радіуса дії, що використовуються в середовищі IoT. Вона містить короткий огляд технічних специфікацій різних версій технологій мобільного зв'язку, а також різних версій технологій LPWAN.

З таблиці видно, що технології мобільного зв'язку 2G, 3G і 4G працюють у діапазоні частот приблизно від 850 МГц до 2100 МГц, тоді як 5G використовує набагато ширший діапазон частот – до 80 ГГц. Крім того, з усіх п'яти технологічних варіантів 5G пропонує найвищу швидкість передавання даних, що перевищує 20 Гбіт/с. З погляду енергоефективності як 2G, так і 5G мають низькі показники споживання, тоді як WiMax демонструє високе енергоспоживання.

Однак варто зазначити, що технології 3G-5G потребують більших витрат на впровадження. У категорії неліцензійованої LPWAN головними претендентами є LoRa і Sigfox, тоді як найбільш перспективними варіантами в ліцензійованій технології LP- WAN є LTE-M (Long-Term Evolution for Machines) і NB-IoT (Narrowband IoT). Ключова відмінність, підкреслена в таблиці, полягає в тому, що технологія UNLICENSED LPWAN працює в межах неліцензійних спектральних ресурсів, що призводить до зниження витрат на розгортання, тоді як технологія LICENSED LPWAN покладається на ліцензовані спектральні ресурси, що призводить до відносно вищих витрат як на пристрої, так і на розгортання.

4.2.3. Нові можливості для масового підключення

Хоча сучасні бездротові технології Інтернету речей досягли певних успіхів у підтримці різних додатків Інтернету речей, вони все ще стикаються з проблемами у задоволенні можливих майбутніх потреб в цій сфері. Наприклад, забезпечення

зв'язку між великою кількістю пристроїв Інтернету речей з обмеженим корисним навантаженням і декількома протоколами випадкового доступу, що використовуються в існуючих технологіях, часто призводить до значних проблем, таких як часті колізії доступу, збільшення затримок і велика кількість накладних витрат на передавання сигналів для пристроїв IoT. Крім того, обмежена доступність бездротових ресурсів для підключення пристроїв Інтернету речей створює дефіцит і неефективне використання цих ресурсів. Тобто, існує безліч поточних ініціатив, спрямованих на подолання обмежень поточних технологій. Серед них найбільш перспективними є рішення CS, NOMA, mMIMO та ML.

Ці нові технології пропонують можливість не лише підтримувати масовий зв'язок, але й забезпечити високу надійність і низьку затримку передавання даних. Однак важливо визнати, що існують певні проблеми та обмеження, які необхідно вирішити для їх ефективного впровадження. Очікується, що розвиток ще більш досконалих технологій дозволить вирішити критичні проблеми IoT. Водночас зусилля повинні бути зосереджені на розумній інтеграції існуючих і нових технологій для розкриття їхнього повного потенціалу та оптимізації продуктивності системи.

4.3. Хмарні рішення

Хмарні рішення IoT пропонують різні послуги, такі як збирання даних у режимі реального часу, передавання даних, моніторинг, аналіз даних, покращене прийняття рішень та управління пристроями. Ці послуги надаються за принципом "плати за користування", що дозволяє користувачам платити лише за ті послуги, якими вони фактично користуються. Хмарні платформи можуть бути інтегровані в численні сфери, включаючи охорону здоров'я, розумні міста, сільське господарство, освіту та управління ланцюгами поставок. Для простоти в Табл.4.3. представлено кілька популярних платформ.

Таблиця 4.3

Популярні хмарні рішення IoT

Хмарна IoT платформа	Провайдер	В режимі реального часу	Візуалізація даних	Тип хмарного сервісу	Аналітика даних	Вартість розробки
ThingSpeak	MathWorks	Так	Так (Matlab)	Громадськість	Так	Безкоштовно
Plotly	Plotly Technologies Inc.	Так	Так	Громадськість	Так	Безкоштовно
Carriots	Altair	Так	Так	Рядовий	Ні	Обмежено до: 10 пристроїв
Exosite	Exosite	Так	Так	IoTSaaS	Так	2 пристрої
GroveStreams	GroveStreams LLC	Так	Так	Рядовий	Так	Обмежено до: 20 потоків, 10K транзакцій, 5 SMS, 500 електронних листів
ThingWorx	PTC	Так	Так	Рядовий	Так	Оплата за використання
Nimbits	З відкритим вихідним кодом	Так	Так	Гібрид	Ні	Безкоштовно

4.4. Технології апаратного та програмного забезпечення

Ця категорія охоплює низку апаратних і програмних технологій, що відповідають за різні аспекти каналів зв'язку IoT. Деякі технології, такі як NFC і M2M, вважаються як апаратними, так і програмними технологіями, тоді як RFID класифікується як виключно апаратна технологія. Розглянемо їх детальніше.

4.4.1. RFID

RFID – це технологія, яка складається з одного або декількох зчитувачів і декількох RFID-міток. Ці мітки – це маленькі мікрочіпи, що мають унікальні коди і можуть бути на таких предметах, як товари в магазині або навіть картки доступу. Коли пристрій для зчитування RFID посилає електромагнітні радіохвилі, мітки відповідають своїми унікальними електронними кодами товару (EPC) [14]. Зчитувач фіксує ці коди і надсилає їх на комп'ютер, який потім може з'ясувати, до чого належать мітки. Цю технологію використовують у різних сферах, наприклад, для відстеження запасів у магазинах, надання доступу до захищених зон або моніторингу пакунків під час їхнього переміщення в процесі доставки.

4.4.2. Бездротовий зв'язок ближнього радіуса дії (NFC)

NFC, розширення технології RFID – це технологія бездротового зв'язку малого радіуса дії, яка використовує індукцію магнітного поля для встановлення зв'язку між пристроями, коли вони знаходяться в безпосередній близькості один від одного без необхідності попереднього встановлення з'єднання. Чіпами NFC оснащені більшість сучасних телефонів, які підтримують такі додатки, як Apple Pay та Google Pay. NFC працює в неліцензованому діапазоні радіочастот на частотах 13,56 МГц. Її типовий діапазон становить близько 20 метрів, при цьому фактична відстань часто визначається розміром антени в пристрої. Очікується, що технологія NFC відіграватиме життєво важливу роль у майбутньому Інтернету речей, забезпечуючи бездротове з'єднання з іншими "розумними" об'єктами. Наприклад, вже сьогодні, використовуючи NFC на мобільному пристрої, користувач може перетворювати свій телефон на різні об'єкти, зокрема використовувати його як кредитну картку для здійснення транзакцій.

4.4.3. M2M

M2M-комунікація набуває все більшої популярності і передбачає прямий зв'язок між комп'ютерами, вбудованими процесорами, інтелектуальними датчиками, виконавчими механізмами та мобільними пристроями.

Він складається з чотирьох основних компонентів: зондування, різнорідний доступ, обробка інформації, а також застосування та обробка. З практичного погляду, M2M функціонує в рамках п'яти компонентів: пристрій для реагування на

запити, шлюзи для взаємодії та з'єднання, територіальна мережа для забезпечення зв'язку між пристроями та шлюзами, додатки, що слугують проміжним програмним забезпеченням, та комунікаційна мережа для полегшення зв'язку між шлюзами та додатками. Технологія M2M застосовується в різних секторах, включаючи охорону здоров'я, розумну робототехніку, кібернетичні транспортні системи (КТС), виробничі системи, технології "розумного будинку" та "розумні" мережі [15].

4.4.4. Зв'язок між транспортними засобами (V2V)

V2V Communications розглядає кожен транспортний засіб як вузол і забезпечує всенапрямлений бездротовий обмін даними між транспортними засобами щодо їхньої швидкості, місцезнаходження тощо. Транспортні засоби, оснащені відповідним програмним забезпеченням, яке часто називають додатками безпеки, можуть використовувати повідомлення від сусідніх транспортних засобів для виявлення потенційних ризиків зіткнення в режимі реального часу.

Існує два типи зв'язку в цій мережі: один – між транспортними засобами, а інший – через дорожню інфраструктуру. Однак структура або організація цього зв'язку є гнучкою, оскільки транспортні засоби переміщуються з одного місця в інше. Цю мережу можна поділити на чотири основні категорії: *безпека та уникнення зіткнень*, *управління дорожньою інфраструктурою*, *телематика транспортних засобів* та розважальні *послуги з підключенням до Інтернету* [15].

5.Застосування IoT

IoT був ефективно інтегрований у різні сфери, що призвело до розроблення інтелектуальних додатків. Хоча деякі з цих додатків вже доступні, інші все ще перебувають на стадії дослідження. Тим не менш, суть цих додатків вказує на те, що Інтернет речей покликаний покращити життя людей, надаючи їм зручності й гнучкості.

Рис. 5.1: Галузі застосування Інтернету речей

Коротко розглянемо сфери людського життя, де вже впроваджено технологію Інтернету речей.

5.1. Розумні міста

Концепцію розумних міст можна розглядати як комплексну парадигму Інтернету речей, де управління державними справами передбачає впровадження рішень на основі інформаційно-комунікаційних технологій (ІКТ). Розумне місто використовує державні ресурси для оцифрування міста та підвищення якості життя. Реальним прикладом реалізації "розумного міста" є "Падова Смарт Сіті", яке було впроваджено в місті Падова, Італія. Барселона та Стокгольм є двома яскравими прикладами "розумних" міст. У Барселоні розпочато проект CityOS, основною метою якого є створення централізованої операційної системи для управління всіма "розумними" пристроями та послугами, доступними в місті. Основну увагу було зосереджено на вдосконаленні "розумного" транспорту та систем водопостачання. Аналогічно, Стокгольм також приділяє значну увагу цим двом сферам і має честь бути одним з перших міст, які впровадили концепцію плати за затори, коли користувачі платять за в'їзд у перевантажені райони.

Нові технології IoT використовуються для розвитку розумних міст у розумному управлінні автопарком, моніторингу якості повітря, енергоменеджменті та потребах розумного сільського господарства за допомогою датчиків, роботів та інших кіберфізичних систем. Усі дані, отримані в цьому процесі, надсилаються до хмари (центральної платформи) для обробки, а отримані результати використовуються для планування стратегій розумного міста [45].

У контексті Індустрії 4.0 поєднання розумних міст з Інтернетом речей і штучним інтелектом може призвести до взаємовигідних результатів. Надзвичайно важливими в розумних містах є системи моніторингу: наприклад, уряд Сінгапуру модернізував свою систему освітлення, щоб забезпечити інтелектуальне керування часом затемнення та ввімкнення. Він також зменшує потужність освітлення шляхом модернізації світлодіодних установок. Автоматизована система зчитування лічильників (AMR) використовується для надання зворотного зв'язку щодо використання води, а також для моніторингу потенційних витоків у режимі реального часу. Також технологія, яка також широко використовується в Сінгапурі, це розумне управління відходами. В межах програми розумного поводження з відходами монітори на кришках контейнерів збирають інформацію про вміст і розташування та передають інформацію команді з утилізації відходів через центральний сервер. Потім можна оптимізувати маршрут команди збирання відходів.

Загалом варто зазначити, що Сінгапур є безперечним піонером та лідером у русі розумних міст і є найрозумнішим містом у світі згідно з першим Індексом розумних міст IMD.

Ініціативу «Розумна нація» започаткував в 2014 році прем'єр-міністр Лі Сянь Лун, а через три роки, було отримано від уряду інвестицію у розмірі 2,4 мільярда сингапурських доларів (тоді еквівалентно 1,73 мільярда доларів США). Було запроваджено широкий спектр розумних технологій як у державному, так і в приватному секторах. Мета цього проєкту полягала в тому, щоб створити місто, що грунтується на цифрових інноваціях і технологіях, яке відповідає потребам громадян, що постійно змінюються.

Одним з ключових напрямів, на який було орієнтовано цю програму, став транспорт, адже у Сінгапурі з високою щільністю забудови земля є надзвичайно дорогою, і лише 12% площі відведено під транспортну інфраструктуру. Щоб оптимізувати ефективність транспорту, використовуючи сенсорні технології, Агентство з науки, технологій і досліджень створило автономний автопарк , щоб допомогти людям похилого віку та жителям з обмеженими можливостями залишатися мобільними. Водночас студенти Національного університету Сінгапуру можуть пересуватися кампусом на безпілотному шатлі.

Місто-держава має електронну систему ціноутворення на дорогах, яка використовує дані про дорожній рух у реальному часі для коригування ставок плати за проїзд та керування заторами.

Для оптимізації транспорту використовуються загальнодоступні або «відкриті дані», на базі яких створені цифрові двійники, що використовуються для випробувань та полегшення транспортного планування. Аналізуються дані з платіжних карток до датчиків у понад 5000 транспортних засобів і відстеження автобусів у реальному часі. Це дало можливість знизити рівень переповненості автобусів на 92%.

Технологія безконтактних платежів використовується для оптимізації пересування та платежів 7,5 мільйонів пасажирів, які щодня користуються громадським транспортом. Як і у все більшій кількості міст, пасажири можуть платити за допомогою безконтактних карток або мобільних гаманців.

Програма Travel Smart спрямована на більш рівномірний розподіл попиту на поїздки в ранкові години пік на залізничній мережі трьома способами: заохочення громадян до переосмислення того, коли вони подорожують, як вони подорожують (наприклад, пересідають на велосипеди) та зменшення кількості поїздок (заохочення роботи віддалено).

Розглянемо в загальному типи задач, важливі для розумних міст, які можуть використовувати IoT.

Структурний стан будівель

Ця послуга передбачає безперервний моніторинг ділянок, схильних до впливу різних зовнішніх факторів, і вимірювання стану будь-якої будівлі. Датчики Інтернету речей, підключені до будівель, можуть зберігати інформацію про міцність будівлі, що допомагає зробити аналіз та визначити, наскільки міцною є будівля або чи потребує вона якихось доопрацювань. Залежно від призначення, можна використовувати різні типи датчиків, зокрема для відстеження вібрацій, щоб виміряти навантаження на будівлю, датчики температури та вологості або інші типи атмосферних датчиків для оцінювання рівня забруднення в певній місцевості. Використання Інтернету речей у цій сфері може зменшити обсяг ручної праці, коли люди повинні вручну оцінювати стан будівлі та умови навколишнього середовища, а також значно знизити загальні витрати на цей процес.

Управління відходами

Утилізація відходів є важливою операцією в будь-якому місті, незалежно від того, чи вважається воно "розумним" чи ні, оскільки вона безпосередньо впливає на придатність території для життя. Таким чином, ефективна система управління відходами має важливе значення для будь-якого суспільства. Інтеграція Інтернету речей в управління відходами пропонує безліч переваг. Вона дозволяє виявляти рівень відходів і відстежувати маршрути сміттєвозів у режимі реального часу, що призводить до більш ефективного планування маршрутів. Крім того, це може впорядкувати ручну працю, пов'язану з розділенням відходів, і контролювати процес утилізації. Датчики на сміттєвозах під'єднані до центральної програмної

системи, досягають цих завдань, аналізуючи та контролюючи систему на основі зібраних даних. Такий підхід зменшує витрати на ручні процеси та покращує управління переробкою [45].

Моніторинг якості повітря та шуму

Створення здорового та безпечного середовища для всіх живих істот має вирішальне значення, а моніторинг якості повітря та рівня шуму в будь-якій місцевості є ключовою частиною досягнення цієї мети. Різноманітні екологічні датчики, зокрема датчики ґрунту, температури та вологості, а також газові датчики, можуть виявляти наявність токсичних і забруднюючих речовин у повітрі та оцінювати рівень забруднення. Ця інформація дозволяє місцевій владі контролювати рівень забруднення, впроваджувати ефективні заходи для його зниження, виявляти сильно забруднені або токсичні райони та визначати відповідні місця для активного відпочинку на свіжому повітрі. Так само важливо підтримувати збалансований рівень шуму для всіх живих істот у суспільстві, включаючи людей і тварин. Використовуючи датчики шуму для вимірювання рівня децибел, центральний орган влади може збирати дані для виявлення шумних зон і регулювати рівень шуму, щоб утримувати його в прийнятних межах [45].

Розумний транспорт і затори на дорогах

У сучасному світі затори на дорогах є значною проблемою, яка впливає майже на кожну країну та місто, особливо зважаючи на те, що більше половини населення планети зараз проживає в містах. Щоб вирішити цю проблему, багато міст впровадили рішення Інтернету речей для створення розумних транспортних систем, спрямованих на управління заторами на дорогах. Ці ініціативи включають розумні світлофори та розумні системи паркування, які разом збільшують пропускну спроможність транспорту, підвищують безпеку та швидкість руху для пасажирів. Основними перевагами розумних транспортних систем є зменшення заторів на дорогах, забезпечення безперешкодного пересування та полегшення паркування. Крім того, ці системи дозволяють швидше реагувати на аварії та сприяють зниженню аварійності завдяки ефективному управлінню транспортними потоками [45]. Цих цілей досягають завдяки використанню різноманітних сенсорних технологій, включаючи акселерометри для вимірювання швидкості, RFID-мітки для ідентифікації транспортних засобів, GPS-датчики для відстеження місцезнаходження, гіроскопи для визначення напрямку руху та камери для запису дорожнього руху та переміщення транспортних засобів. Деякі реальні застосування цих сенсорів можна побачити в додатках для управління та моніторингу дорожнього руху [15], додатках для забезпечення безпеки та додатках для виявлення аварій.

Розумна енергетика

Традиційна енергосистема – це електрична мережа, яка включає лінії електропередач, трансформатори та різноманітні комунікації, що відповідають за

доставку електроенергії від електростанцій до домівок чи підприємств. Одним із суттєвих обмежень традиційної електромережі є її односторонній зв'язок, що не дозволяє електростанціям ефективно реагувати на зростаючий попит на електроенергію з боку споживачів. Для вирішення цієї проблеми розумна мережа встановлює двосторонній зв'язок між комунальними підприємствами та споживачами, що дозволяє ефективніше управляти економічними, стійкими та безпечними енергетичними ресурсами. Інтеграція Інтернету речей в енергосистеми дозволяє обладнати будинки та підприємства розумними лічильниками, які контролюють виробництво, зберігання та споживання енергії та передають ці дані в розумну мережу.

