2. Історія розвитку IoT

Концепція і термін для неї вперше сформульовані засновником дослідницької групи Auto-ID (англ.) при Массачусетському технологічному інституті Кевіном Ештоном (англ. Kevin Ashton) [5] в 1999 році на презентації для керівництва компанії Procter & Gamble. У презентації розповідалося про те, як всеосяжне впровадження засобів радіочастотної ідентифікації (RFID) зможе видозмінити систему управління логістичними ланцюгами в корпорації та дозволить порахувати і відстежити товари без людського втручання.

У 2004 році в Scientific American була опублікована велика стаття [7], присвячена «інтернету речей», що наочно показує можливості концепції в побутовому застосуванні: в статті наведена ілюстрація, що показує як побутові прилади (будильник, кондиціонер), домашні системи (система садового поливу, охоронна система, система освітлення), датчики (теплові, датчики освітленості і руху) і «речі» (наприклад, лікарські препарати, що забезпечені ідентифікаційної міткою) взаємодіють один з одним за допомогою комунікаційних мереж (інфрачервоних, бездротових, силових і слабкострумових мереж) і забезпечують повністю автоматичне виконання процесів (включають кавоварку, змінюють освітленість, нагадують про прийом ліків, підтримують температуру, забезпечують полив саду, дозволяють зберігати енергію і керувати її споживанням). Самі по собі представлені варіанти домашньої автоматизації були не новими, але упор в публікації робився на об'єднанні пристроїв і «речей» в єдину обчислювальну мережу, яка обслуговується інтернет-протоколами. Тому розгляд «інтернету речей» як особливого явища сприяло набуттю концепцією широкої популярності [2].

У звіті Національної розвідувальної ради США (англ. National Intelligence Council) 2008 року «інтернет речей» фігурує як одна з шести потенційно руйнівних технологій, вказується, що повсюдне і непомітне для споживачів перетворення в інтернет-вузли таких поширених речей, як товарна упаковка, меблі, паперові документи, може завдати шкоди національній інформаційній безпеці [8].

Період з 2008 по 2009 рік аналітики корпорації Cisco вважають «справжнім народженням "інтернету речей"», так як, за їхніми оцінками, саме в цьому проміжку кількість пристроїв, підключених до глобальної мережі, перевищила чисельність населення Землі [9], тим самим «інтернет людей» став« інтернетом речей ».