Розумні системи водопостачання

Вода є одним з найважливіших природних ресурсів, і її дефіцит є поширеною проблемою в багатьох куточках світу. Тому впровадження систем розумного водопостачання – це не розкіш, а необхідність. Основна роль систем розумного водопостачання полягає в моніторингу, вимірюванні та ефективному розподілі використання води. Компанії Hauber-Davidson та Idris розробили помітну модель у цій галузі – розумний лічильник води. Ці лічильники можуть виявляти надходження і відтік води та виявляти будь-які потенційні витоки. Крім того, розумні лічильники води можуть використовувати дані з розумних річкових датчиків та інформацію про погоду для прогнозування паводків [45].

5.2. Медицина та охорона здоров'я

Сектор охорони здоров'я зазнав значного прогресу завдяки інтеграції Інтернету речей,пропонуючи рішення для реальних проблем охорони здоров'я та покращуючи спосіб життя людей. Дослідники запропонували різні додатки в галузі охорони здоров'я, які використовують носимі сенсорні пристрої для моніторингу стану здоров'я пацієнтів, діагностики захворювань, оповіщення про надзвичайні ситуації та сповіщення користувачів у разі потреби. Дистанційний моніторинг економить час як пацієнтів, так і лікарів, зменшуючи при цьому загальні витрати на охорону здоров'я. Крім того, обмін даними, зібраними з цих пристроїв, з дослідниками в галузі охорони здоров'я сприяє розробленню більш безпечних і своєчасних медичних рішень, а також допомагає у пошуку ліків і вакцин від нових хвороб. Розглянемо детальніше кілька застосувань Інтернету речей в охороні здоров'я.

Моніторинг електрокардіограми (ЕКГ)

ЕКГ вимірює електричні сигнали серця і слугує індикатором здоров'я серця,допомагаючи виявити такі стани, як аритмія, подовжений інтервал QT та ішеміяміокарда. Цікавим прикладом може бути система моніторингу даних ЕКГ, де використовується біпотенціальний чіп, який кріпиться на футболку користувача і передає дані на смартфон через Bluetooth. Поєднання систем Інтернету речей з

аналітикою великих даних дозволяє здійснювати моніторинг ЕКГ у режимі реального часу [46].

Моніторинг рівня глюкози

Діабет – це захворювання, яке характеризується вищим рівнем глюкози в крові, ніж у людей без діабету. Серед різних підходів до виявлення діабету найбільш поширеним методом діагностики залишається метод пальцевої проби, що передбачає невеликий укол на кінчику пальця з подальшим вимірюванням рівня глюкози в крові. Поява технології Інтернету речей дозволила вдосконалити цей процес, зробивши його швидшим, доступнішим та зручнішим для пацієнтів. У [84] описано інтегрований з Інтернетом речей неінвазивний пристрій для постійного моніторингу рівня глюкози в крові, що усуває потребу в тестуванні за допомогою пальцевої палички. Варто зазначити, що оптичні датчики, такі як інфрачервоні світлодіоди та фотодіоди ближньої інфрачервоної області також використовуються для вимірювання рівня глюкози.

Моніторинг температури

Традиційні методи вимірювання температури передбачають використання термометрів у роті, вусі або прямій кишці, але ці методи часто спричиняють дискомфорт для пацієнта і створюють підвищений ризик інфікування. Однак нещодавні досягнення в галузі додатків для моніторингу температури на основі Інтернету речей дозволили ефективно вирішити ці проблеми. Наприклад, у [86] описано 3D-друкований пристрій, який можна вставляти у вухо. Цей пристрій використовує інфрачервоний датчик для вимірювання температури барабанної перетинки, забезпечуючи точність і залишаючись незалежним від навколишнього середовища.

Моніторинг артеріального тиску

У багатьох діагностичних процесах вимірювання артеріального тиску є обов'язковим етапом. Однак основна проблема традиційного методу полягає в тому, що він вимагає, щоб кров'яний тиск вимірювала інша людина. Тому інтеграція Інтернету речей у моніторинг артеріального тиску стала корисною як для лікарів, так і для пацієнтів. Наприклад, гаджет без манжети [47], який можна носити без манжети, здатний вимірювати як систолічний, так і діастолічний тиск, а результати зберігати в хмарі.

Моніторинг насичення киснем

Пульсоксиметр надзвичайно корисний неінвазивний пристрій для вимірювання насичення киснем, долає обмеження традиційних методів і дозволяє здійснювати моніторинг у режимі реального часу. Інтеграція технологій на основі Інтернету речей призвела до значного прогресу в пульсоксиметрії, особливо в галузі охорони здоров'я. У дослідженні [46] було запропоновано вдосконалену неінвазивну систему пульсоксиметрії, здатну вимірювати рівень кисню, частоту

серцевих скорочень і параметри пульсу, передаючи ці дані на центральний сервер.

Моніторинг настрою

Інтеграція Інтернету речей у сферу моніторингу настрою пропонує численні переваги. Інтернет речей може визначати психічний стан людини, аналізуючи серцебиття за допомогою натільних пристроїв. У [92] описано натільний пристрій, здатний відстежувати емоції водія, включаючи гнів, стрес, жах і смуток. Інтелектуальна система, аналізуючи варіації емоцій, визначає, чи увійшов водій у підсвідомий стан, і відповідно зупиняє двигун постійного струму транспортного засобу.

Управління медикаментозним лікуванням

Дотримання графіка прийому ліків є життєво важливим, але складним завданням для людей похилого віку з проблемами пам'яті. На щастя, інтеграція Інтернету речей пропонує вирішення цієї проблеми, і численні дослідження реалізують використання Інтернету речей для відстеження дотримання пацієнтами режиму прийому ліків. У [48] було створено медичну коробку, яка нагадує людям про необхідність приймати ліки, з трьома лотками для різного часу доби. Система також вимірює життєво важливі параметри здоров'я (наприклад, артеріальний тиск, температуру, рівень кисню в крові тощо) і полегшує двосторонній зв'язок між пацієнтами та лікарями через мобільний додаток.

Система реабілітації

Застосування Інтернету речей у цій сфері є універсальним і довело свою ефективність у різних сферах, включаючи лікування раку, відновлення після спортивних травм, реабілітацію після інсульту та подолання фізичної інвалідності. Наприклад, в одномуз досліджень було представлено інноваційний розумний ходунок [98]. Лікарі та опікуни можуть отримати доступ до зібраних даних через мобільний додаток, що сприяє кращому моніторингу та підтримці, оскільки ці ходунки використовують мультимодальний датчик для моніторингу моделі ходьби пацієнта.

Фітнес

Регулярна фізична активність і підтримання високого рівня фізичної форми суттєво впливають на якість життя людини. Розробники створили різноманітні додатки звикористанням Інтернету речей для полегшення моніторингу фізичної активності та популяризації здорового способу життя. Ці підходи передбачають оцінку рівня активності користувачів та виявлення метрик, зокрема тривалість фізичноїактивності та періоди бездіяльності, використовуючи дані акселерометра смартфона. Сьогодні носимі фітнес-трекери, легко доступні на ринку і набули популярності як зручні пристрої для моніторингу рівня фізичної активності: наприклад, "розумні килимки", які дають уявлення про режим тренувань

користувачів, а також для оцінки фізичної активності та моніторингу тренувального навантаження для оптимізації стратегій гідратації спортсменів [49].

Інші помітні програми

Застосування Інтернету речей у галузі охорони здоров'я неймовірно різноманітне і виходить далеко за межі раніше згаданих сфер. Існує безліч сфер, де IoT вже впроваджений і де його потенційні переваги реалізуються, що призводить до значного зростання впровадження технології IoT в охорону здоров'я (HIoT). Наприклад, для лікування раку методи на основі Інтернету речей стали потужним інструментом. Інноваційний підхід до лікування раку на основі Інтернету речей представлений в недавньому дослідженні, яке охоплює різні етапи, включаючи хіміотерапію і променеву терапію. Крім того, ця система безпечно зберігає результати лабораторних аналізів на хмарному сервері, дозволяючи лікарям контролювати дозування ліків і надаючи можливість дистанційних консультацій через спеціальний мобільний додаток. Крім того, HIoT знайшов застосування у виявленні уражень шкіри, з помітними досягненнями у виявленні раку легенів завдяки сучасним алгоритмам ML і системам на основі IoT.

Інтернет речей революціонізував сферу хірургічної підготовки та медичних процедур, створивши рішення наступного покоління. Однією з таких розробок є система хірургічного навчання, яка використовує віртуальну реальність для імітації реалістичного навчального середовища. Ця платформа також дозволяє взаємодіяти з хірургами з усього світу, сприяючи спільному навчанню та обміну досвідом. Моніторинг рівня гемоглобіну в крові став більш доступним завдяки портативним пристроям, оснащеним фотоплетизмографічними датчиками, світлодіодами та фотодіодами. Ці пристрої дозволяють неінвазивне вимірювання рівня гемоглобіну, покращуючи медичний моніторинг та діагностику.

Численні інші додатки HIoT сьогодні використовуються або знаходяться на стадії дослідження, що підкреслює постійний революційний вплив Інтернету речей на сферу охорони здоров'я. Очікується, що Інтернет речей продовжуватиме стимулювати розвиток і вдосконалення надання медичних послуг і поліпшення результатів лікування пацієнтів.

Якщо розглянути розвиток цієї сфери на рівні держави, то буде доречно знову пригадати одного з лідерів серед розумних міст – Сінгапур. Охорона здоров’я – це ще один напрям, який активно інтелектуалізується в Сінгапурі, адже до 2050 року 47% населення Сінгапуру буде віком понад 65 років. Щоб зменшити наслідки від старіння населення на міські медичні служби, Сінгапур оцифрував свою систему охорони здоров’я.

Ініціатива електронної охорони здоров’я Сінгапуру – це комплексна цифрова платформа, яка спрямована на покращення якості та доступності медичних послуг у країні. Ініціатива здійснюється Міністерством охорони здоров’я (МОЗ) та Управлінням розвитку медіакомпаній Infocomm (IMDA), і в ній беруть

участь різні зацікавлені сторони в галузі охорони здоров'я, включаючи постачальників медичних послуг, технологічні компанії та пацієнтів.

Платформа електронної охорони здоров'я складається з кількох компонентів, які працюють разом, щоб забезпечити безперебійне обслуговування пацієнтів. Деякі з ключових компонентів включають:

HealthHub — це онлайн-портал, який дозволяє пацієнтам керувати своїм здоров'ям і самопочуттям. Він надає такі функції, як запис на прийом, отримання рецепта та доступ до медичних записів.

Телемедицина: телемедицина дозволяє пацієнтам дистанційно консультуватися з лікарями за допомогою відеоконференцій або обміну повідомленнями. Це може бути особливо корисно для пацієнтів, які живуть далеко від медичних закладів або мають проблеми з пересуванням.

TeleRehab: дозволяє пацієнтам виконувати вправи у власному домі – переносні пристрої Інтернету речей (IoT) відстежують прогрес пацієнтів і передають дані своєму терапевту через бездротову мережу.

Використання ШІ в Сінгапурі допомагає зменшити самотність серед старіючого населення: чат-боти на основі штучного інтелекту спілкуються з людьми похилого віку, розповідають їм про діяльність громади та інтегрують повідомлення, які пропагують здоровий спосіб життя.

Розумна система сповіщення людей похилого віку на основі штучного інтелекту відстежує регулярні рухи людей і вивчає їх, повідомляючи опікуна якщо відбувається щось незвичайне та може знадобитися термінова допомога.

5.3. Розумне сільське господарство та навколишнє середовище

Сільське господарство відіграє важливу роль в економічному розвитку країни. Різні фактори, зокрема вологість ґрунту та параметри навколишнього середовища, такі як рівень вуглекислого газу, температура та вологість, можуть суттєво впливати на врожайність сільськогосподарських культур. Для покращення результатів сільського господарства стає необхідним впровадження надійних систем спостереження на полях. Інтеграція Інтернету речей дозволяє ефективно досягти цієї мети.

Розглянемо декілька прикладів застосування IoT у цій галузі розумного сільського господарства, а також наведем короткий огляд відповідних досліджень.

Водозберігаюче зрошення

Дефіцит води в сільському господарстві викликає все більше занепокоєння, що зумовлює необхідність динамічного підходу до зрошення через мінливі потреби культур у воді. Інтеграція Інтернету речей революціонізує традиційне зрошення під час повеней, пропонуючи рішення проблеми нестачі води у вирощуванні сільськогосподарських культур. У [50] запропоновано бездротову

систему на основі сенсорних мереж, що використовує нейронні мережі для водоефективного зрошення. Цей метод підвищує ефективність зрошення, мінімізуючи втручання людини та зменшуючи втрати через надмірний дренаж.

Моніторинг навколишнього середовища для вирощування сільськогосподарських культур

Різні фактори навколишнього середовища, включаючи температуру, вологість, атмосферний тиск, рівень вуглекислого газу, температуру ґрунту та pH ґрунту, відіграють вирішальну роль у вирощуванні сільськогосподарських культур. Пристрої Інтернету речей, інтегровані в сільськогосподарські системи, можуть відчувати і аналізувати ці фактори навколишнього середовища, що дозволяє здійснювати віддалений моніторинг полів і створювати оптимальне сільськогосподарське середовище, пристосоване до цих змінних. У [51] розроблено бездротову систему моніторингу навколишнього середовища, яка використовує енергію ґрунту для забезпечення економічно ефективного дистанційного моніторингу стану сільськогосподарських угідь.

Моніторинг інформації про тваринний та рослинний світ

Ефективне сільськогосподарське виробництво вимагає всебічного моніторингу інформації як про рослини, так і про тварин, що має вирішальне значення для покращення виробництва, збільшення прибутковості та забезпечення високої якості продукції.

1. Інформаційний моніторинг життя тварин: Моніторинг різних аспектів поведінки тварин, включаючи споживання їжі, температуру тіла, рівень активності та стан здоров'я, дозволяє відстежувати їх фізіологічне та харчове благополуччя, забезпечуючи їх здоровий розвиток. У роботі [52] автори запропонували систему вимірювання температури тіла свиней на основі інфрачервоноговипромінювання, що дозволяє на ранній стадії виявляти захворювання.
2. Інформаційний моніторинг життєдіяльності рослин: Бездротові сенсорні пристрої, підключені до рослин, дозволяють здійснювати віддалений і безперервний моніторинг як зовнішніх факторів (таких як хвороби, шкідники, колір листя), так і внутрішніх (включаючи вміст хлорофілу і швидкість фотосинтезу). Ця технологія дозволяє виявляти хвороби на ранніх стадіях і сприяє загальному здоровому росту рослин. У [50] розроблено систему відстеження цитрусових, яка оцінює умови навколишнього середовища для оптимального росту, виявлення та запобігання хворобам рослин для забезпечення міцного здоров'я цитрусових культур.

Інтелектуальна сільськогосподарська техніка

Інтелектуальна техніка автономно керує широким спектром сільськогосподарських операцій, таких як обробка ґрунту, посів, пересадка,

внесення добрив, пестицидів, підживлення, зрошення, збирання врожаю, і все це виконується з точністю та ефективністю. Більше того, вона має можливість збирати різноманітні дані про ферму, включаючи вологість ґрунту та якість води, а також інформацію про навколишнє середовище, таку як температура та вологість, які можуть бути ефективно використані для впровадження точного землеробства та покращення селекційних практик. Технологія Інтернету речей відіграє ключову роль у мінімізації ручної праці в сільському господарстві, дозволяючи здійснювати віддалений моніторинг і стандартизацію функцій техніки за допомогою датчиків і бездротового зв'язку. У [45] описано універсальний автономний транспортний засіб-робота, який оснащено технологією Bluetooth для дистанційного керування та який здатний самостійно виконувати низку завдань, зокрема землеробство, посів та зрошення.

Якість та безпека сільськогосподарської продукції

Інтернет речей значно покращує якість, безпеку та відстежуваність сільськогосподарської продукції, особливо у сфері складування, логістики та дистрибуції, завдяки автоматичній ідентифікації, відстеженню та точному підрахунку продукції. Різні країни впровадили системи відстеження в режимі реального часу, такі як американські, європейські, шведські, японські та австралійські системи, визнаючи нагальну потребу в ефективному відстеженні в сільському господарстві. У [53] розробили комплексну платформу відстеження безпечності сільськогосподарської продукції, яка полегшує автоматичне збирання, обробку та відображення даних у реальному часі для покращення відстеження та зменшення пов'язаних з цим витрат.

Моніторинг захворювань

Інтеграція Інтернету речей для безперервного моніторингу в режимі реального часу пропонує фермерам та відповідним органам влади можливість виявляти хвороби на ранній стадії та впроваджувати профілактичні заходи до того, як вони загостряться. Навколишнє середовище на фермі відіграє ключову роль у виникненні захворювань. Наприклад, фреймворк, представлений в [44], інтегрує різні сенсорні пристрої через бездротові сенсорні мережі для моніторингу різних факторів навколишнього середовища.

5.4. Розумний будинок

У розумному будинку стратегічно розміщені різні типи датчиків, кожен з яких виконує свою специфічну функцію. Розумні будинки спрощують щоденні завдання для користувачів, що особливо корисно для тих, хто схильний забувати про рутинні дії, такі як замикання дверей або вимикання приладів. Від розумних дверних замків до обслуговування побутових приладів, таких як кавоварки, обігрівачі та розумні лампочки, і навіть використання камер спостереження для посилення безпеки – розумні будинки пропонують широкий спектр можливостей.

Крім того, користувачі можуть керувати цими пристроями за допомогою голосових команд і віддалено контролювати домашнє обладнання. Розумні будинки сприяють підвищенню енергоефективності, автоматично вимикаючи пристрої, які не використовуються, і повідомляючи користувачів про будь-які незвичайні інциденти. MavHome [45],наприклад, використовує алгоритми прогнозування для виконання різних завдань у відповідь на ініційовані користувачем події. Що стосується енергозбереження, то інтелектуальний будинок досягає цього завдяки використанню датчиків і контекстно-орієнтованим можливостям Інтернету речей. Дані, зібрані цими датчиками, передаються до контекстного агрегатора, який потім пересилає їх до контекстно-орієнтованого сервісного механізму. Цей механізм аналізує дані і визначає відповідні дії. Наприклад, він може вирішити вимкнути кондиціонер, якщо температура занадто низька, перекрити подачу газу в разі виявлення витоку або вимкнути світло, коли в будинку немає мешканців.

5.5. Інтелектуальна виробнича система

З розвитком та еволюцією Інтернету речей, промислового Інтернету речей, штучного інтелекту та кіберфізичних систем багато країн вирішили трансформувати свої виробничі системи в інтелектуальні виробничі системи (Smart Manufacturing System, SMS). Завдяки інтеграції інтелектуальних технологій ці системи сприяють швидкому та широкому потоку даних всередині та між виробничими процесами. Оснащені цими даними, використовуючи передові інформаційно-комунікаційні технології, інтелектуальні виробничі системи здатні швидко реагувати на глобальні потреби, ефективно використовувати матеріали, енергію та трудові ресурси, а також вчасно доставляти продукцію, виготовлену на замовлення. Що відрізняє модель розумного виробництва від інших парадигм виробництва, так це її бачення наступного покоління виробництва з розширеними можливостями. Ці системи адаптуються до нових обставин, використовуючи інформацію в режимі реального часу для інтелектуального прийняття рішень, а також проактивно прогнозуючи та запобігаючи потенційним збоям.

5.6. Інтернет робототехнічних речей (IoRT)

Інтернет робототехнічних речей – це концепція, яка поєднує в собі принципи Інтернету речей та робототехніки. IoRT – це нова технологія, яка включає роботів в екосистему IoT як об'єкти, що забезпечують комунікацію, співпрацю та автоматизацію. Ці роботи легко інтегруються в інтелектуальне середовище, виконуючи широкий спектр завдань. Ці завдання охоплюють від особистої діяльності в "розумних" будинках до застосунків у галузі охорони здоров'я. Крім того, вони поширюються на професійну діяльність, таку як моніторинг, доставка та управління об'єктами на виробництві або складах.

5.7. Нафтогазова промисловість

Нафтогазова промисловість, стикаючись зі значними витратами та ризиками для безпеки, використовує дистанційний моніторинг на основі Інтернету речей для нагляду за польовим обладнанням у режимі реального часу та прийняття рішень на основі даних. Ці рішення дозволяють здійснювати дистанційний моніторинг польового обладнання, аналіз польових даних, спільне прийняття рішень на основі даних та виконання команд управління для оптимізації роботи активів при одночасному зниженні ризиків для здоров'я, безпеки та навколишнього середовища. Крім того, інтеграція Інтернету речей у нафтовій промисловості зосереджена на скороченні людської праці, мінімізації втрат часу та підвищенні точності завдяки автоматизації, прикладом чого є система оптимізації свердловин компанії Equinor на нафтовому родовищі Баккен. Розгорнувши пристрої Інтернету речей та алгоритми ML на близько 50 свердловинах, компанія Equinor досягла 33% збільшення видобутку нафти за рахунок оптимізації експлуатації та обслуговування свердловин.

5.8. Розумна торгівля (рітейл)

Впровадження Інтернету речей у роздрібній торгівлі створило гнучке середовище, яке приносить користь як покупцям, так і продавцям. Це дозволяє всьому сектору роздрібної торгівлі мігрувати з офлайн в онлайн, дозволяючи клієнтам самостійно здійснювати покупки за допомогою самообслуговування, а також сприяючи безперешкодній взаємодії між рітейлерами та їхніми клієнтами. Крім того, рітейлери можуть використовувати технології Інтернету речей, такі як RFID, для моніторингу товарів і розгортання датчиків для збирання даних про клієнтів, які вони потім можуть використовувати для аналізу купівельної поведінки клієнтів і підвищення прибутковості бізнесу. Крім того, клієнти мають можливість здійснювати платежі через онлайн-транзакції та відстежувати свої замовлення за допомогою онлайн-сервісів.

5.9. Промисловий Інтернет речей (IIoT)

На думку численних дослідників ринку, IIoT має величезний потенціал, оскільки є розширенням IoT, спеціально адаптованим для промислового сектора та його застосувань. Він дає змогу галузям і підприємствам покращити та оптимізувати свою діяльність, використовуючи комунікацію M2M, аналітику великих даних та інтелектуальний аналіз. Сфера застосування IIoT дуже широка і охоплює широкий спектр підключених промислових пристроїв і систем. Підключені електролічильники, системи водовідведення, витратоміри, монітори трубопроводів, виробничі роботи та різні інші типи промислового обладнання та пристроїв включені в цей список. Одним з помітних застосувань IIoT є гірничодобувна промисловість, де такі компанії, як CISCO, впровадили рішення

IIoT для підвищення безпеки та ефективності в підземних шахтах. Ці рішення передбачають зв'язок між людьми, відстеження місцезнаходження шахтарів і транспортних засобів, моніторинг стану транспортних засобів і автоматизацію управління будівлями.

5.10. Соціальне життя та розваги

Було розроблено кілька додатків для моніторингу та покращення соціальної активності людини, на додачу до роботи чи професійної діяльності, оскільки соціальне життя та розваги є невід'ємними частинами життя людини. Портативні пристрої, такі як мобільні телефони та планшети, мають сенсорні можливості та комунікаційні технології, які полегшують взаємодію між людьми. Інтеграція Інтернету речей у соціальне життя людини може сприяти виявленню емоцій, побудові спільноти та емоційній підтримці. CircleSense – це додаток, який аналізує соціальну активність людини за допомогою різних датчиків, щоб визначити її соціальне коло. Він також відстежує місцезнаходження людини за допомогою датчиків місцезнаходження і використовує технологію Bluetooth для ідентифікації людей, які знаходяться поблизу. Кемі, штучний домашній собака, виражає прихильність і співчуття завдяки використанню ефективної обчислювальної технології. Ця технологія аналізує різні аспекти поведінки людини, такі як вираз обличчя, мова, жестикуляція, рухи рук і режим сну, щоб ідентифікувати та належним чином реагувати на її емоції.

6. Проблеми безпеки та конфіденційності IoT

Неоднорідність пристроїв та різноманітність додатків Інтернету речей призводять до виникнення проблем безпеки та конфіденційності. Люди в першу чергу стурбовані потенційними вторгненнями в особисте життя і загрозами безпеці під час використанні цих технологічних пристроїв.

Автор концепції Індустрія 4.0. Клаус Шваб у своїй книзі «Технології Четвертої промислової революції» [8] визначив таку інфраструктуру кіберризиків (рис. 6.1).

Рис. 6.1. Інфраструктура кіберризиків за версією Всесвітнього економічного форуму

Високий рівень неоднорідності у поєднанні з широким спектром систем IoT, як очікується, збільшить кількість загроз безпеці власників пристроїв, які все частіше використовуються для взаємодії людей, машин та речей у будь-якій варіації. Традиційні заходи забезпечення безпеки та дотримання конфіденційності не можуть бути застосовані до технологій IoT, зокрема через їх обмежену обчислювальну потужність. Крім того, велика кількість підключених пристроїв породжує проблему масштабованості. Водночас для досягнення визнання з боку користувачів необхідно обов'язково забезпечити дотримання безпеки, конфіденційність та моделі довіри, що підходять для контексту IoT. Для запобігання несанкціонованому доступу користувачів

(тобто людей та пристроїв) до системи повинні використовуватися механізми автентифікації та авторизації, гарантована безпека, конфіденційність та цілісність персональних даних. Щодо персональних даних користувачів та їх інформації – повинні забезпечуватися захист і конфіденційність, насамперед тому, що пристрої мають доступ до неї та здатні нею керувати (наприклад, відомості про звички користувачів). Нарешті, довіра (надійність, англ. Trustworthy) – це основна проблема, оскільки IoT середовище характеризується різними типами пристроїв, які повинні обробляти дані відповідно до потреб та прав користувачів.

Звернемо увагу, що адаптація та самовідновлення відіграють ключову роль в IoT інфраструктурах, які мають бути в змозі протистояти несподіваним змінам у навколишньому середовищі. Відповідно, до питань конфіденційності та безпеки слід ставитись гнучко. Поряд із традиційними рішеннями для забезпечення безпеки потрібно використовувати спеціальні механізми, вбудовані безпосередньо у пристрої з метою оперативної діагностики, ізоляції та профілактики порушень.

6.2. Безпека

Різні рівні IoT вразливі до різних видів атак, які залежать від технологій і протоколів, що використовуються на цих рівнях. Згідно з [54], шари IoT, включаючи рівень сприйняття, мережевий рівень і рівень додатків, стикаються з різними атаками. Оскільки основна роль рівня сприйняття полягає в збирання даних, проблеми безпеки на цьому рівні зосереджені на фальсифікації даних і знищенні пристроїв сприйняття. Цей рівень стикається з такими атаками, як атаки захоплення вузлів (*Node Capture Attacks*), атаки введення шкідливого коду (*Malicious code Injection Attacks*), атаки введення неправдивих даних (*False Data Injection Attacks*), атаки повторного відтворення (*Replay Attacks*), атаки криптоаналізу (*Cryptanalysis Attacks*) та атаки побічних каналів (*Side Channel Attacks*), підслуховування та втручання, а також атаки позбавлення сну (*Eavesdropping and Interference, Sleep Deprivation Attacks*).

Оскільки основною функцією *мережевого рівня* є передача зібраних даних, особливо з використанням бездротових технологій, проблеми безпеки на цьому рівні пов'язані з доступністю мережевих ресурсів і бездротової мережі. Виклики на мережевому рівні охоплюють *атаки типу "відмова в обслуговуванні" (Denial-of-Service Attacks, DoS), спуфінг-атаки (Spoofing Attacks), атаки типу "карстова воронка" (Sinkhole Attacks), атаки типу "черв*оточина" *(Wormhole Attacks), атаки типу "людина всередині" (Man-in-the-Middle Attacks), атаки типу "інформація про маршрутизацію" (Routing Information Attacks), атаки типу "Сибіла" (Sybil Attacks) та несанкціонований доступ* [140]. На *прикладному* рівні, який зосереджений на наданні запитуваних користувачем послуг, виклики насамперед пов'язані з *програмними атаками, включаючи фішингові атаки, шкідливі віруси/хробаки, шкідливі скрипти*.

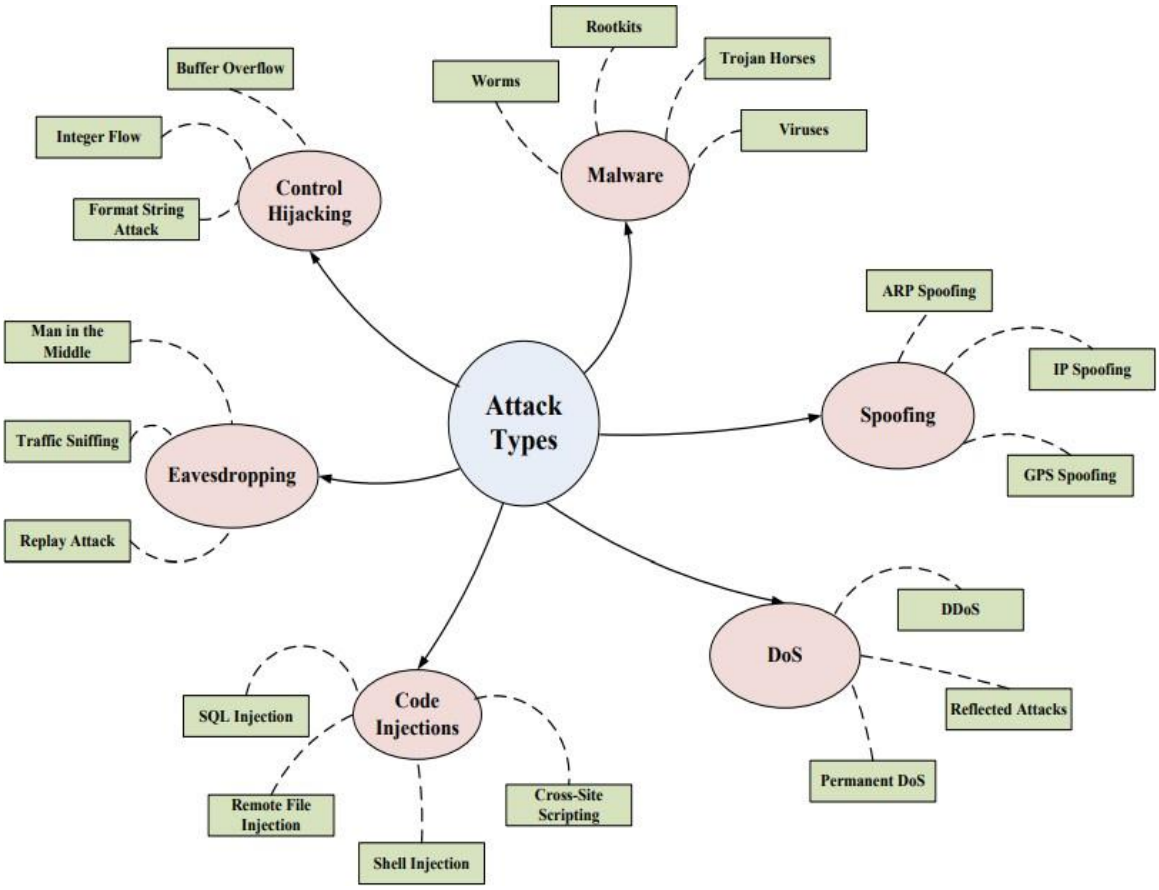

Рис.6.2. Атаки на кіберфізичні системи

Дослідницький підрозділ компанії Palo Alto Networks наводить статистику з атак на IoT системи, що відображена на рис.6.3. Відповідно до цієї статистики, 57% IoT-пристроїв уразливі для атак середнього або високого ступеня серйозності, що робить IoT легкою здобиччю для зловмисників. 41% атак використовують уразливості пристроїв.

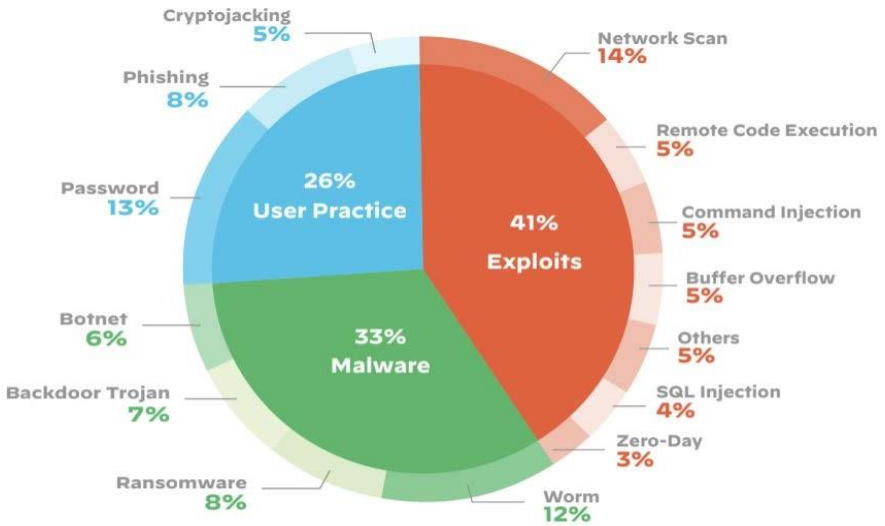

Рис. 6.3. Статистика атак на IoT системи

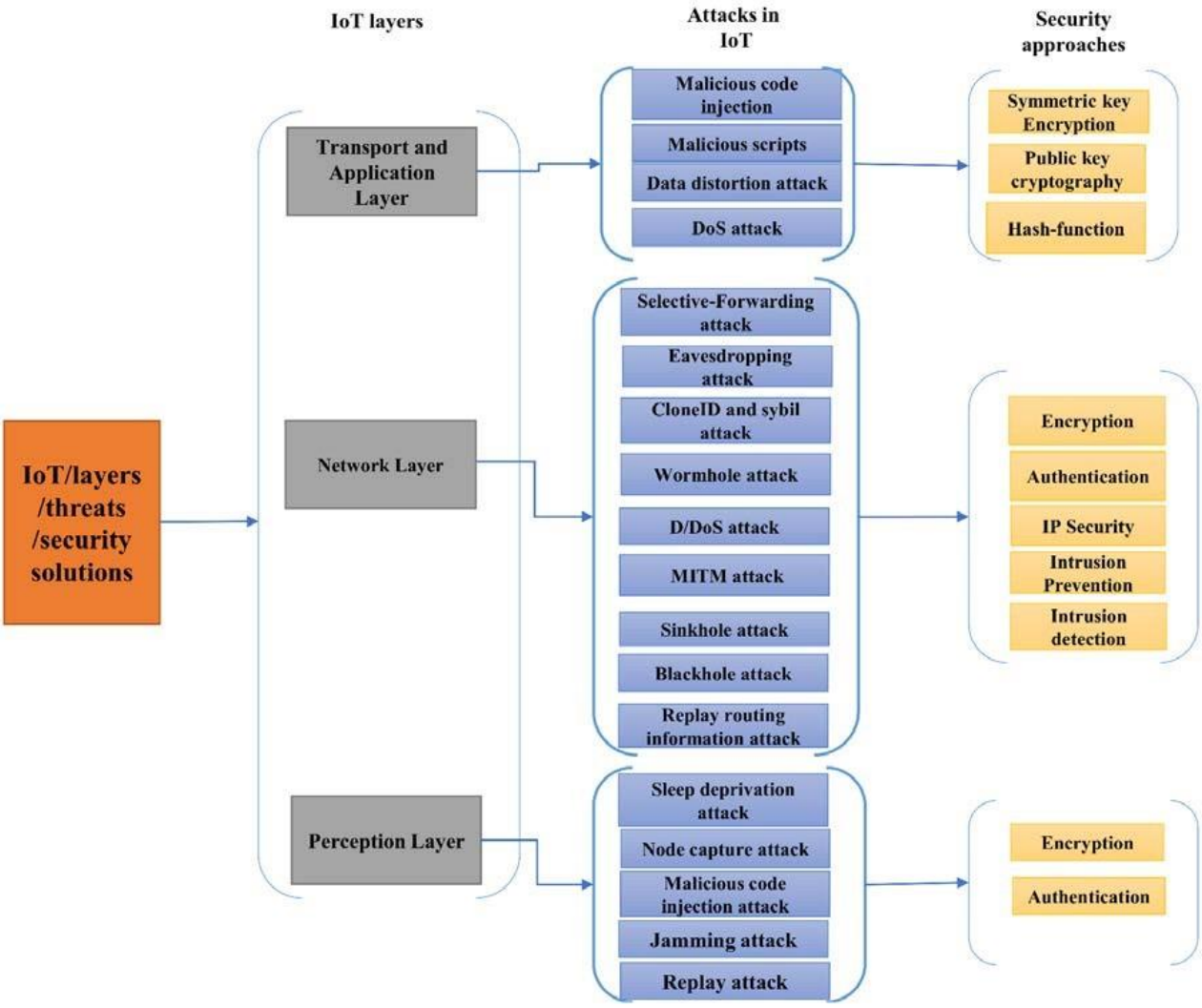

Рис. 6.4. Атаки за архітектурними рівнями IoT

Відповідно, не існує єдиного універсального підходу до кібербезпеки систем Інтернету речей. Саме ця ідея – “No one-size-fits-all” і покладено в основу підходу NIST до кібербезпеки IoT систем (рис. 6.5) [27].