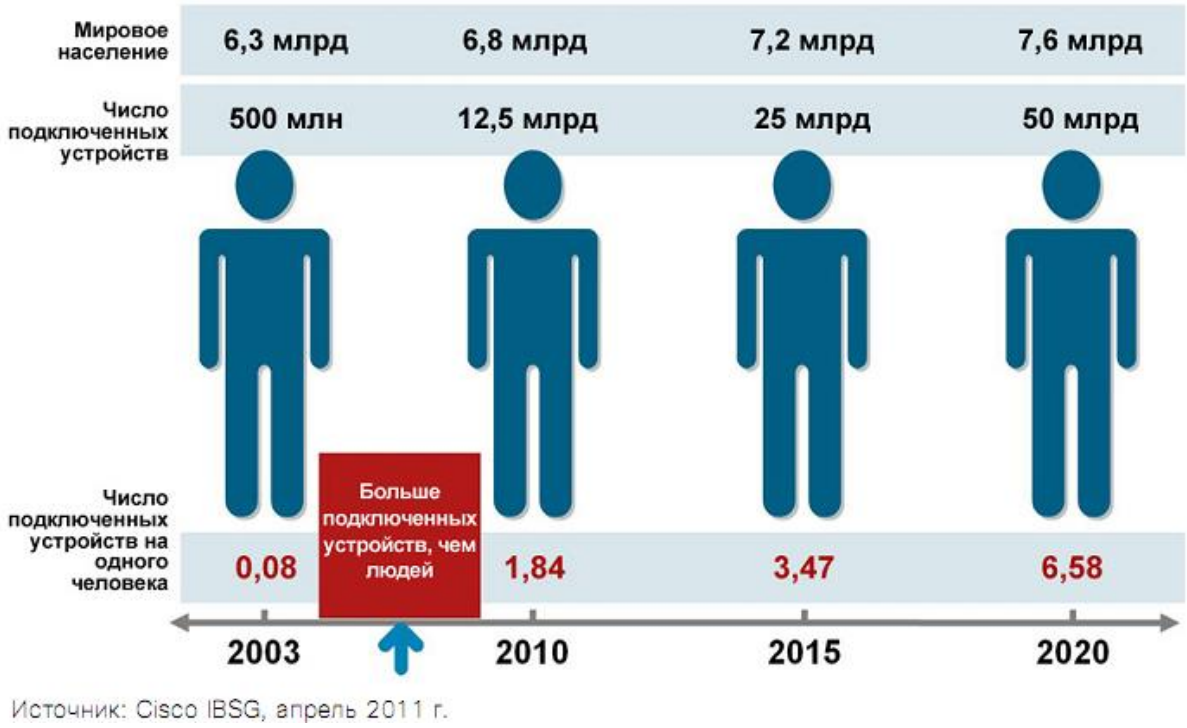


Рис. 2

З 2009 року за підтримки Єврокомісії в Брюсселі щорічно проводиться конференція «Internet of Things» [10] [11], на якій представляють доповіді єврокомісари і депутати Європарламенту, урядові чиновники з європейських країн, керівники таких компаній як SAP, SAS Institute, Telefónica, провідні вчені великих університетів і дослідницьких лабораторій.

З початку 2010-х років «інтернет речей» стає рушійною силою парадигми «туманних обчислень» (англ. Fog computing), що розповсюджує принципи хмарних обчислень від центрів обробки даних до величезної кількості взаємодіючих географічно розподілених пристроїв, яка розглядається як платформа «інтернету речей» [12].

Починаючи з 2011 року Gartner поміщає «інтернет речей» в загальний цикл зрілості нових технологій на етап «технологічного тригера» із зазначенням терміну становлення більше 10 років, а в 2012 році випущений спеціальний цикл зрілості для технологій «інтернету речей» [14].

За прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме 1,9 трлн. дол. [3]. Деякі інші аналітичні агентства висловлюють ще більш оптимістичні прогнози. Найбільші світові IT компанії вже почали перегони за лідерство на цьому ринку. Так корпорація Intel у 2014 році після випуску «SoC Edison» оголосила конкурс «Make it Wearable» («Зробіть його одягненим») з призовим фондом $1,3 млн на найкраще застосування своєї системи для концепції IoT та створила власний підрозділ «Internet of Things Solutions Group» для розвитку цього напрямку. Компанія «Google» на початку 2014 року за 3,2 млрд доларів купила невелику фірму «Nest Labs», яка займається випуском інтелектуальних термостатів [6]. Спеціалісти цієї компанії займались впровадженням на американському ринку технологій IoT.

Виробники побутової техніки також працюють у цьому напрямку. Так на виставці CES 2014 у Лас-Вегасі була представлена велика кількість побутової техніки (холодильники, телевізори, пральні машини) з можливістю підключення до інтернет.

Значення на ринку прогнозується на рівні 80 мільярдів доларів. Лідерами у розробці та впровадженні інтернету речей є країни, в який розвинена індустрія виробництва мікропроцесорів та вбудованих комп'ютерів — це США, Китай, Південна Корея. Також значний прогрес у цій галузі демонструють європейські країни та Японія.

В Україні вперше розпочато підготовку фахівців за спеціальністю «Програмні технології Інтернет речей» кафедрою інформаційних систем і технологій на факультеті інформаційних технологій у Київському національному університеті імені Тараса Шевченка 2016 року.