Для виявлення та захисту від несанкціонованого доступу необхідно запропонувати безпечні та надійні схеми автентифікації.

Для захисту від хробаків, вірусів і шкідливих скриптів, що проникають через брандмауери, необхідно впроваджувати методи виявлення вірусів і скриптів,такі як методи honeypot, статичний аналіз коду і динамічне виявлення дій.

Рис. 6.5. NIST про кібербезпеку IoT [27].

Крім того, впровадження захищених протоколів маршрутизації є важливим для забезпечення безпечної маршрутизації.

6.3. Конфіденційність

Пристрої Інтернету речей безперервно генерують величезні обсяги даних в режимі реального часу, які проходять три основні етапи:

- збирання даних,
- агрегація даних
- інтелектуальний аналіз даних та аналітика

Хоча ці процеси покращують наше життя, надаючи різні послуги, вони також викликають занепокоєння щодо конфіденційності даних в Інтернеті речей. Порушення конфіденційності в IoT може мати серйозні наслідки як для мережі IoT, так і для її користувачів, зокрема фінансові втрати, пошкодження майна і навіть ризики для безпеки людей.

Наприклад, розглянемо розумну мережу, де зловмисники можуть легко перехопити контроль над розумними" лічильниками, що дозволить їм отримати

доступ до зібраних даних або маніпулювати ними. Це потенційно може поставити під загрозу конфіденційність і приватність даних про споживання енергії. Використовуючи ці змінені дані, постачальники комунальних послуг можуть робити неточні оцінки попиту та пропозиції енергії в мережі, що призведе до помилкових рішень щодо диспетчеризації енергії. Це, своєю чергою, може призвести до дисбалансу попиту та пропозиції енергії, що потенційно може спричинити масові відключення електроенергії.

У сфері охорони здоров'я, якщо зловмиснику вдасться отримати дані про стан здоров'я пацієнта, він зможе маніпулювати рецептами на ліки або медичними записами, що призведе до значних ризиків для здоров'я і потенційного страхового шахрайства. Тому вкрай важливо розгортати схеми збереження конфіденційності, щоб запобігти витоку даних і гарантувати, що приватні дані залишаться недоступними для зловмисників.

Відповідно, існує три основні групи механізмів захисту конфіденційності в контексті обробки даних Інтернету речей:

- захист конфіденційності під час збирання даних
- захист конфіденційності під час агрегації даних
- захист конфіденційності під час інтелектуального аналізу даних та аналітики

Хоча для захисту конфіденційності при збиранні, аналізі та аналітиці даних можуть застосовуватися різні методи, такі як шифрування і управління ключами, більшість зусиль щодо захисту конфіденційності в IoT зосереджені на агрегації даних. Агрегація даних передбачає обробку релевантних даних у декількох місцях, що ускладнює забезпечення конфіденційності за допомогою традиційних методів шифрування.

У результаті дослідники розробили кілька механізмів збереження конфіденційності спеціально для агрегації даних, які можна класифікувати так:

- *Збереження конфіденційності* на *основі анонімності,* яке використовує такі методи, як K-анонімність, L-різноманітність і T-близькість для захисту конфіденційності ідентифікаційної інформації під час агрегації даних.
- *Захист конфіденційності* на *основі шифрування*, який не дозволяє зловмисникам підслуховувати дані під час агрегації, використовуючи такі методи шифрування, як гомоморфне шифрування, механізми зобов'язань, обмін секретами та докази з нульовим знанням.
- *Збереження конфіденційності на основі збурень,* коли такі методи, як кастомізація даних, спільне використання даних і введення випадкового шуму, збурюють необроблені дані, щоб забезпечити конфіденційність під час агрегації.

Зокрема схеми збереження конфіденційності на основі збурень є популярними в IoT завдяки тому, що вони безпосередньо працюють з

необробленими даними. Однак багато з цих схем збереження конфіденційності на основі збурень жертвують корисністю даних для досягнення конфіденційності. Таке зменшення корисності даних може перешкоджати підтримці сервісів, запитуваних додатками IoT. Тому значним викликом в області збереження конфіденційності даних в IoT є розроблення схем, які забезпечують баланс між конфіденційністю та корисністю даних, що робить цю сферу важливою для майбутніх досліджень. Отже, захист конфіденційності даних в Інтернеті речей має вирішальне значення для запобігання цим негативним наслідкам і підтримки безпеки і цілісності як окремих осіб, так і екосистеми Інтернету речей.

Аутентифікація та конфіденційність

Що стосується аутентифікації, підхід, запропонований у [8], передбачає використання механізму інкапсуляції, що налаштовується користувачем, а саме протокол прикладного рівня для IoT — «інтелектуальна служба забезпечення безпеки» (*Intelligent Service Security Application Protocol*). Він поєднує крос-платформні зв'язки із шифруванням, підписом та автентифікацією для підвищення ефективності розроблення додатків IoT створенням системи захищеного зв'язку між різними речами.

У роботі [54] описано першу повністю реалізовану двосторонню схему автентифікації для IoT на основі існуючих стандартів, зокрема, протокол датаграм безпеки транспортного рівня (*Datagram Transport Layer Security, DTLS*), який розташовується між транспортним і прикладним рівнями. Ця схема основана на криптографічному алгоритмі RSA і призначена для IPv6 з використанням стандарту 6LoWPANs (*IPv6 over Low power Wireless Personal Area Networks*). Аналіз результатів, що базуються на реальних системах IoT, показує, що така архітектура забезпечує цілісність повідомлення, конфіденційність, енергоефективність, низькі значення затримки пакетів та навантаження на пам’ять.

Щодо конфіденційності та цілісності – в [54] наведено результати аналізу того, як існуючі системи управління ключами можуть бути застосовані в контексті IoT. Це дозволяє класифікувати протоколи систем управління ключами (*Key Management System, KMS*) за чотирма основними категоріями: структура пула ключів, математична база, механізм взаємодії та структура відкритого ключа. У роботі [54] автори стверджують, що більшість протоколів KMS не підходять для IoT. Проте протоколи KMS придатні для сценаріїв, у яких обчислювальні потужності є доволі низькими порівняно з використанням криптографії з відкритим ключем (*Public Key Cryptography, PKC*). Але для таких схем необхідне введення кількох контрзаходів для управління пристроєм аутентифікації та щоб уникнути MITM атаки (*Man In The Middle*).

Більш практичний підхід [55] пропонує модель передавання зі схемами шифрування підпису, в якій розглядаються вимоги безпеки IoT (тобто анонімність, надійність та стійкість до атак) за допомогою ONS запитів (*Object Naming Service*). Проте, з погляду стійкості до атак, результати моделі передавання є дуже слабкими через використання шифрування з урахуванням «точка–точка» (*hop by hop*).

Не існує унікального та єдино правильного рішення, яке може гарантувати конфіденційність в IoT. У цьому контексті багато зусиль було докладено для WSN (*Wireless Sensor Network*). Наприклад, протокол аутентифікації для IoT, представлений у [55], використовує легкий метод шифрування, оснований на операції XOR.

У межах WSN автентифікація користувача та схема узгодження ключа для гетерогенних бездротових сенсорних мереж також запропонована, наприклад. Це рішення дозволяє віддаленому користувачеві безпечно домовитися про сеансовий ключ із сенсорним вузлом за допомогою протоколу розподілу ключів. Тобто, він забезпечує взаємну автентифікацію між користувачами, сенсорними вузлами та шлюзовими вузлами (*gate way node, GWN*). Для того, щоб застосувати таку схему для архітектури з обмеженими ресурсами, використовуються лише прості хеш та XOR обчислення.

Метод перевірки автентичності та контроль доступу, представлений у [56], спрямований на створення ключа сеансу із застосуванням еліптичної криптографії (*Elliptic Curve Cryptography, ECC*). Крім того, запропоновано механізм захисту даних у хмарних сховищах, оснований на поєднанні «класичної» проблеми Діффі–Хеллмана та проблеми дискретного логарифмування у групі точок еліптичної кривої. Зазначається, що протокол, оснований на еліптичних кривих, має невеликий розмір ключа без шкоди криптостійкості, що робить еліптичну криптографію привабливою для використання в тих областях, де існують проблеми через обмеження пам'яті та обчислювальних потужностей.

Контроль доступу

Управління доступом належить до дозволів у сфері використання ресурсів, призначених для різних суб'єктів у мережі IoT. У [54] визначено два суб'єкти: власники даних та збирачі даних. Користувачі та речі як власники даних повинні дозволяти передавати лише відомості, необхідні для виконання конкретного завдання. Водночас збирачі даних повинні вміти ідентифікувати або підтверджувати справжність (аутентифікувати) користувачів речей як законних власників даних, від яких вона збирається.

Оскільки у IoT обробляються потокові, а не дискретні дані, як у традиційних системах, то основні проблеми в цьому контексті відносяться до продуктивності та часових обмежень, адже потік даних інтенсивніший, ніж у традиційних СУБД. Велика кількість вузлів авторизованих користувачів використовує широкий спектр різних типів даних, що відповідають рівням конфіденційності та безпеки. Тому використовують ієрархічну схему управління доступом для цього рівня. Схема враховує обмежену обчислювальну потужність та ємність пристрою зберігання. Кожному користувачеві та/або вузлу дається лише один ключ; інші необхідні ключі отримують за допомогою детермінованого алгоритму деривації ключа (deterministic key derivation algorithm), підвищуючи рівень безпеки (оскільки обмін ключів обмежений) і скорочуючи витрати на зберігання для множини вузлів.

Для підвищенні продуктивності та масштабованості СУБД може використовуватись підхід, який усуває проблему аутентифікації зовнішніх потоків даних з використанням безперервної автентифікації в потоках даних (*Continuous Authentication on Data Streams, CADS*). Для цього передбачається наявність постачальника послуг, який збирає дані від одного або кількох власників разом з інформацією аутентифікації і водночас опрацьовує запити безлічі клієнтів. Постачальник послуг повертає клієнтам результати запитів, а також інформацію про перевірку, що дозволяє їм перевірити справжність та повноту отриманих результатів на основі інформації автентифікації, наданої власником даних.

Через велику кількість потокових даних компанії можуть купувати ресурси, необхідні розгортання систем управління потоками даних (*Data Stream Management Systems, DSMS*), відбувається так званий аутсорсинг даних. Тоді пропонується делегувати зберігання та обробку потоку спеціалізованій третій особі з сильною інфраструктурою DSMS. Однак, тут постає питання довіри: третя особа може діяти зловмисно, наприклад, з метою збільшення свого прибутку. Рішення полягає в тому, щоб прийняти метод аутентифікації потоку так, щоб клієнти могли перевірити цілісність і актуальність отриманих від сервера даних. При цьому метод повинен задовольняти вимоги IoT пристроїв, що характеризуються обмеженими ресурсами з погляду енергоспоживання, обчислювальної потужності та запам’ятовуючих пристроїв.

Головними проблемами, пов'язаними з контролем доступу в сценарії IoT, є такі питання:

- Як гарантувати права доступу в середовищі, в якому не лише користувачі, а й речі можуть взаємодіяти із системою?
- Який підхід використання найефективніший: централізований, розподілений або напіврозподілений для управління масштабованою IoT архітектурою?
- Як обробляти величезний обсяг даних, що передаються (тобто у вигляді потоку даних)?

Що стосується ідентифікації, то однією з особливостей сьогодні є збільшення мобільності портативних та потужних бездротових пристроїв. Для вирішення цієї проблеми потрібно доопрацювати архітектуру щодо правил іменування, адресації, крім того необхідний розвиток певної структури управління даними для IoT.

Без відповіді залишаються такі проблемні аспекти:

- для управління контролем доступу IoT система може здійснювати реєстрацію користувачів та речей, для чого необхідна наявність відповідного повноважного органу для видачі посвідчень або сертифікатів;
- користувачі/речі повинні мати можливість надати облікові дані/сертифікати системі IoT для того, щоб взаємодіяти з іншими авторизованими/дозволеними пристроями;
- визначення конкретних ролей і функцій у межах IoT для управління процесами авторизації.

Для вирішення цих проблемних питань нещодавно було запропоновано кілька нових рішень. У [55] представлено схему авторизації для пристроїв з обмеженими ресурсами, яка поєднує технології функцій, що фізично не можуть бути клоновані *(Physical Unclonable Functions, PUFS)* із вбудованим модулем ідентифікації абонента *(Subscriber Identity Module, eSIM).* Перша забезпечує недорогі, безпечні секретні ключі із захистом від злому для M2M пристроїв. Друга забезпечує мобільний зв'язок, що гарантує масштабованість, сумісність та відповідність протоколам безпеки.

Групове передавання розглянуто в [56], де використовується загальний секретний ключ, позначений як груповий, загальний для кількох кінцевих точок обміну даними. Такі ключі управляються та поширюються на основі централізованого підходу. Зауважимо, що такий механізм знижує накладні витрати (кількість обчислювальних ресурсів) та мережевий трафік через зміни складу в групах, викликаних користувальницькими з'єднаннями, як це відбувається в IoT. Такий протокол може бути застосований у двох відповідних сценаріях: 1) безпечна агрегація даних в IoT та 2) комунікація в автомобільних однорангових мережах VANETs (англ. Vehicle to Vehicle, V2V).

6.3. Правові та регуляторні питання

Окрім технічних методів забезпечення безпеки та конфіденційності IoT систем необхідно дотримуватись вимог діючого законодавства щодо захисту персональних даних користувачів, які обробляються.

Тому розглянемо правові аспекти,що стосуються ефективності чинних законів у захисті користувачів у цьому контексті.Важливість цього питання зумовлена дедалі більшим розмиванням межі між фізичною та віртуальною сферами в IoT.

Для існують виклики, такі як фінансові обмеження, вразливі місця в системі безпеки та проблеми конфіденційності даних, які можуть мати небезпечні для життя наслідки, особливо у випадку витоку даних у сфері охорони здоров'я. Для ефективного вирішення цих проблем вирішальне значення має проактивний підхід, що передбачає проведення масштабних досліджень. Ці дослідження повинні бути зосереджені на виявленні специфічних проблем Інтернету речей з подальшим впровадженням надійних технічних рішень. Ефективне виконання цього процесу не тільки забезпечить безпеку системи Інтернету речей, але й сприятиме підвищенню довіри користувачів до реєстрації в мережі Інтернету речей.

Для пом'якшення етичних проблем важливе значення має підвищення обізнаності користувачів, а також інтеграція самоадаптивних політик безпеки та політик, що динамічно модифікуються, під час розробки додатків Інтернету речей. Необхідно також запроваджувати нові закони і стандарти, інтегруючи існуючі нормативні акти, такі як GDPR, HIPPA, FIPPS, Закон про конфіденційність електронних комунікацій та інші, для всебічного вирішення питань безпеки, конфіденційності та правових питань. Крім того, вирішення технічних проблем передбачає впровадження адаптованих і нових стандартів, а також впровадження стандартної ідентифікації

адрес. Деякі приклади таких технічних рішень включають передові методи шифрування, електронні підписи,інтеграцію стандартні протоколи та правила, що обмежують використання даних третіми сторонами. Такий цілісний підхід спрямований на подолання багатогранних викликів,з якими стикається Інтернет речей.

6.3.1. GDPR та IoT: рекомендації щодо захисту особи та конфіденційності користувачів

IoT передбачає постійне збирання та зв'язування даних користувачів, щоб забезпечити персоналізований досвід на основі здійсненого аналізу. Для цього необхідна послідовна ідентифікація користувачів і пристроїв, що створює ризик для конфіденційності користувачів. Загальноєвропейський регламент із захисту персональних даних (General Data Protection Regulation, GDPR) [57] містить численні положення, пов'язані з цими ризиками, проте їх може бути недостатньо для забезпечення справедливого балансу між інтересами користувачів і розробників.

У розділі 5 ми вже розглянули те, що IoT – це технологічний сектор, який швидко розвивається. В ЄС розроблення та впровадження IoT можна побачити в таких сферах, як охорона здоров'я, комунальні послуги, міське планування та управління, логістика та управління ланцюгом поставок, сільське господарство та торгівля. Величезні обсяги персональних даних тепер збираються та обмінюються пристроями та службами IoT.

Визначальною характеристикою IoT є всеохоплюючий, часто непрозорий збір і безперебійне зв'язування даних користувачів для надання персоналізованого досвіду. Щоб увімкнути цю функціональність, пристрої та служби IoT мають бути підключені та обмінюватися даними про взаємодію користувачів із кількома вузлами в мережі. Також необхідна послідовна ідентифікація користувачів і пристроїв у мережі.

Ці функції IoT, які створюють численні ризики для конфіденційності, часто розроблені таким чином, щоб залишатися непоміченими користувачами, щоб забезпечити якнайкращий досвід. Потенційно корисні висновки можна зробити з пов'язаних наборів даних, зокрема даних, створених за допомогою підключених пристроїв і послуги. Аналітика, зроблена на основі таких зібраних даних, може стимулювати персоналізоване, потенційно дискримінаційне прийняття рішень. Неможливість анонімізації даних, слабкі стандарти кібербезпеки і непрозора робота багатьох пристроїв і послуг Інтернету речей ще більше посилюють ці ризики конфіденційності та обізнаність користувачів про них. Існує фундаментальна суперечність між цілісним і непрозорим характером Інтернету речей і необхідністю інформувати користувачів і контролювати збирання і обробку їхніх персональних даних для захисту від загроз конфіденційності.

В Європейському Союзі ризики профілювання та персоналізованої аналітики, що забезпечується всеосяжним збиранням даних і безперебійним зв’язком, відображаються в нормативному ландшафті. Зокрема, GDPR містить численні положення, пов’язані з ризиками, спричиненими технологіями ідентифікації. Однак суворі правові вимоги, визначені в статтях GDPR, можуть бути недостатніми для забезпечення справедливого балансу між інтересами користувача щодо конфіденційності та інтересами розробників Інтернету речей і контролерів даних.

Відповідно до таксономії шкоди Інтернету речей, розробленої Пеппетом, існують суперечності між конфіденційністю та ідентифікацією в Інтернеті речей. Визначено чотири основні проблеми, пов'язані з розробленням та регулюванням технологій ідентифікації в Інтернеті речей:

1. зв'язок між ідентифікаційними даними користувачів та записами, отриманими з пристроїв та послуг Інтернету речей, що може призвести до потенційно деталізованого профілювання, висновків та дискримінації;
2. розкриття чутливої інформації іншим користувачам Інтернету речей та контролерам даних, яку суб'єкт даних волів би тримати в таємниці, а також перешкоджання контролю користувача над таким розкриттям;
3. створення інформації або висновків про користувача, які не можна було передбачити, коли користувач встановлював політику доступу або вирішив використовувати пристрій/послугу;
4. обмеження нагляду користувача та прозорості в управлінні ідентифікацією та профілюванням, що може сприяти порушенню недоторканності приватного життя та підривати довіру.

Проактивне вирішення цих проблем вимагає правового та етичного узгодження вибору дизайну IoT, бізнес-практик і регуляторних положень.

З огляду на необхідність повсюдного збирання і безперешкодного зв'язку персональних даних для забезпечення ідентифікації в Інтернеті речей, закони про захист даних і приватності набувають особливої актуальності. Законодавство про захист даних безпосередньо стосується питання про те, як збалансувати приватність з вільним потоком даних та іншими бізнес-інтересами.

В Європейському Союзі правовий ландшафт нещодавно зазнав значних змін завдяки GDPR, який набув чинності 25 травня 2018 року.[57] GDPR спрямований на створення гармонізованого стандарту захисту даних в ЄС з метою досягнення балансу між вільним потоком даних і фундаментальними інтересами суб'єктів даних. Оскільки IoT збирає, обробляє і поширює значні обсяги і різновиди персональних даних, GDPR повинен розглядатися як ключова структура управління для розроблення і розгортання систем IoT.

GDPR запровадив нові керівні принципи захисту даних (статті 5 і 25) і стандарти, яким повинні відповідати розробники і контролери даних для пристроїв і послуг IoT. У контексті ризиків для приватності, пов'язаних з технологіями

ідентифікації в Інтернеті речей, GDPR є особливо актуальною правовою базою через його застосовність у всіх секторах, які обробляють персональні дані, і його широкий географічний вплив.

Стандарти, що стосуються інформованої згоди, обов'язків щодо повідомлення, конфіденційності за задумом (*Privacy by Design*) і конфіденційності за замовчуванням (*Privacy by Default*), оцінки впливу на захист даних, алгоритмічної прозорості, автоматизованого прийняття рішень і профілювання, тепер застосовуються в Європі та за її межами і можуть допомогти вирішити проблему суперечностей між приватністю та ідентифікацією в Інтернеті речей.

Однак сьогоднішні положення також потребують подальшої конкретизації та впровадження в розроблення і розгортання технологій Інтернету речей, щоб мінімізувати вплив технологій профілювання та ідентифікації на конфіденційність користувачів. Ключові поняття залишаються розпливчастими або невизначеними в GDPR.

Це створює невизначеність щодо того, як збалансувати інтереси суб'єктів даних у недоторканності приватного життя та інтереси контролерів даних щодо ідентифікації та надання пов'язаних з ними послуг Інтернету речей. Наприклад, вимоги щодо повідомлення суб'єктів даних у разі порушення їхніх даних (стаття 34) застосовуються лише до порушень, які можуть становити "високий ризик для прав і свобод фізичних осіб". На жаль, "високий ризик" залишається невизначеним, а це означає, що незрозуміло, які сектори або конкретні типи даних вважаються найбільш загрозливими.

В інших випадках накладаються обмеження на обсяг захисту, який повинні забезпечувати контролери даних, що зводить до мінімуму захист, який вони пропонують від внутрішньої ідентифікації, аналітики та профілювання, що порушує недоторканність приватного життя. Наприклад, стаття 22 GDPR, яка стосується автоматизованого прийняття рішень та профілювання, обмежує визначення "автоматизованого прийняття індивідуальних рішень" рішеннями, що стосуються суб'єктів даних, "заснованими виключно на автоматизованій обробці, включаючи профілювання, яке має правові наслідки для нього або неї або аналогічним чином суттєво впливає на нього або неї". Як зазначають деякі експерти, це визначення містить невизначену термінологію (наприклад, "виключно автоматизована", "правові або подібні значущі наслідки"), що може створити лазівку, в якій номінальна участь людини в комп'ютеризованому процесі прийняття рішень зробить ці положення незастосовними.

Отже, контролери даних в Інтернеті речей стикаються з подвійним викликом: операційні системи, розроблені для безперебійної роботи у фоновому режимі, повинні інформувати користувачів і контролювати їхні дані відповідно до нечітко визначених стандартів захисту даних. Пристрої та послуги Інтернету речей часто характеризуються "максималізмом даних", тобто надмірним збором, зберіганням і передачею персональних даних на підставі того, що вони можуть виявитися корисними в майбутньому. Ця тенденція прямо суперечить закликам

до мінімалізму даних або обмеження цілей (стаття 5(1)(b)), інформованої згоди для конкретних і чітко визначених цілей (стаття 7) і конфіденційності за задумом (стаття 25).

По-друге, складна аналітика, що використовується для профілювання користувачів і надання персоналізованих послуг, може виявити непередбачувані кореляції та інформацію про суб'єктів даних. Цей аспект Інтернету речей знову ж таки суперечить очікуванням, що інформована згода буде надаватися для конкретних і чітко визначених цілей (Стаття 7). Крім того, очікується, що за певних обставин контролери даних повинні проводити оцінку впливу щодо захисту даних (DPIA; стаття 35), в якій повинні бути визначені потенційні ризики обробки. Невизначена цінність персональних даних, які генеруються та обробляються пристроями та послугами Інтернету речей, неминуче обмежує обсяг ризиків, які можна передбачити, і, таким чином, знижує рівень захисту, який фактично пропонує DPIA.

По-третє, визнаючи цю невизначеність, вимоги щодо повідомлення, накладені на контролерів даних (Статті 13,14), можуть бути недостатніми для забезпечення значущої прозорості, яка доносить до суб'єктів даних складність і невизначеність використання Інтернету речей та пов'язаних з ним зв'язків між даними, профілюванням і аналітикою. Наприклад, контролерам даних може бути дозволено повідомляти про ризики за допомогою загальних шаблонів або піктограм, орієнтованих на неспеціалізовану аудиторію, які погано інформують користувачів про їхні суб'єктивні ризики або втрату контролю над їхньою ідентичністю. Такі форми розкриття інформації обмежують здатність користувачів робити усвідомлений вибір щодо того, які додатки Інтернету речей використовувати і як управляти збором, обробкою та передачею персональних даних, необхідних для їхньої функціональності.

Нарешті, залишається незрозумілим, наскільки захищеними будуть інтереси суб'єктів даних, коли вони вступатимуть у конфлікт із "законними інтересами" контролерів даних. У зв'язку з принципом прозорості (стаття 5), статті 15-17 визначають кілька прав суб'єктів даних для здійснення контролю за розкриттям персональних даних і, таким чином, запобігання вторгненням у приватне життя або дискримінаційному поводженню, що підживлюється IoT. Однак у деяких випадках ці права можуть переважати над "законними інтересами" контролерів даних. GDPR не містить вказівок щодо досягнення справедливого балансу між інтересами обох сторін.

6.3.2. Принципи та керівні положення GDPR для забезпечення прозорості та довіри до IoT

З огляду на ризики для приватності, пов'язані з IoT, і відсутність ясності в ключових положеннях GDPR, що стосуються IoT, в майбутньому суб'єкти даних можуть зіткнутися з пристроями та послугами, які порушують юридично сумісний,

але етично небажаний баланс між приватністю та ідентифікацією. Однак GDPR може надати альтернативні підстави для вирішення суперечностей між конфіденційністю та ідентифікацією в IoT. Зокрема, керівні принципи GDPR щодо законної обробки даних (стаття 5) можуть забезпечити підстави для вирішення суперечностей між конфіденційністю та ідентифікацією в Інтернеті речей.

Керівні принципи GDPR

Можна спостерігати кілька конфліктних моментів між керівними принципами GDPR та ідентифікацією в IoT. Керівні принципи GDPR, визначені в статті 5, є наступними:

1. *Законність, справедливість і прозорість (стаття 5(1)a)*

Ці три принципи описують зобов'язання контролерів даних мати законні підстави для обробки персональних даних. Для забезпечення законності обробки ключову роль відіграє прозорість. Суб'єкти даних повинні знати про цілі обробки та отримувати відповідні повідомлення та інформацію про її обсяг. Незважаючи на те, що справедливість не визначена, Робоча група за статтею 29 та науковці вважають, що справедливість пов'язана з обізнаністю, тобто суб'єкти даних повинні бути поінформовані про обробку даних. Це особливо актуально для розробників Інтернету речей, оскільки пристрої часто збирають величезні обсяги персональних даних, деякі з яких можна вважати чутливими (наприклад, FitBit, дані про стан здоров'я). Безперешкодне впровадження цих технологій може призвести до того, що користувачі забудуть про те, що їхні дані постійно збираються [58].

2. *Обмеження мети (стаття 5(1)(b))*

Принцип обмеження мети означає зобов'язання контролерів даних використовувати зібрані дані лише для конкретних і чітко визначених цілей. Використання зібраних даних для інших цілей має бути сумісним з первинною метою. Згода суб'єкта даних або законодавство держави-члена може бути підставою для легітимізації додаткової обробки, не пов'язаної з початковою метою.

Цей принцип може створити труднощі для Інтернету речей, адже досить часто величезні обсяги даних збираються для нечітких або широко визначених цілей. Об'єднання датчиків або зв'язок існуючих, але раніше не пов'язаних між собою наборів даних, може запропонувати нові можливості для аналізу даних, які не були передбачені під час збору даних. Відповідно профілювання, зроблене на базі такої аналітики, стає можливим завдяки послугам ідентифікації, які пов'язують пристрої і дані, які вони збирають. За відсутності значущої прозорості щодо того, як використовуються дані користувачів, ці характеристики IoT суттєво підривають можливості користувачів захищати своє приватне життя і контролювати свою ідентичність.

3. Мінімізація даних (Стаття 5(1)c)

Контролери даних зобов'язані використовувати лише ті дані, які є "адекватними, релевантними та обмеженими тим, що необхідно для цілей, для яких вони обробляються". Контролери даних повинні забезпечити, щоб зібрані дані були необхідними для передбачуваного обсягу їхньої обробки, і щоб надмірні дані не збиралися за межами цього обсягу.

Для Інтернету речей контролери даних повинні встановити, що дані, які збираються, необхідні для надання їхнього продукту або послуг. Цей принцип кидає виклик типовому "максималізму даних" Інтернету речей і, відповідно, аналітиці великих даних, які вимагають збору і зв'язування великих обсягів даних для персоналізації послуг (але не для безпосередньої функціональності окремого пристрою або послуги).

4. Точність (стаття 5(1)d)

Контролери даних зобов'язані зберігати та використовувати лише точні дані. Точність означає необхідність того, щоб дані були правильними та повними щодо "цілей, для яких вони обробляються". Неправильні дані повинні бути виправлені або видалені без зайвої затримки. [57] Як наслідок, розробники Інтернету речей стикаються зі значними труднощами в управлінні та оновленні своїх наборів даних, щоб відповідати цій вимозі. Верифікація особи користувача має вирішальне значення для забезпечення точності, особливо коли одним і тим самим пристроєм потенційно можуть користуватися кілька людей. Без верифікації дані про використання від декількох користувачів можуть бути помилково записані під профілем одного користувача, що призведе до неточної обробки.

5. Обмеження зберігання (стаття 5(1)e)

Принцип обмеження зберігання зобов’язує контролерів даних не зберігати персональні дані «довше, ніж це необхідно для цілей, для яких персональні дані обробляються». Зберігання також дозволяється без зв’язку з конкретною метою обробки, коли дані «оброблятимуться виключно для цілей архівування в суспільних інтересах, наукових чи історичних дослідницьких чи статистичних цілей». Цей принцип може суперечити конкуруючим інтересам і правам суб’єктів даних (наприклад, право на доступ, право бути забутим) або іншим зобов’язанням відповідно до законів держав-членів, які вимагають довших або коротших періодів зберігання даних (наприклад, стаття 23 GDPR стосується доступу до історичних даних для кримінальних розслідувань).

6. Чесність і конфіденційність (стаття 5(1)f)

Контролери даних повинні запровадити відповідні механізми безпеки для захисту від незаконного доступу, порушень даних, втрати чи витоку даних. Для розробників IoT відповідні стандарти кібербезпеки та механізми мають бути вбудовані в дизайн пристроїв і послуг. Ця вимога може бути особливо складною

для технологій із спрощеною функціональністю або низькою обчислювальною потужністю (наприклад, RFID або WiFi), які не можуть підтримувати такі інтенсивні механізми, як шифрування. Ефективність механізмів безпеки може швидко знизитись через нещодавно виявлені недоліки або типи атак. Таким чином, цілісність і конфіденційність вимагають від розробників IoT довгострокових зобов'язань щодо виявлення нових загроз і відповідного виправлення своїх пристроїв і служб.

7. Підзвітність (стаття 5(2))

Принцип підзвітності має бути досягнутий за допомогою трьох основних обов'язків, які випливають із шести попередніх принципів. По-перше, контролери даних зобов'язані вести облік своєї діяльності з обробки даних. По-друге, вони повинні запровадити механізми «конфіденційності за задумом» і «конфіденційності за замовчуванням». По-третє, контролери даних повинні провести оцінку впливу на захист даних для обробки даних із високим ризиком. Ці положення спрямовані на те, щоб контролери даних серйозно ставилися до своїх зобов'язань щодо поваги до всіх фундаментальних принципів і могли продемонструвати відповідність, якщо це вимагається. Вимоги до оцінки впливу, характерні для IoT, ще не були виведені з вищезазначених принципів, але їх потрібно буде вирішити.

6.3.3. Позаюридичні вказівки для розробників IoT, які використовують технології ідентифікації

Сім керівних принципів GDPR мають вирішальне значення для збалансування конфіденційності, довіри та ідентифікації в IoT. Однак, профілюванню та подальшій незаконній дискримінації не завжди можна запобігти. Захист конфіденційності та стійкість систем проти кібератак також не завжди можуть бути гарантовані. Тому, замість того, щоб зосереджуватися лише на неспроможній обіцянці гарантувати конфіденційність у будь-який час, зміцнення довіри користувачів через прозорість і чесне повідомлення про ризики може бути кращим варіантом.

Відкритість і чесність щодо можливих ризиків можуть бути кращими, ніж змушувати користувачів вірити, що їхні інтереси будуть захищені в усіх випадках. Користувачам потрібна високоякісна, зрозуміла та достатньо широка інформація, щоб прийняти обґрунтоване рішення про те, чи варто довіряти системі та в кінцевому підсумку приймати її. Діалог між розробниками та користувачами має вирішальне значення, оскільки IoT є неперервним, часто прихованим і може призвести до непередбачуваної та непрозорої дискримінації. Потенційні користувачі з меншою ймовірністю приймуть IoT, якщо постачальники та програми не сприймаються як такі, що заслуговують на довіру, тобто очікувані переваги та ефективність, обіцяні IoT, можуть не матеріалізуватися, якщо ці ризики не сприймати серйозно на ранній стадії.

Керівні принципи GDPR забезпечують міцну основу для пропозиції додаткових вказівок, які можуть допомогти усунути розрив між чіткими правовими вимогами GDPR та етично бажаним дизайном і комунікацією в IoT. Вищий рівень захисту бажаний як для розробників IoT і контролерів даних, з одного боку, так і для користувачів, з іншого. Розкриття більшої кількості та більш деталізованої інформації, ніж це вимагається законом, щодо того, як IoT збирає та обробляє персональні дані користувачів, або, іншими словами, більша прозорість з боку постачальників, сприяє більшій довірі між користувачами та постачальниками.

Однак такі позаправові вказівки не повинні бути спрямовані лише на досягнення більшої прозорості в IoT шляхом усунення очевидних прогалин у законодавстві про захист даних. Забезпечення конфіденційності як заборони обробки персональних даних також є важливим. Щоб зрозуміти різницю між цими цілями, повчальним є формулювання Поля де Герта та Сержа Гутвірта щодо права на захист даних і права на приватність. Відповідно до цього підходу закон про захист даних є «інструментом прозорості», який використовується для захисту осіб від зловживань владою та шкідливої обробки даних більш впливовими особами. Стаття 8 Хартії основоположних прав Європейського Союзу закріплює «право на захист даних», яке надає особам право на обробку персональних даних чесно та на законній правовій основі. Закон про захист даних досягає цього в першу чергу шляхом опису захисних умов, яких необхідно дотримуватися під час обробки персональних даних, які забезпечуються через інформаційні зобов'язання та індивідуальні права. Заборони на обробку менш поширені в законодавстві про захист даних; скоріше мета полягає в тому, щоб описати умови для законної обробки персональних даних і забезпечити наявність достатньої інформації для суб'єктів даних для перевірки дотримання цих умов [59].