3. Загальні принцип побудови та архітектура IoT

Для практичної реалізації всі навколишні предмети і пристрої (домашні прилади і посуд, одяг, продукти, автомобілі, промислове обладнання та ін.) повинні бути забезпечені мініатюрними ідентифікаційними і сенсорними (чутливими) пристроями. Тоді при наявності необхідних каналів зв'язку з ними можна не тільки відслідковувати ці об'єкти і їх параметри в просторі і в часі, але і керувати ними, а також впроваджувати інформацію про них в загальну «розумну планету». У загальному вигляді з інформаційно-комунікаційної точки зору Інтернет речей можна записати у вигляді такої символічної формули:

IoT = Сенсори (датчики) + Дані + Мережі + Послуги.

По суті Інтернет речей - це глобальна мережа комп'ютерів, датчиків (сенсорів) і виконавчих пристроїв (актуаторів), що зв'язуються між собою з використанням інтернет протоколу IP (Internet Protocol)[1].

Архітектура Інтернету речей

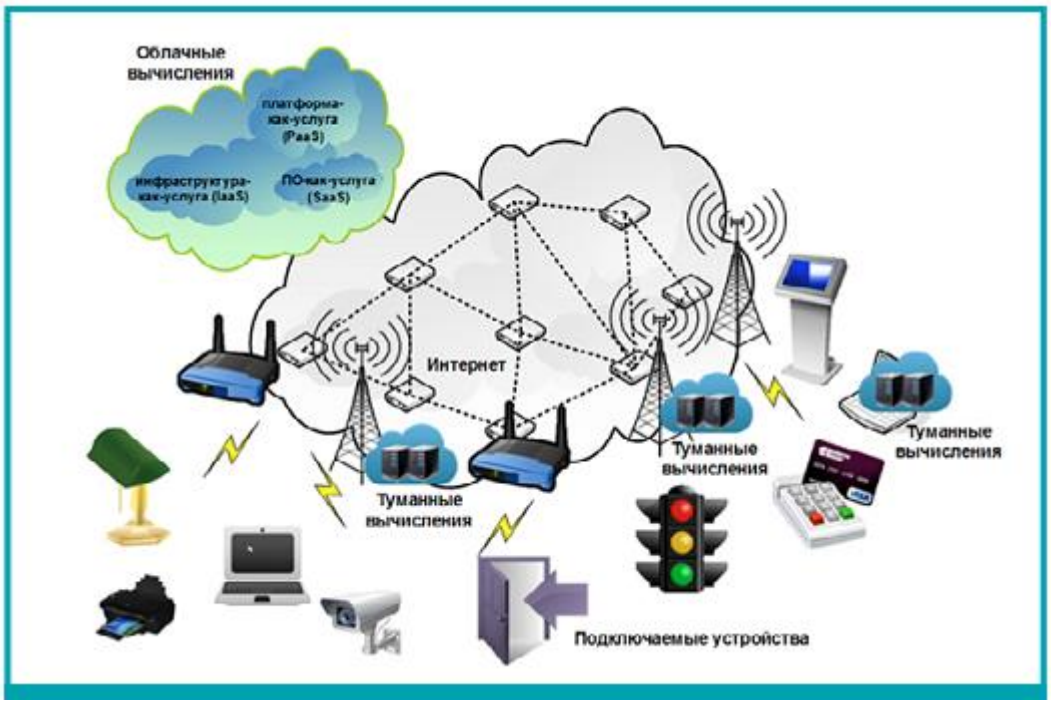


Рис. 3. Архітектура Інтернету речей

Інтернет речей або, як його ще називають, Мережа Мереж є мережею різноманітних підключених до інтернету пристроїв, що реалізують різні **моделі взаємодії** - «Річ - Річ» (Thing-Thing), «Річ - Користувач» (Thing-User) і «Річ - веб-Об'єкт »(Thing-Web Object).

З'єднання «розумних речей» (від англ .: Smart Things) в єдину мережу надає критично важливі якісні зміни для розвитку людської життєдіяльності.