Натомість, «право на приватність» можна розглядати як «інструмент непрозорості», який надає суб'єктам даних можливість «зупинну владу» та встановлює «нормативні обмеження» для владних установ, які обробляють персональні дані [58]. Стаття 7 Декларації прав людини надає особам право приховувати та вилучати інформацію про своє приватне життя, а також забороняє необґрунтоване втручання державних органів у приватне життя осіб. Незважаючи на те, що право на приватність не є абсолютним, воно активно забороняє деякі форми втручання в приватне життя, включаючи втручання через обробку персональних даних. Захист даних входить у захист конфіденційності з умовами обробки та забезпечує наявність достатньої інформації, яка дозволяє суб'єктам даних ефективно здійснювати інформаційне самовизначення.

Отже, прозорість є додатковим і необхідним набором засобів захисту, але сама по собі є недостатньою перевіркою повноважень контролерів даних. З цього випливає, що постачальники та контролери даних повинні серйозно ставитися як до захисту даних (або прозорості), так і до конфіденційності (або непрозорості) при розробці та управлінні IoT.

Розглянемо одинадцять вказівок для відновлення справедливого балансу між прозорістю (або правом на захист даних), непрозорістю (або правом на конфіденційність) і ідентифікацією в IoT, які утворюють триступеневу модель прозорості, яка може допомогти суб'єктам даних усвідомити реальні ризики для конфіденційності, пов'язані з технологіями профілювання та ідентифікації в Інтернеті речей, і, таким чином, краще контролювати розкриття персональних даних і модифікацію своєї особи.

6.4. Триступенева модель прозорості

Розглянемо триступеневу модель прозорості, описану на основі відомих ризиків конфіденційності Інтернету речей, керівних принципів GDPR і недоліків у відповідних положеннях. Також для розробників IoT і контролерів даних запропоновано одинадцять етичних рекомендацій щодо того, як інформація про функціональні можливості IoT має надаватися користувачам понад юридично обов'язкові вимоги GDPR [57].

Як зазначено в Розділі 6.2, юридично обов'язкові положення GDPR забезпечують недостатній захист конфіденційності та ідентифікації користувачів. Тому бажано додатково дотримуватись наведених нижче вказівок, які відповідають духу закону (наприклад, керівним принципам статті 5), щоб допомогти користувачам краще зрозуміти обсяг і ризики збору, обробки та передачі персональних даних пристроями та службами IoT. Завдяки цій інформації користувачі матимуть кращі можливості для прийняття більш обґрунтованого вибору щодо використання пристроїв і послуг Інтернету речей, а також ефективнішого керування збором, обробкою та передачею їхніх персональних даних.

З цією метою в цьому розділі описано триступеневу модель прозорості, яка описує етичні ідеали щодо прозорості та розкриття інформації контролерами даних і постачальниками Інтернету речей, а також описує кілька інструментів непрозорості, які допомагають користувачам приховувати та контролювати особисту інформацію. Модель призначена для інформування розробників Інтернету речей і контролерів даних про те, як зменшити деякі ризики, пов'язані з Інтернетом речей, і відповідати духу керівних принципів GDPR, коли його юридично обов'язкові положення пропонують недостатній захист для суб'єктів даних. Ці пропозиції відповідають вимогам політики ЄС щодо визначення принципів і вказівок для пристроїв Інтернету речей.

Триступенева модель прозорості складається з одинадцяти позаправових вказівок, які відповідають трьом сферам:

1. керівні принципи GDPR (стаття 5);
2. двозначності та етично небажані обмеження в положеннях GDPR, що стосуються IoT;
3. відомі ризики для конфіденційності внаслідок профілювання та

ідентифікації в IoT.

У моделі стверджується, що давати абсолютні обіцянки щодо захисту конфіденційності користувачів є неправильним, адже таким чином постачальники IoT і контролери даних вводять в оману користувачів. Щоб досягти значущого захисту даних через прозорість і конфіденційність користувачів через непрозорість, а отже, щоб підвищити довіру користувачів, контролери даних повинні:

- відкрито описувати можливі ризики (наприклад, дискримінацію) систем Інтернету речей (наприклад, повідомлення, оцінка впливу на захист даних, політики конфіденційності);
- показати, які існують механізми для обмеження неточних або небажаних передбачень і припущень, а отже, і дискримінації на основі профілювання (наприклад, гнучкі моделі згоди, точні моделі прогнозування, право доступу, етичні практики обміну інформацією з третіми сторонами, відмова від профілювання, алгоритмічна прозорість та антидискримінаційні інструментів в автоматизованому прийнятті рішень і профілюванні);
- продемонструвати прозорі плани на випадок непередбачених ситуацій для пом'якшення ризиків (дискримінації), якщо система скомпрометована (наприклад, кіберризики, повідомлення про порушення даних, технології підвищення конфіденційності).

6.4.1. Перший крок: Прозора інформація про можливі ризики

1. Оцінка впливу на захист даних (DPIA)

Кожного разу, коли використовується «систематична та широка оцінка особистих аспектів, що стосуються фізичних осіб, яка ґрунтується на автоматизованій обробці, включаючи профілювання» та нові технології обробки даних, DPIA буде обов'язковим, якщо обробка «імовірно призведе до високого ризику для права і свободи фізичної особи». Через зростаючу важливість IoT і пов'язані з цим ризики для конфіденційності DPIA буде обов'язковим для більшості пристроїв IoT. Розробники IoT повинні будуть оцінити можливі ризики своїх пристроїв. Якщо їх оцінка вказує на високий ризик конфіденційності, попередня консультація з наглядовим органом буде обов'язковою.

Незважаючи на те, що Робоча група зі статті 29 випустила вказівки, в яких зазначено, що DPIA має бути (принаймні частково) загальнодоступним і має «постійно переглядатися та регулярно переоцінюватися», їх рекомендація не є юридично обов'язковою. GDPR не розглядає це питання. Проте рекомендується розглянути можливість публікації результатів і методів DPIA та регулярно переглядати документ, щоб допомогти зачепленим даним, регуляторам і національним наглядовим органам ефективно розглядати та реагувати на ризики, коли вони виникають.

Цей тип повторюваної прозорості допоможе суб'єктам даних краще зрозуміти можливі ризики використання продукту або послуги Інтернету речей і таким чином зробити більш обґрунтований вибір, даючи згоду на обробку даних, підвищуючи їх здатність захищати свою конфіденційність через непрозорість.48 Повідомлення про ризики може допомогти підвищити довіру до пристроїв IoT. Крім того, навіть якщо DPIA не передбачено законом, розробникам IoT все одно слід розглянути можливість оцінки своїх технологій. У випадках, коли DPIA вважається непотрібним, публічна заява про причини такого рішення може мати аналогічний ефект. Це допоможе підвищити довіру до пристроїв IoT, оскільки користувачі бачать, що контролери даних серйозно ставляться до їхньої конфіденційності, ретельно оцінюють можливі ризики та виходять за рамки того, що передбачено законом для забезпечення конфіденційності.

2. Цілі мають бути чіткими

Стаття 12 має на меті забезпечити прозору інформацію та комунікацію, щоб суб'єкти даних могли реалізувати свої права, як визначено в GDPR. Використовувана мова має бути «стислою, прозорою, зрозумілою та легкодоступною, з використанням чіткої та простої мови» [57] враховуючи те, що потенційна аудиторія є неспеціалістом. Ці вимоги є особливо важливими, коли мова йде про дітей (ст. 12, (1)).

Хоча інтуїтивно краще спілкуватися із суб'єктами даних короткою та зрозумілою мовою задля простоти та уникнення плутанини, цей підхід також обмежує якість інформації, що передається. Можливі негативні наслідки збору та обробки даних, зокрема витоки через хакерство, аналіз даних внаслідок витоку даних з датчиків, а також можливості аналітики великих даних може бути важко передати простою мовою. Більш докладна комунікація може знадобитися, коли розкриваються невизначені, але великі ризики впливу, наприклад, наслідки порушення даних або ідентифікація користувачів третьою стороною. Більш детальна інформація щодо характеру та ймовірності високого ризику впливу є важливою для того, щоб користувачі IoT мали достатньо інформації, щоб зробити обґрунтований вибір щодо подальшого використання та керування даними або вжити додаткових заходів для захисту своєї конфіденційності після порушення.

3. Піктограми не завжди можуть бути найкращим інструментом для спілкування

Для досягнення законності, справедливості та прозорості обізнаність суб'єктів даних є ключовою. GDPR запроваджує нові зобов'язання щодо прозорості. Це відображено в статтях 13-14, які встановлюють обов'язки сповіщення для контролерів даних. Серед іншого, контролери даних повинні інформувати суб'єктів даних про заплановані цілі обробки даних, контактні дані контролера даних, одержувачів персональних даних суб'єкта, період, протягом

якого персональні дані будуть зберігатися, використання профілювання та право заперечувати проти нього (Статті 13(2)(b) і 14(2) (c)), а також наявність автоматизованого прийняття рішень, включаючи профілювання (Статті 13(2)(f) і 14 (2)g)). У статті 12(7) зазначено, що інформацію про заплановані цілі обробки, зазначені у статтях 13-14, можна передати за допомогою стандартизованих значків поряд із короткими текстами [58]. Більшість пристроїв IoT мають маленькі екрани, які ускладнюють читання заяв про політику, що може бути проблематично, якщо юридично необхідна добровільна та інформована згода для обробки. Це буде у випадку, коли пристрій або послуга Інтернету речей збирає або обробляє конфіденційні дані, або коли альтернативна правова основа для обробки (наприклад, законодавство держави-члена, «законні інтереси ' контролера даних) є недоступною.

Аналогічно, оскільки надана інформація має на меті поінформувати суб'єктів даних про те, що станеться з їхніми персональними даними, і дати їм змогу прийняти обґрунтоване рішення щодо участі в цих процесах, то стандартизованих значків і коротких описів може виявитися недостатньо. Зокрема, вимога щодо інформування суб'єктів даних про логіку, задіяну в автоматизованому прийнятті рішень (включно з профілюванням), буде складною через непрозорість і складність, притаманну алгоритмічним системам [59].

Незважаючи на те, що простота та стандартизоване спілкування, які пропонують піктограми, є бажаними, їхня здатність інформувати є обмеженою, навіть якщо вони супроводжуються коротким описовим текстом. Додаткову інформацію про функціональні можливості використовуваних систем, особливо у випадку складних алгоритмів і інструментів машинного навчання, слід надавати користувачам, які хочуть дізнатися більше, особливо тому, що непрозорість і незрозумілість систем на основі штучного інтелекту є чудовим джерелом дискримінації. Дотримання цього вищого етичного стандарту прозорості допоможе гарантувати, що користувачі не будуть неналежним чином розголошувати особисті дані та інформацію, яку вони могли б залишити прихованою.

4. Конфіденційність не повинна бути ворогом прозорості

Щоб гарантувати довіру та обізнаність щодо обробки даних, GDPR не лише вимагає від контролерів даних повідомляти суб'єктів даних про передбачувані цілі обробки (статті 13-14), але також дозволяє суб'єктам даних запитувати більш-менш ту саму інформацію в будь-який час відповідно до права на доступ (стаття 15). Право на доступ надає суб'єктам даних можливість самостійно керувати конфіденційністю, не покладаючись на контролерів даних для надання відповідної та своєчасної інформації. Інформацію щодо обсягу та мети обробки даних можна отримати через право доступу, без якого інші права, такі як виправлення (Стаття

16), видалення (Стаття 17) або заперечення проти обробки (Стаття 21) неможливо ефективно застосувати.

У той же час стаття 15 (4) і пункт 63 дозволяють контролерам даних обмежувати запитувану інформацію на основі конфліктів з правами та свободами інших. Ці свободи включають права на конфіденційність інших суб'єктів даних або інтереси контролерів даних, наприклад комерційну таємницю та права інтелектуальної власності. 56 GDPR закликає до справедливого балансу між інтересами осіб, інших суб'єктів даних і контролерів даних. Таким чином, потрібен баланс між прозорістю постачальника, яка забезпечує конфіденційність (або непрозорість) користувача за визначенням, та інтересами конфіденційності (або непрозорості) інших суб'єктів даних. Простіше кажучи, користувачі не мають абсолютного права на прозорість постачальника, якщо таке розкриття ризикує відкрити конфіденційну інформацію інших суб'єктів даних.

Знайти цей баланс буде дуже складно у випадках, коли запитується інформація про профілювання та автоматизоване прийняття рішень. Використовувані профілі зазвичай створюються на основі даних референтних груп (наприклад, особисті дані інших користувачів). Групові права на конфіденційність недостатньо визнаються в чинному законодавстві про захист даних, яке зосереджується на індивідуальному суб'єкті даних, а не на колективі. 57 Цей факт може бути використаний як лазівка, щоб не розголошувати інформацію про профілювання, оскільки можна стверджувати, що ця інформація порушує права конфіденційність інших суб'єктів даних. Занепокоєння щодо конфіденційності інших не можна використовувати для запобігання доступу до відповідної інформації про обсяг і логіку автоматизованої обробки. Необхідно розробити нові підходи до того, як захистити «групову конфіденційність» 58 паралельно з індивідуальною конфіденційністю.

6.4.2. Другий крок: Прозорі процедури для зменшення ризиків профілювання

5. Впровадити антидискримінаційні інструменти та процедури

Однією з найбільш нагальних проблем, пов'язаних із IoT, є дискримінація. У пункті 39 GDPR зазначено, що «онлайн-ідентифікатори, надані їхніми пристроями, програмами, інструментами та протоколами, такі як адреси інтернет-протоколів, ідентифікатори файлів cookie або інші ідентифікатори, такі як радіочастотні ідентифікаційні мітки» можуть призвести до ідентифікації та профілювання. Це додатково підтверджується в Декларації 71, де зазначено, що «контролер повинен використовувати відповідні математичні або статистичні процедури для профілювання», щоб запобігти дискримінації або упередженню під час профілювання або автоматизованого прийняття рішень. Конфіденційні або проксі-дані, а також неточні або неповні дані можуть стати основою для дискримінаційних

ефектів, особливо коли набори даних пов’язані. Це особливо складно, коли пристрій має кілька користувачів, оскільки поведінка одного користувача може ненавмисно вплинути на прогнози про іншого користувача.

Потрібна критична оцінка походження даних. Споживачі можуть надавати неправильні дані або не повністю розуміти наслідки, якщо їхню поведінку будуть постійно контролювати. Навіть якщо користувачі усвідомлюють потенційні наслідки використання ними пристрою чи послуги, зміна налаштувань може виявитися незручною або шкідливою [58]. Отже, слід вжити організаційних заходів, щоб гарантувати точність і надійність зібраних даних, але в кінцевому підсумку покладатися на право користувачів приховувати особисту інформацію (наприклад, підтвердження того, чи є запис точним чи ні) або свідомо надавати неправдиву інформацію заради непрозорості або неясності.

Крім того, обробка даних також може призвести до неочікуваних упереджень, оскільки потенційні зв’язки між категоріями даних, які часто виявляються лише шляхом агрегування та зв’язування різнорідних наборів даних, можуть бути невідомі на момент збирання даних. Слід запровадити такі інструменти, як етичний алгоритмічний аудит, щоб виявляти дискримінацію. Слід розглянути схеми внутрішнього аудиту для захисту від дискримінації захищених груп, а також для захисту жертв непередбаченої дискримінації [58].

6. Розкажіть користувачам про припущення та висновки

Відповідно до пункту 63 статті про право доступу (стаття 15), воно має на меті «інформувати користувачів про законність обробки та перевіряти її». Слід надати прямий доступ до даних, які зберігаються, якщо це можливо. Це дозволяє не лише перевірити точність зібраних даних, але й виправити, якщо вони є неточними. Крім того, стаття 15(1)(h) дозволяє суб’єктам даних отримувати «значущу інформацію про логіку, а також значення та передбачувані наслідки» автоматизованої обробки, включаючи профілювання. Однак розголошення детальної інформації про алгоритми, які використовуються для таких процесів, може негативно вплинути на комерційні інтереси контролерів даних, включаючи комерційні таємниці та права інтелектуальної власності.

Необхідно запровадити інструменти, які надають користувачам значущу інформацію про обсяг даних, що обробляються, і висновки, отримані на їх основі. Існуючі механізми, такі як менеджер повідомлень Google, є відправною точкою. Такі інструменти повинні надавати більше, ніж загальний огляд профілювання або автоматизованого прийняття рішень, підкріплений припущеннями та висновками на основі даних Інтернету речей, як того вимагає законодавство. Натомість, щоб допомогти суб’єктам даних зрозуміти типи зроблених висновків і керувати ними, а також забезпечити можливість надати додаткову інформацію для виправлення неточних або небажаних висновків, розкриття інформації на індивідуальному рівні є кращим. Цей вищий етичний стандарт для розкриття процесу та результатів

аналітики може допомогти оптимізувати послуги (для користувачів, які вирішують виправити проблемні висновки) і підвищити довіру користувачів, зробивши найбільш невизначене та непередбачуване використання даних IoT більш прозорим.

7. Етичні практики обміну даними

Питання щодо конфіденційності не обов'язково стосуються лише контролерів даних, які спочатку збирали особисті дані користувача через пристрої та служби Інтернету речей. Навпаки, треті сторони, з якими контролери даних діляться зібраними даними, також можуть становити ризик для конфіденційності користувачів, оскільки навряд чи можна уникнути можливості створення розширених особистих профілів. Таким чином даних важливою в контексті обміну даними є анонімізація. [60] Страхові компанії або роботодавці можуть, наприклад, мати більший інтерес до отримання даних для оцінки поточної поведінки. і зробити висновок про майбутні ризики, наприклад, майбутню ймовірність погіршення здоров'я, визначену за даними FitBit. GDPR вимагає, щоб одержувачі даних попереджали, якщо планується обмін даними (ст. 13 і 14).

Однак перед тим, як ділитися даними, рекомендується провести оцінку можливих ризиків. Можливості, наприклад, расової та економічної дискримінації слід оцінити перед застосуванням зібраних даних. Користувачі можуть не передбачити можливих ризиків, які можуть бути спричинені висновками, зробленими на основі їхніх даних, особливо коли набори даних надаються третім сторонам і об'єднуються для пов'язаних, але різних цілей обробки. Експерти навіть припускають, що слід розглянути «оцінку соціального впливу», яка «враховуватиме суспільні інтереси, а також інтереси та права підприємств і користувачів» і розглядати такі фактори, як практика обміну, оскільки «відносини B2B не розроблені з конфіденційністю як основним пріоритетом» [60].

Такі оцінки можуть допомогти підтримувати конфіденційність через непрозорість, гарантуючи, що конфіденційна інформація не генерується та не передається третім сторонам поза умовами, погодженими користувачем. Надзвичайні ризики, такі як дискримінація за проксі-атрибутами або аналітичні висновки щодо неспостережуваних аспектів приватного життя користувача, повинні бути виявлені та пом'якшені за допомогою таких оцінок.

8. Гнучка згода

Стаття 7 регулює динаміку влади між суб'єктами даних і контролерами даних. Згідно зі статтею 7 (4), свобода, з якою надається згода, буде оцінюватися на основі того, чи є зобов'язання ділитися даними попередньою умовою для використання послуги. Це відповідає статті 13(2)(e), яка вимагає від контролера даних вказати, чи існує «законодавча або договірна вимога або вимога, необхідна для укладення договору, а також чи зобов'язаний суб'єкт даних надавати

персональні дані та про можливі наслідки ненадання таких даних» у випадках, коли дані збираються від суб'єкта даних.

Іншими словами, політика конфіденційності, яка забороняє використання послуги через те, що суб'єкт даних відмовився поділитися всіма своїми даними (наприклад, попередньо відзначені поля), більше не буде законною. Такі домовленості також є сумнівними з етичної точки зору, оскільки вони підривають здатність користувача приховувати особисту інформацію.

Щоб задовольнити цю вимогу, бажано використовувати гнучку та налаштовану систему згоди. [60] Слід вказати, які дані необхідні для пропонованої послуги та якими даними можна ділитися добровільно. Маючи на руках цю інформацію, користувачі можуть зробити усвідомлений вибір щодо того, чи користуватися пропозиціями Інтернету речей особисто чи уникати публічних місць із підтримкою Інтернету речей.

Щодо останнього, навіть якщо таке розкриття буде потрібно, користувачі все одно будуть змушені вибирати двійковий варіант «прийми або залиш», якщо окремі форми збору даних не можуть бути відключені для кожного користувача окремо. Звичайно, перш ніж дати згоду на певні аспекти моніторингу або взагалі уникати простору, користувачі повинні бути попереджені про наявність моніторингу та обсяг збору даних. Таким чином, публічні простори являють собою унікальну проблему для балансу між прозорістю, конфіденційністю через непрозорість і перевагами пристроїв і послуг Інтернету речей.

9. Відключення та заперечення

Пристрої IoT постійно збирають дані про своїх користувачів, тому було запропоновано розглянути варіанти відключення, які вимикають відстеження. Цей підхід пов'язаний із таким положенням GDPR, як право на заперечення проти профілювання в статті 21. Рамкова основа зазначає, що щодо цілей прямого маркетингу заперечення суб'єкта даних завжди переважатиме інтереси контролерів даних. Однак, оскільки профілювання можна використовувати й для інших цілей, наприклад щоб оптимізувати послуги, контролери даних можуть скасувати заперечення, продемонструвавши законні інтереси [59].

Однак, контролерам даних рекомендується оцінити, чи потрібне профілювання для їхніх послуг, і, можливо, вони повинні діяти відповідно до запиту користувача або принаймні розглянути варіанти відмови для конкретних цілей [60]. Щоб стимулювати суб'єктів даних ділитися та давати згоду на обробку їхні дані, контролери даних повинні інформувати їх про соціальні чи індивідуальні переваги та надавати варіанти відмови від цих переваг, вимикаючи збирання даних, які не є суттєвими для функціонування пристрою чи служби. Це дає змогу користувачам обґрунтовано оцінити альтернативні витрати попереднього збору даних заради конфіденційності.

6.4.3. Третій крок: Прозорі плани на випадок непередбачених ситуацій на випадок зламу системи

10. Конфіденційність за замовчуванням і конфіденційність за задумом

У своїх принципах і різних статтях GDPR (наприклад, 6, 24, 32-34) зазначено, що слід використовувати «конфіденційність за замовчуванням» *(Privacy by Default)* і «конфіденційність за задумом» (*Privacy by Design)*, псевдонімізацію, шифрування та інші засоби підвищення конфіденційності. Такий підхід повинен допомогти підвищити довіру користувачів і суспільне визнання ідентифікації технологій, а також покращити конфіденційність користувачів. Однак, засоби підвищення конфіденційності у більшості випадків мають недоліки. Слід припустити, що достатньо мотивований супротивник завжди зможе повторно ідентифікувати користувача [61].

Замість того, щоб обіцяти, що персональні дані завжди можна захистити, слід передати реалістичні очікування щодо того, наскільки їхні дані можуть бути захищені. Бажано пояснити, що захист даних буде гарантований у міру можливостей контролера даних. Однак, контролери даних повинні пояснити, що ризики для конфіденційності залишаться навіть за оптимальних умов, таким чином надаючи користувачам реалістичну оцінку того, чи справді їх особисту інформацію можна приховати. Пояснення планів дій на випадок витоку даних може допомогти. Наприклад, які заходи застосовуються в разі атаки на системи? Як будуть пом'якшені негативні наслідки витоку даних? Також важливо визначити, наскільки ефективними будуть PET у випадках кібератак або витоку даних.

Такий тип прозорості допоможе користувачам зробити усвідомлений вибір при прийнятті рішення про використання послуги, оскільки вони матимуть більш реалістичні очікування щодо пов’язаних ризиків і пом’якшувальних факторів. Подібним чином це може змусити контролерів даних прийняти більш надійні плани на випадок непередбачених обставин, які можуть служити перевагою для потенційних користувачів. Якщо прозорість і управління ризиками підвищують довіру між контролерами даних і користувачами, а більша довіра веде до більш широкого впровадження технології, тоді докладне повідомлення про те, як конфіденційність за проектом і конфіденційність за замовчуванням реалізовано в пристрої або службі, може принести користь як користувачам, так і постачальникам.

11. Будьте чесними, якщо кібербезпека зазнає невдачі

Гігієна кібербезпеки тісно пов’язана із захистом конфіденційності. Безпека є однією з головних проблем в Інтернеті речей, що відображено в принципах і статтях GDPR, а також у розглянутій літературі. [60] Стаття 33 GDPR вимагатиме від контролерів даних повідомляти наглядовий орган, якщо відбувається

порушення даних, що становить «ризик для прав» та свободи фізичних осіб». Однак контролери даних повинні інформувати суб'єкта даних лише у серйозних випадках, коли наслідки порушення даних, ймовірно, становлять «високий ризик» для суб'єкта даних (стаття 34).

Незважаючи на те, що зрозуміло, що не про кожний витік потрібно повідомляти, бар'єр «високого ризику» слід серйозно переглянути або принаймні надати послідовне операційне визначення. Залишається незрозумілим, хто буде оцінювати цей ризик або як будуть сформульовані наслідки для користувачів. Наявність нижчого порогу для повідомлення про витік даних може допомогти підвищити довіру користувачів, інакше вони не будуть знати про порушення та витік даних. Постачальники IoT можуть розробити внутрішні визначення та кодекси поведінки, щоб визначити, коли існують «високі ризики», і що в таких випадках слід повідомляти суб'єктам даних.

Підводячи підсумки, варто зазначити, що дотримання запропонованих одинадцяти інструкцій, спрямованих на розробників і контролерів даних IoT можуть значно підвищити довіру користувачів до IoT системи та прийняття того, що персональні дані користувачів збираються та опрацьовуються цією системою. Рекомендації описують бажані з етичної точки зору вимоги, яких слід дотримуватися на додаток до юридично обов'язкових вимог GDPR. Щоб продемонструвати, як інструкції можуть бути застосовані на практиці та змінити вибір дизайну та практику розробників і контролерів даних IoT, розглядаються два випадки використання: IoT у громадських місцях і підключених містах, а також підключені автомобілі. Ці випадки показують, як застосування керівних принципів відрізняється залежно від типів простору, що контролюється (наприклад, публічний, приватний і змішаний), і людей, за якими здійснюється моніторинг (наприклад, неідентифіковані, відомі та випадкові «користувачі»).

7. Виклики та майбутні напрямки розвитку IoT

Про те, яке важливе місце займає Інтернет речей у сучасному світі, ще кілька років тому можна було лише мріяти. Сьогодні IoT захопив весь світ і продовжує розширювати свій вплив на різні сфери. Тим не менш, IoT також стикається з численними проблемами і викликами, які створюють перешкоди для його впровадження і поширення. Розглянемо основні проблеми та виклики, з якими стикається IoT.

7.1. Основні дослідницькі виклики

Основні дослідницькі виклики стосуються складних і критичних проблем у системі Інтернету речей, які не мають прямих або заздалегідь визначених рішень. Ці виклики вимагають широких досліджень і розвідок для того, щоб запропонувати ефективні рішення. Вони охоплюють широкий спектр пов'язаних питань і міркувань та можуть не мати чітких або остаточних відповідей, залишаючи простір для постійних досліджень, експериментів і відкриттів.

Розглянемо детальніше основні виклики у сфері Інтернету речей.

Побудова інтелектуальних середовищ на основі парадигми IoT

Створення розумного середовища вимагає величезної кількості пристроїв, датчиків і додаткових технологій, які полегшують їх взаємозв'язок. Управління цією великою кількістю об'єктів є першочерговим завданням у сфері Інтернету речей та інтелектуальних середовищ. Крім того, важке завдання збирання, зберігання та проведення ефективного аналізу величезних обсягів даних залишається серйозною проблемою і створює проблеми зіткнення в межах IoT.

Робота з великими обсягами пристроїв і даних в IoT вимагає управління. Одним з підходів є використання децентралізованих систем замість централізованих, що зменшує обсяг даних, які надсилаються в хмару для обробки. Такі методи, як фільтрація, стиснення та балансування навантаження, можуть ще більше зменшити розмір даних. Використання технологій Інтернету речей з надійними можливостями управління та обслуговування пристроїв також є корисним. Крім того, використання технологій великих даних, таких як Hadoop і Spark, дозволяє ефективно обробляти значні обсяги даних IoT. Такий цілісний підхід забезпечує готовність до розширення ландшафту Інтернету речей.

Сумісність

Об'єднання пристроїв різних виробників у мережу Інтернету речей може створювати проблеми з моніторингом та управлінням. Різні галузі зараз покладаються на різні стандарти для підтримки своїх додатків. З огляду на величезні обсяги даних, різноманітні типи пристроїв і присутність різних організацій, використання стандартних інтерфейсів набуває вирішального значення. Ця важливість посилюється, особливо для додатків, які повинні враховувати як міжорганізаційну співпрацю, так і широкий спектр системних обмежень. Вирішення цих проблем вимагає від усіх галузей дотримання певних стандартів, але досягнення такої універсальної відповідності може бути складним і важко реалізовуваним завданням.

Масштабованість

Очікується, що в майбутньому різнорідні пристрої будуть постійно приєднуватися до мережі Інтернету речей, яка постійно розширюється. Як наслідок, зі збільшенням кількості пристроїв забезпечення безперебійного зв'язку, ефективного управління даними та загальної продуктивності системи в невеликих масштабах стає все складнішим завданням. Тому масштабованість Інтернету речей є постійним викликом для майбутнього цієї технології. Для ефективного вирішення проблем масштабованості необхідно побудувати масштабовану архітектуру, використовуючи такі технології, як модульні компоненти, балансувальники навантаження та розподілені системи.

Енергоефективність

Невеликі розумні пристрої, що входять до складу IoT систем, часто мають обмежений заряд акумулятора, який нелегко замінити. Це обмеження може призвести до глобальної енергетичної кризи та високого енергоспоживання, а також до обмежень пам'яті та обчислювальних можливостей. Як наслідок, процеси маршрутизації та ресурсоємні додатки можуть не працювати ефективно на таких пристроях. Хоча деякі протоколи маршрутизації підтримують зв'язок використовуючи низьке енергоспоживання, вони все ще перебувають на ранніх стадіях розвитку, і обмежена енергія смарт-пристроїв може бути недостатньою для повного використання цих протоколів маршрутизації WSN. Щоб ефективно вирішити ці проблеми, важливо наголосити на створенні малопотужного обладнання та впровадженні енергоефективних протоколів, таких як MQTT-SN або CoAP, замість того, щоб покладатися на більш енергоємні альтернативи, такі як HTTP. Крім того, використання бездротових оновлень прошивки (OTA) може гарантувати, що пристрої залишатимуться оптимізованими та без помилок, таким чином зменшуючи потребу у фізичних візитах для технічного обслуговування. Інший ефективний підхід - циклічний режим роботи, який допомагає значно зменшити енергоспоживання.

Управління мобільністю

Управління мобільністю в IoT означає здатність безперешкодно керувати пристроями, які переміщуються в мережі. Це дуже важливий аспект, оскільки багато пристроїв Інтернету речей не є стаціонарними і потребують зв'язку при зміні місця розташування. Присутність мобільних пристроїв у мережах IoT може призвести до проблем з ефективною роботою протоколів маршрутизації та мереж IoT. Сьогодні методи, що використовуються для пристроїв, які рухаються, наприклад, у сенсорних мережах, мобільних спеціальних мережах та автомобільних мережах, не можуть ефективно вирішувати різні проблеми, пов'язані з маршрутизацією, оскільки ці датчики мають обмежену обчислювальну потужність та енергетичні ресурси. Для вирішення цих проблем системи IoT використовують різні методи і протоколи управління мобільністю, спрямовані на забезпечення надійного і безперебійного зв'язку для мобільних пристроїв в екосистемі IoT.

Вартість технічного обслуговування та послуг

Мережа IoT складається з величезної кількості пристроїв, що використовують різні дорогі технології зв'язку. Це неминуче призводить до збільшення витрат на обслуговування та ремонт цих численних пристроїв і з'єднань. Отже, важливим завданням є вирішення цієї проблеми шляхом розроблення пристроїв і датчиків, які потребують мінімального обслуговування.

Проблема з відключенням інтернету

Порушення зв'язку з Інтернетом, який є ключовим для роботи IoT, призводить до зниження продуктивності додатків IoT та погіршення якості послуг. Крім того, обмеження на кількість пристроїв, які можуть одночасно взаємодіяти з базовою станцією, обмежують доступ користувачів до цих послуг. Ця проблема є особливо проблематичною у віддалених або ненадійних мережевих умовах, де підтримка постійного інтернет-з'єднання виявляється складним завданням. Отже, вирішення проблеми відключень інтернету в IoT є вкрай важливим для підтримки надійності та ефективності систем IoT.

Обробка, аналіз та управління даними

Процедура обробки, аналізу та управління даними є надзвичайно складною через неоднорідність пристроїв Інтернету речей та великі масштаби генерації даних. Наразі більшість систем використовують централізовані хмарні системи для виконання обчислювально складних завдань і передавання даних. Однак, постійне занепокоєння викликають обмеження традиційних хмарних архітектур, коли мова йде про ефективну обробку величезних обсягів даних, що генеруються і використовуються пристроями з підтримкою Інтернету речей. Крім того, ці архітектури намагаються задовольнити відповідні обчислювальні вимоги, одночасно дотримуючись чітких

часових обмежень. Для вирішення цієї проблеми більшість систем наразі покладаються на існуючі рішення, такі як мобільні хмарні обчислення та туманні обчислення, які використовують периферійну обробку.

Інші виклики

Окрім згаданих викликів, технологія Інтернету речей стикається з кількома іншими проблемами. Широке впровадження пристроїв і технологій Інтернету речей у поєднанні з нашим способом життя призвело до того, що користувачі стали дуже залежними від додатків Інтернету речей. Ця залежність є особливо критичною у сфері охорони здоров'я, де пацієнти значною мірою залежать від медичних додатків. Більше того, пристрої Інтернету речей іноді можуть несподівано втручатися в діяльність людини, що призводить до непередбачуваної та автономної поведінки.

Мережа Інтернету речей вносить невизначеність, ускладнюючи розмежування між фізичними та віртуальними пристроями і навіть людьми через легкість трансформації між цими категоріями. Контроль якості та трафіку став складнішим через мініатюризацію та величезну кількість пристроїв Інтернету речей. Управління унікальними ідентифікаторами для кожного пристрою Інтернету речей також викликає все більше занепокоєння.

Крім того, IoT виходить за межі географічних кордонів, і такі додатки, як охорона здоров'я, пропонують послуги на міжнародному рівні. Держави стикаються з викликами, пов'язаними з глобальним поширенням Інтернету речей, оскільки дані, отримані в межах їхніх кордонів, можуть бути зібрані і передані постачальникам послуг, розташованим у будь-якій точці світу, що викликає занепокоєння щодо конфіденційності даних і юрисдикції.

Вирішення цих багатогранних проблем вимагатиме ретельного розгляду та міжнародної співпраці для забезпечення ефективного та безпечного впровадження технології Інтернету речей.

7.2. Етичні міркування

Термін "етична проблема" відноситься до ситуації, що характеризується зіткненням моральних принципів, цінностей або етичних норм [58]. Сфера Інтернету речей стикається з цими етичними проблемами, змушуючи окремих осіб або організації робити складний вибір в умовах конфлікту інтересів. Ці рішення часто стосуються визначення того, що є етично правильним або неправильним.

Існує п'ять основних категорій, на які поділяють етичні проблеми, пов'язані з Інтернетом речей [63]. Метою постановки цих питань є захист прав на недоторканність приватного життя шляхом регулювання того, як організації управляють інформацією, що генерується пристроями IoT. Ці етичні стандарти, розроблені для встановлення керівних принципів для організацій, повинні також

викликати занепокоєння окремих осіб щодо конфіденційності, оскільки вони слугують правовими гарантіями для захисту людей.