Повсюдне поширення розумних речей робить нераціональним використання традиційної моделі «Клієнт - Сервер» з точки зору обміну трафіком. У місцях їх знаходження часто дуже важко забезпечити високошвидкісні канали з низькою затримкою, а власна обчислювальна потужність дозволяє проводити необхідну обробку даних, реалізуючи концепцію «туманних обчислень» (від англ.: Fog Computing) (рис.1). Функціональним елементом туманних обчислень є мікроконтролери, які об'єднуються в розподілену обчислювальну мережу. Їх завдання здійснювати зберігання та обробку інформації, що надходить, надаючи обчислювальні потужності для різноманітних прикладних задач, які здійснюють адміністрування систем без участі людини. Отримувані ж на цьому рівні структуровані дані можуть передаватися через **спеціалізовані інтерфейси програмування** додатків (API - Application Programming Interface) в різноманітні системи хмарних обчислень для подальшої обробки, в тому числі і з залученням людських ресурсів.

Як канали зв'язку використовуються конвергентні мережі на базі протоколу IP, а місця установки датчиків настільки різноманітні, що використання провідної інфраструктури дуже обмежене. Їх підключення все частіше здійснюється за допомогою бездротових технологій. До недавнього часу для цього використовувалися традиційні технології для користувальницької передачі даних - WiFi, 2G, 3G ...

Зараз в технології міжмашинної взаємодії для зв'язку все ще застосовують ієрархії протоколів, розроблені IEEE (Institute of Electrical and Electronics Engineers). Відповідно до її принципами все бездротові мережі сьогодні прийнято ділити на чотири типи:

персональні WPAN (Wireless Personal Area Network),
локальні WLAN (Wireless Local Area Network),
міські WMAN (Wireless Metropolitan Area Network)
глобальні WWAN (Wireless Wide Area Network) бездротові мережі.

Складнощі з організацією електроживлення знижують популярність мереж сімейства стандартів 802.11. Для підключення розумних пристроїв на невеликих відстанях (до 10 метрів) застосовуються стандарти, які використовують mesh-архітектуру, що володіють підвищеною живучістю і розроблені для мінімізації енергоспоживання, - 6LoWPAN, Bluetooth Low Energy (BLE), ZigBee IP і т.д. А для організації зв'язності на великих відстанях розробляється ряд спеціалізованих радіотехнологій з низьким енергоспоживанням.

На вертикальних ринках вже використовується ряд технологій - C-UNB (Cooperative Ultra Narrowband), LoRa (Long Range), але самими перспективними для інтернету речей є технології EC-GSM (Extended Coverage GSM) і NB-CIoT (Narrowband Cellular IoT), які передбачають використання мереж мобільного зв'язку. Для цієї мети планується виділяти смуги частот нижче використовуваних в мобільних мережах, і операторам необхідно тільки додати відповідні трансівери на базових станціях і оновити ПЗ.

З'єднання розумних об'єктів в єдину мережу за допомогою IP-протоколу утворює мережу мереж, продукує велику кількість найрізноманітніших телеметричних даних. І цінність одержуваної інформації цілком визначається протоколами прикладного рівня, що працюють поверх мережі.

Головним завданням при цьому є **однозначна ідентифікація кожного елемента**. З огляду на необхідну розрядність найкраще для цього підходить унікальна IPv6 адреса, що виділяється кожному пристрою в сучасних мережах. Ідентифікатор використовується не тільки для маршрутизації пакетів, але і для зіставлення з фізичними параметрами властивими пристроям (mac-адреса, RFID, Electronic Identifcation (EID), QR-кодами ...).

Розумні об'єкти, що володіють унікальним ідентифікатором в залежності від конструкції, здатні не тільки передавати потоки даних, що збираються сенсорами, а й здійснювати передачу команд для зміни стану підключених до них пристроїв.

Протоколи взаємодії між цими компонентами є стеками і тут добре зарекомендували себе стандарти, адаптовані для використання через низькошвидкісні канали. Обмін повідомленнями працює за схемою видай / підпишись (publish / subscribe). Для цього виділяється спеціалізований «сервер» для передачі інформації - брокер. Вся передана інформація поділяється за напрямками на різні канали. Різноманітні датчики передають інформацію про різні фізичні

величини по відповідних каналах, в той час як споживачі підписуються на їх отримання, дуже гнучко обмінюючись необхідною інформацією.

Описаний принцип набув широкого поширення в цілому ряді протоколів - MQTT (MQ Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol, AMQP (Advanced Message Queuing Protocol) і т.д.

Найбільш цікавим є протокол CoAP (Constrained Application Protocol). Він є адаптацією протоколу Web (web transfer protocol) для роботи за технологією міжмашинної взаємодії. Він не тільки добре інтегрується з HTTP, а й підтримує адміністрування підключених пристроїв.

Система управління відповідає за конфігурацію, оновлення програмного забезпечення та моніторинг роботи обладнання. Можливості управління розумними об'єктами істотно менші в порівнянні з «класичними» пристроями (маршрутизаторами, комп'ютерами, серверами ...) і мають свою специфіку. Для цих цілей розроблено ряд стандартів, які працюють за технологією Клієнт - Сервер - CWMP, OMA-DM, Lightweight M2M

Все частіше ми чуємо про злом пристроїв і їх використанні в шкідливих цілях, а всі питання безпеки вирішуються індивідуально кожним виробником пристроїв і програмного забезпечення. З огляду на широту поширення розумних об'єктів і ускладнення цільових атак, не дивно, що посилена увага в розробці протоколів приділяється безпеці.

Заходи щодо забезпечення безпеки можна умовно розділити за **чотирма напрямками** - підключення, ідентифікація, шифрування трафіка і безпеку додатків.

Збереження цілісності та конфіденційності даних досягається застосуванням шифрування для аутентифікації і збереження цілісності повідомлень. Процедура передбачає підтвердження даних користувача і ліквідності використовуваних сертифікатів, що досить складно реалізувати в глобальних масштабах, тому виробники часто жорстко вбудовують облікові дані в програмно-апаратний комплекс. Ця інформація дозволяє чітко ідентифікувати пристрій, але не годиться для забезпечення безпеки. На транспортному рівні питання безпеки передачі даних вирішується в рамках протоколів Transport Layer Security (TLS) і Datagram TLS (DTLS) шляхом створення захищеного тунелю для додатків.

Але незважаючи на це, додатки є найбільш вразливою частиною рішення. Їх безконтрольне поширення становить серйозну загрозу. **Надання розподіленої платформи для обробки даних різними додатками** - одна з особливостей архітектури інтернету речей, і основні тенденції в удосконаленні протоколу їх безпечного підключення OAuth 2.0 Internet of Things - виявлення розумних речей і їх аутентифікація, використання цифрових ідентифікаторів і централізоване управління доступом до ресурсів. І майбутнє глобальних туманних обчислень цілком залежить від можливості взяти процеси під контроль і забезпечити безпечну самостійну конфігурацію розподілену інформаційну мережу.

Фундаментальними характеристиками Інтернету речей є:

– **Взаємозв'язаність**. Всі пристрої взаємодіють через глобальну або локальну інфраструктуру інформаційного обміну.

– **Сервіси, орієнтовані на пристрої**. Інтернет речей здатний забезпечити семантичну узгодженість між фізичними об'єктами реального світу і їх інформаційним поданням у віртуальному просторі і об'єднати фізичні пристрої з урахуванням правил і обмежень.

– **Гетерогенність**. Пристрої в IoT неоднорідні за визначенням і можуть належати різним мережам і апаратних платформ, що не є перешкодою до взаємодії.