1. *Міркування щодо конфіденційності інформації*: Організації повинні поводитися з отриманими даними відкрито і прозоро. За винятком особливих випадків, вони повинні пропонувати особам вибір, дозволяючи їм не розкривати свою особу або використовувати псевдонім.
2. *Збирання інформації*: Організації можуть збирати запитувані дані, застосовуючи суворіші критерії для отримання "чутливої" інформації. І навпаки, вониповинні визначити свій підхід до роботи з незапитуваною інформацією. В обох ситуаціях організації зобов'язані визначити обставини збирання такої інформації та попередньо повідомити про це відповідні сторони.

3. *Управління даними*: Організації повинні визначити ситуації, в яких вони можуть використовувати або ділитися зібраною інформацією. За певних умов організація може використовувати персональні дані для цілей прямого маркетингу. Тим не менш, вони мають можливість розкривати їх на міжнародному рівні, але перед цим вони повинні встановити гарантії, які будуть використовуватися для захисту цієї інформації.

4. *Цілісність інформації*: Організації повинні збирати та обмінюватися точною, актуальною та вичерпною інформацією. Необхідно вживати розумних запобіжних заходів для запобігання зловживанню, втручанню, втраті та несанкціонованому доступу, зміні чи розголошенню інформації.

5. *Виправлення та доступність інформації*: Запитуючи доступ до своєї інформації, суб'єкти владних повноважень повинні чітко сформулювати свої обов'язки щодо надання доступу та внесення виправлень до інформації, якою вони володіють. Це передбачає зобов'язання надавати доступ та вносити необхідні зміни, за винятком випадків, коли застосовується певний виняток.

Висновки

Інтернет речей швидко став невід'ємною частиною 21го століття, покращуючи процес прийняття щоденних рішень і відкриваючи інноваційні споживчі послуги, такі як оплата за фактом використання. Безперешкодна інтеграція розумних пристроїв і технологій автоматизації революціонізувала кожен аспект нашого життя. Однак, на тлі цього технологічного дива ми повинні визнати, що існують значні проблеми, пов'язані з безпекою, конфіденційністю, правами інтелектуальної власності, захистом і довірою. Ці проблеми продовжують вимагати подальшого дослідження.

У навчальному посібнику надано всебічний огляд Інтернету речей для новачків, які прагнуть дослідити цю сферу і отримати глибоке розуміння, щоб розробляти власні IoT системи. Розглянуто фундаментальні концепції Інтернету речей, історичний розвиток, архітектуру, переваги та таксономію технології. Досліджено різноманітні застосування в таких сферах, як розумні міста та охорона здоров'я, а також розглядаються виклики та можливі майбутні напрямки. Також посібник може бути корисним для дослідників, зацікавлених у розробленні практичних проектів Інтернету речей або у створенні нових теоретичних підходів у сфері Інтернету речей, забезпечуючи їх глибоким розумінням різних аспектів Інтернету речей. Це, своєю чергою, забезпечує хорошу основу для дослідників, які зацікавлені в розробленні реалістичних проектів IoT або розробленні нових теоретичних підходів в області IoT набуваючи глибоких знань у різних аспектах Інтернету речей.

Поширення послуг IoT вимагає, щоб були гарантовані безпека та конфіденційність. Проведений огляд публікацій та робіт наочно демонструє, наскільки багато залишається невирішених проблем, проливає світло на напрями досліджень у галузі безпеки IoT. Досі не сформульовано єдиної концепції щодо вимог безпеки та конфіденційності у такому різнорідному середовищі із застосуванням різних технологій та стандартів зв'язку. Відповідні рішення необхідно розробити та реалізувати. Вони повинні бути незалежними від платформ і дозволяти гарантувати контроль доступу та конфіденційність користувачів та речей, надійність серед пристроїв та користувачів, дотримання певних політик безпеки асності та конфіденційності. Потрібно проведення науково-дослідної роботи з напряму забезпечення безпеки IoT у мобільних пристроях, яке набуває все більшого поширення сьогодні. Багато зусиль докладається світовою науковою спільнотою для вирішення існуючих невирішених завдань. При цьому в процесі роботи з'явиться безліч нових питань, з якими доведеться зіштовхнутися.

Список використаної літератури

[1] Z. Mei and L. Yangqun, "Internet of Things Experiment Platform Based on Open Source Ecosystem," 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA), Xiangtan, China, 2019, pp. 263-269, doi: 10.1109/ICSGEA.2019.00068. Andrianandrianina Johanesa, T.V.; Equeter, L.; Mahmoudi, S.A. Survey on AI Applications for Product Quality Control and Predictive Maintenance in Industry 4.0. Electronics 2024, 13, 976. https://doi.org/10.3390/electronics13050976

[2] Internet of Things. URL: https://www.britannica.com/science/Internet-of-Things [дата звернення: 2.09.2023].

[3] Sun, X.; Zhao, C.; Li, H.; Yu, H.; Zhang, J.; Qiu, H.; Liang, J.; Wu, J.; Su, M.; Shi, Y.; et al. Wearable Near-Field Communication Sensors for Healthcare: Materials, Fabrication and Application. Micromachines 2022, 13, 784. https://doi.org/10.3390/mi13050784 W. Contributors, “Internet of things,” 2023. [дата звернення: 2.09.2023].

[4] Xie, R.; Chen, M.; Liu, W.; Jian, H.; Shi, Y. Digital Twin Technologies for Turbomachinery in a Life Cycle Perspective: A Review. Sustainability 2021, 13, 2495. https://doi.org/10.3390/su13052495

[5] W. Noonpakdee, "Challenges in promoting the Internet of Things Ecosystem for a government," 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 2023, pp. 704-708, doi: 10.1109/ICUFN57995.2023.10199849.

[6] W. Najib, S. Sulistyo and Widyawan, "Trust Based Security Model in IoT Ecosystem," 2022 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2022, pp. 195-199, doi: 10.1109/ICITISEE57756.2022.10057930.

[7] What is cybersecurity URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity [дата звернення: 2.09.2023

[8] Schwab, K. (2016) The Fourth Industrial Revolution. World Economic Forum.

[9] ARPANET [Електронний ресурс] // DARPA. – URL: https://www.darpa.mil/about-us/timeline/arpanet. – [дата звернення: 1.09.2023].

[10] The little-known story of the first IoT device URL:https://www.ibm.com/blog/little-known-story-first-iot-device/– [дата звернення: 5.09.2023].

[11] V. Gazis, "A Survey of Standards for Machine-to-Machine and the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 482-511, Firstquarter 2017, doi: 10.1109/COMST.2016.2592948.

[12] Weiser, M. (1991) The Computer for the 21st Century. Scientific American, 265, 94-104. http://dx.doi.org/10.1038/scientificamerican0991-94

[13] Foote, K.D. (2022, January), A Brief History of the Internet of Things, Dataversity, URL: https://www.dataversity.net/brief-history-internet-things/). [дата звернення: 2.09.2023].

[14] IEEE-USA Communications & Information Policy Committee (CCIP), RFID: The State of Radio Frequency Identification (RFID) Implementation and Policy Implications , IEEE, 2005.

[15] M. Saifuzzaman, T. N. Ananna, M. J. M. Chowdhury, M. S. Ferdous, and F. Chowd- hury, “A systematic literature review on wearable health data publishing under differ- ential privacy,” International Journal of Information Security, vol. 21, no. 4, pp. 847– 872, 2022.

[16] State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally. URL: https://iot-analytics.com/number-connected-iot-devices/ [дата звернення: 2.09.2023].

[17] M. H. Miraz, M. Ali, P. S. Excell and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," 2015 Internet Technologies and Applications (ITA), Wrexham, UK, 2015, pp. 219-224, doi: 10.1109/ITechA.2015.7317398.

[18] Hype Cycle for the Internet of Things, 2015. URL: https://www.gartner.com/en/documents/3987602 [дата звернення: 2.09.2023].

[19] Buleje et al., "A Versatile Data Fabric for Advanced IoT-Based Remote Health Monitoring," 2023 IEEE International Conference on Digital Health (ICDH), Chicago, IL, USA, 2023, pp. 88-90, doi: 10.1109/ICDH60066.2023.00021.

[20] S. Gupta, "Role of Internet of Things (IOT) in Smart Finance and Banking," 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 467-470, doi: 10.1109/CICTN57981.2023.10140915.

[21] Industry 4.0 and Industrial IoT. URL: https://infohub.delltechnologies.com/en-US/l/ready-solutions-for-ai-data-analytics-edge-analytics-for-industry-4-0-with-confluent-platform/industry-4-0-and-industrial-iot-1/ [дата звернення: 5.09.2023].

[22] What are the keys to Industry 4.0? URL: https://www.velatia.com/en/blog/what-are-the-keys-to-industry-4-0/ [дата звернення: 5.09.2023].

[23] What is Industry 4.0? URL: https://www.calsoft.com/what-is-industry-4-0/ [дата звернення: 5.09.2023].

[24] Houbing Song; Glenn A. Fink; Sabina Jeschke, "Legal Considerations of Cyber-Physical Systems and the Internet of Things," in Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications , IEEE, 2017, pp.93-115, doi: 10.1002/9781119226079.ch5.

[25] Iureva, R.A., Kremlev, A.S., Subbotin, V., Kolesnikova, D.V., Andreev, Y.S. (2020). Digital Twin Technology for Pipeline Inspection. In: Czarnowski, I., Howlett, R., Jain, L. (eds) Intelligent Decision Technologies. IDT 2020. Smart Innovation, Systems and Technologies, vol 193. Springer, Singapore. https://doi.org/10.1007/978-981-15-5925-9_28

[26] Y. Wang, C. -F. Chen, P. -Y. Kong, H. Li and Q. Wen, "A Cyber–Physical–Social Perspective on Future Smart Distribution Systems," in Proceedings of the IEEE, vol. 111, no. 7, pp. 694-724, July 2023, doi: 10.1109/JPROC.2022.3192535.

[27] NIST IoT principles. URL: https://www.nist.gov/itl/applied- cybersecurity/nist-cybersecurity-iot-program/principles [дата звернення: 5.09.2023].

[28] David Nunes; Jorge Sa Silva; Fernando Boavida, "Future of Human-In-the-Loop Cyber-Physical Systems," in A Practical Introduction to Human-in-the-Loop Cyber-Physical Systems , IEEE, 2018, pp.239-239, doi: 10.1002/9781119377795.part3

[29] ISO 23247-1:2021 Automation systems and integration Digital twin framework for manufacturing. URL: https://www.iso.org/ru/standard/75066.html [дата звернення: 25.09.2023].

[30] Grieves, Michael. (2002). SME Management Forum Completing the Cycle: Using PLM Information in the Sales and Service Functions.

[31] Glaessgen, E.; Stargel, D. The digital twin paradigm for future NASA and US Air Force vehicles. In Proceedings of the 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference 20th AIAA/ASME/AHS Adaptive Structures Conference 14th AIAA, Honolulu, HI, USA, 23–26 April 2012; p. 1818.

[32] What's New in the 2022 Gartner Hype Cycle for Emerging Technologies. URL: https://www.gartner.com/en/articles/what-s-new-in-the-2022-gartner-hype-cycle-for-emerging-technologies [дата звернення: 5.09.2023].

[33] Anaya, V., Alberti, E., Scivoletto, G. (2024). A Manufacturing Digital Twin Framework. In: Soldatos, J. (eds) Artificial Intelligence in Manufacturing. Springer, Cham. https://doi.org/10.1007/978-3-031-46452-2_10

[34] Digital Twins. URL: https://www.it.ua/knowledge-base/technology-innovation/cifrovoj-dvojnik-digital-twin [дата звернення: 8.09.2023].

[35] Digital model, digital shadow, or digital twin – what is at the core of data-driven shipbuilding? URL: https://www.cadmatic.com/en/resources/blog/digital-model-digital-shadow-or-digital-twin/ [дата звернення: 8.09.2023].

[36] Digital Twins and AI: Transforming Industrial Operations. URL: https://www.reliableplant.com/Read/31897/digital-twins-ai [дата звернення: 10.09.2023].

[37] Fett, M.; Kraft, M.; Wilking, F.; Goetz, S.; Wartzack, S.; Kirchner, E. Medium-Level Architectures for Digital Twins: Bridging Conceptual Reference Architectures to Practical Implementation in Cloud, Edge and Cloud–Edge Deployments. Electronics 2024, 13, 1373. https://doi.org/10.3390/electronics13071373

[38] Singh, P.; van Gulijk, C.; Sunderland, N. The BowTie as a Digital Twin: How a BowTie Looks Different from a Data Perspective. Safety 2024, 10, 34. https://doi.org/10.3390/safety10020034

[39] Digital twin market: Analyzing growth and emerging trends URL: https://iot-analytics.com/digital-twin-

market-analyzing-growth-emerging-trends/ [дата звернення: 10.11.2023].
[40] The Internet Of Things 2015: Explaining everything you need to know about the IoT URL: https://www.linkedin.com/pulse/internet-things-2015-explaining-everything-you-need-know-greenough/ [дата звернення: 10.11.2023].
[41] Deploy and review the continuous patient monitoring application template. URL: https://learn.microsoft.com/en-us/azure/iot-central/healthcare/tutorial-continuous-patient-monitoring [дата звернення: 10.11.2023].
[42] Atlam, H.F., Wills, G.B. (2020). IoT Security, Privacy, Safety and Ethics. In: Farsi, M., Daneshkhah, A., Hosseinian-Far, A., Jahankhani, H. (eds) Digital Twin Technologies and Smart Cities. Internet of Things. Springer, Cham. https://doi.org/10.1007/978-3-030-18732-3_8
[43] Guth, J. et al. (2018). A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences. In: Di Martino, B., Li, KC., Yang, L., Esposito, A. (eds) Internet of Everything. Internet of Things. Springer, Singapore. https://doi.org/10.1007/978-981-10-5861-5_4
[44] Abdmeziem M.R., Tandjaoui D., Romdhani I. Architecting the internet of things: State of the art. (2016) Studies in Systems, Decision and Control, 36, pp. 55 - 75, Cited 79 times. DOI: 10.1007/978-3-319-22168-7_3
[45] Tanwar S., Tyagi S., Kumar S. The Role of Internet of Things and Smart Grid for the Development of a Smart City (2018) Lecture Notes in Networks and Systems, 19, pp. 23 - 33, Cited 100 times. DOI: 10.1007/978-981-10-5523-2_3
[46] B. Pradhan, S. Bhattacharyya, and K. Pal, “Iot-based applications in healthcare devices,” Journal of healthcare engineering, vol. 2021, pp. 1–18, 2021.
[47] Elhayatmy G., Dey N., Ashour A.S. Internet of Things Based Wireless Body Area Network in Healthcare (2018) Studies in Big Data, 30, pp. 3 - 20, Cited 104 times. DOI: 10.1007/978-3-319-60435-0_1
[48] L. Agustine, I. Muljono, P. R. Angka, A. Gunadhi, D. Lestariningsih, and W. A. Weliamto, “Heart rate monitoring device for arrhythmia using pulse oximeter sen- sor based on android,” in 2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM), pp. 106–111, IEEE, 2018.
[49] M. Sundholm, J. Cheng, B. Zhou, A. Sethi, and P. Lukowicz, “Smart-mat: Recognizing and counting gym exercises with low-cost resistive pressure sensing matrix,” in Pro- ceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing, pp. 373–382, 2014.
[50] X. Chen, “Study on growth condition monitoring and management techniques of millet field based on internet of things,” Shanxi Agricultural University, 2015.
[51] S. Porto, C. Arcidiacono, and G. Cascone, “Developing integrated computer-based information systems for certified plant traceability: Case study of italian citrus-plant nursery chain,” Biosystems Engineering, vol. 109, no. 2, pp. 120–129, 2011.
[52] Q. Xie, M. Wu, J. Bao, P. Zheng, W. Liu, X. Liu, and H. Yu, “A deep learning-based detection method for pig body temperature using infrared thermography,” Computers and Electronics in Agriculture, vol. 213, p. 108200, 2023.
[53] L. Jiang and K. Sun, “Research on security traceability platform of agricultural prod- ucts based on internet of things,” in 2017 7th International Conference on Mechatron- ics, Computer and Education Informationization (MCEI 2017), pp. 146–150, Atlantis Press, 2017.
[54] Yan Z., Zhang P., Vasilakos A.V. A survey on trust management for Internet of Things (2014) Journal of Network and Computer Applications, 42, pp. 120 - 134, Cited 924 times. DOI: 10.1016/j.jnca.2014.01.014
[55] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Trans. Inf. Syst. Secur. (TISSEC), 2005, Vol. 8, № 2, pp. 228–258.
[56] Mahmoud, Magdi S., Mutaz M. Hamdan, and Uthman A. Baroudi. "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges." Neurocomputing 338 (2019): 101-115.
[57] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 20.08.2023 р.).
[58] Sandra Wachter, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review, Volume 34, Issue 3, 2018, Pages

436-449, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2018.02.002.

[59] Badii C., Bellini P., Difino A., Nesi P. Smart city IoT platform respecting GDPR privacy and security aspects, (2020) IEEE Access, 8, art. no. 8966344, pp. 23601 - 23623, DOI: 10.1109/ACCESS.2020.2968741

[60] Li C., Palanisamy B. Privacy in Internet of Things: From Principles to Technologies (2019) IEEE Internet of Things Journal, 6 (1), art. no. 8428405, pp. 488 - 505, DOI: 10.1109/JIOT.2018.2864168

[61] O'Connor Y., Rowan W., Lynch L., Heavin C. Privacy by Design: Informed Consent and Internet of Things for Smart Health, (2017) Procedia Computer Science, 113, pp. 653 - 658, DOI: 10.1016/j.procs.2017.08.329

[62] Atlam H.F., Wills G.B. IoT Security, Privacy, Safety and Ethics, (2020) Internet of Things, pp. 123 – 149. DOI: 10.1007/978-3-030-18732-3_8