– **Динамічність**. Стан пристроїв змінюється постійно: включення і виключення, контекстна і технологічна інформація, включаючи місце розташування і швидкість. Кількість підключених пристроїв також може динамічно змінюватися.

– **Масштабність**. Кількість пристроїв, які будуть «спілкуватися» і отримувати керуючий вплив в десятки разів перевищить кількість вузлів в поточній мережі Інтернет. Очевидно, що кількість комунікацій, які можуть бути ініційовані пристроями, радикально перевищить можливе число з'єднань, ініціаторами яких виступають люди. Тому на перший план виходять питання інтерпретації даних, з метою їх подальшого застосування.

Можливі сценарії використання парадигми Інтернету речей (IoT) і їх взаємний зв'язок добре відображені на інфографіку, підготовленої компанією Libelium (рис. 4)

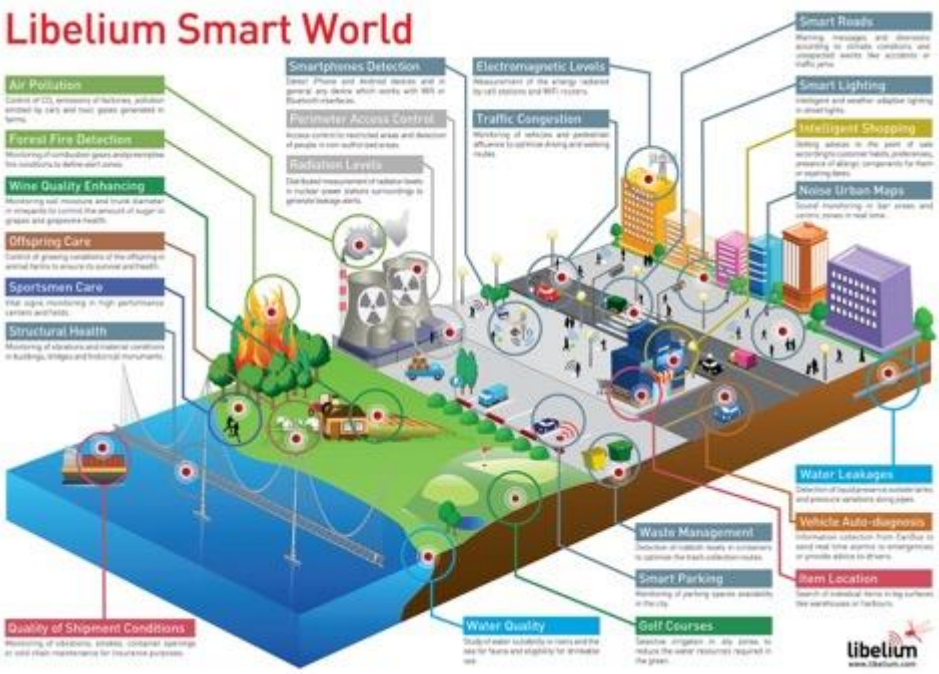


Рис. 4. «Розумний» світ

Рівні Інтернету речей

Інтернет речей включає три рівні (рис. 5):

Рис. 5.

компоненти,
структурні блоки,
система систем.

Базові можливості залежать від компонентів. Структурні блоки охоплюють технології продуктів, які виникають в результаті інтеграції нових компонентів Інтернету речей з компонентами традиційних технологій.

Система систем описує унікальні способи можливого об'єднання і інтеграції структурних блоків, а також і їх розгортання в різних галузях.

Компоненти призначені спеціально для певного застосування, а значить - і для вирішення конкретних задач.

Наприклад, в системі водопостачання використовуються вимірювальні прилади, датчики тиску і витрат, а також компоненти контролю значень.

Структурні блоки - це загальні для багатьох рішень елементи, надзвичайно важливі для успішної роботи.

Як приклади можна привести модулі комунікації, безпеки, аналітики, віддалені обчислювальні вузли і модулі оновлень.

Структурні блоки є основою багатьох рішень і включають модулі комунікації, безпеки і аналітики, віддалені обчислювальні вузли і модулі оновлення. Серед інших прикладів структурних блоків: програмне забезпечення, побутова техніка, мобільні пристрої, технології забезпечення безпеки та конфіденційності, а також комунікаційні та мережеві технології.

Сюди також входить побутова та комерційна електроніка; автомобільний, повітряний і водний транспорт; технології автоматизації будинків (включаючи моніторинг і вимірювання показників); а також інтернет- і мережеві протоколи (наприклад, IPv6).

Структурні блоки використовуються для створення систем, які потім об'єднуються в систему систем. У світі Інтернету речей відмінності визначаються підтримуваним операційним сценарієм.

Наприклад, автомобіль - це система, що складається з численних структурних блоків і компонентів.

Система систем для вуличного руху дозволяє автомобілю і водієві взаємодіяти з системами вуличного руху, щоб орієнтуватися в маршрутах і дорожній рух. Для автовиробників контекст зміщується на *системи підтримки споживачів*.

Зібрана інформація з безпеки, умов і стилю водіння, а також записи про технічне обслуговування передаються в системи підтримки клієнтів виробника, утворюючи систему систем обслуговування клієнтів. В обох сценаріях рішення Інтернету речей виконує координацію і взаємодію багатьох систем меншого масштабу, кожна з яких має власний рівнем автономності, залежно та взаємодії.

Прикладами системи систем також є IBM Smarter Cities® і інтелектуальні енергосистеми, системи контролю навколишнього середовища, наземний транспорт, авіація і аеронавтика, безпека і спостереження. Сюди ж можна віднести рішення в наступних сферах: фармацевтика, медицина і охорона здоров'я, роздрібна торгівля, ланцюжки поставок, обробка і виробництво, сільське господарство, контроль за продовольчими товарами та харчовими продуктами, ЗМІ та розваги, а також операційні сценарії і економічні обґрунтування.

4. Класифікація систем IoT

За застосуванням**: побутові – промислові**. Промислові можна поділити За сферою застосування: транспорт, сільське господарство, медицина, військові і т.д.

За важливістю наслідків застосування: **звичайні – критичні.**

За можливостями щодо руху:

статичні – динамічні.

За вимогами до часу проходження сигналу:

реального часу – мало критичні до часу.

За ступенем захищеності:

сильно захищені – слабо захищені

Інтернет речей: проблеми і перешкоди

Проблеми безпеки

Інтернет речей може викликати величезні зміни у повсякденному житті, надавши звичайним користувачам абсолютно новий рівень комфорту. Але якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, за допомогою надійного криптографічного алгоритму, замість користі вони принесуть шкоду, надавши кіберзлочинцям лазівку для підриву інформаційної безпеки. Оскільки речі із вбудованими комп'ютерами зберігають дуже багато інформації про свого власника, зокрема можуть знати його точне місцезнаходження, доступ до такої інформації може допомогти зловмисникам вчинити злочин[8].

Відсутність на даний час стандартів для захисту таких автономних мереж дещо сповільнює впровадження інтернету речей у повсякденне життя.

Є чинники, здатні уповільнити розвиток Інтернету речей. З них найсерйознішими вважаються три: **перехід до протоколу IPv6, енергоживлення датчиків і прийняття загальних стандартів.**

Перехід до IPv6. У лютому 2010 року в світі не залишилося вільних адрес IPv4.

Хоча рядові користувачі не знайшли в цьому нічого страшного, даний факт може істотно уповільнити розвиток Інтернету речей, оскільки мільярдам нових датчиків знадобляться нові унікальні IP-адреси. Крім того, IPv6 спрощує управління мережами за допомогою автоматичної настройки конфігурації і нових, більш ефективних функцій безпеки.

Живлення датчиків. Щоб Інтернет речей повністю реалізував свої можливості, його датчики повинні працювати абсолютно автономно. А тепер уявіть, що це означає: нам знадобляться мільярди батарейок для мільярдів пристроїв, встановлених по всій планеті і навіть в космосі. Це абсолютно неможливо. Потрібно йти іншим шляхом. Датчики повинні навчитися отримувати електроенергію з навколишнього середовища: від вібрації, світла і повітряних потоків.

Стандарти. В області стандартів було досягнуто значного прогресу, проте попереду нас чекає велика робота, особливо в таких областях, як безпека, захист особистої інформації, архітектура і комунікації. IEEE - одна з організацій, яка намагається вирішити зазначені проблеми за рахунок стандартизації методів передачі пакетів IPv6 по мережах різних типів.

Важливо відзначити, що перешкоди існують, але не є непереборними. Переваги ж Інтернету речей настільки великі, що людство обов'язково знайде рішення для всіх перерахованих проблем. Це лише питання часу.

ВИСНОВКИ

Впровадження повсюдного інтернету речей - це все-таки віддалена перспектива. Розумна держава, розумні міста і навіть розумний будинок на даному етапі розвитку - поки екзотика, особливо в нашій країні. Впровадження інтернету речей відбуваються не в глобальних масштабах, а всередині компаній. Технологія розумних речей здатна підвищити продуктивність праці в першу чергу в виробничому сегменті, логістичному бізнесі, транспортних і енергетичних компаніях. Складність впровадження полягає в тому, що жоден виробник не має в своєму складі закінченого рішення, що включає всі компоненти. Необхідно використання великої кількості систем від різних виробників і від їх правильного підбору та інтеграції залежить те, наскільки точно реалізоване рішення буде відповідати завданням і вимогам конкурентного середовища.

и

Навички фахівця професіонала в області IoT

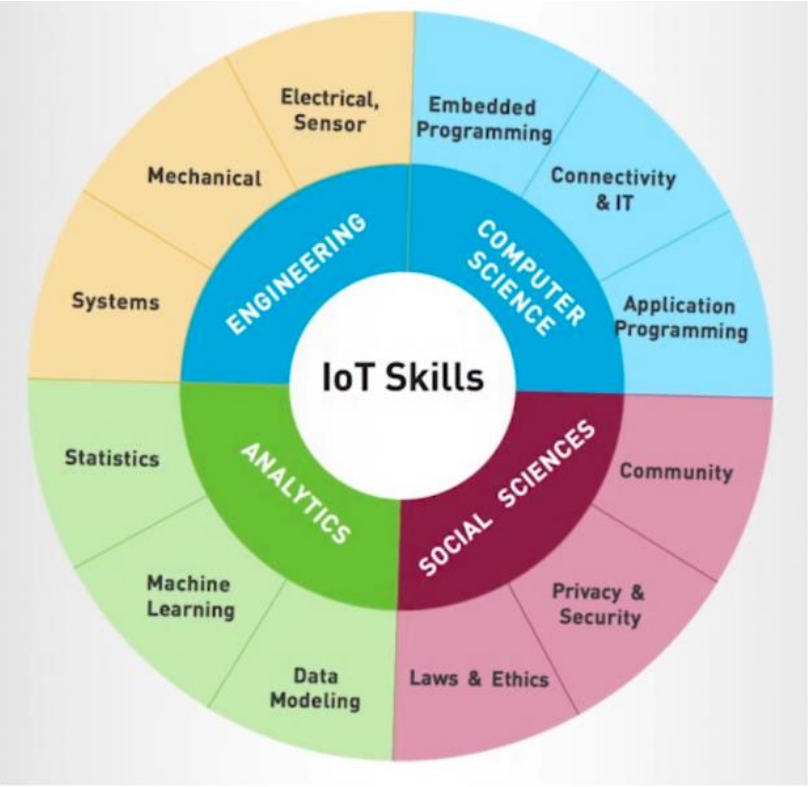

IoT Skills
ENGINEERING
COMPUTER SCIENCE
ANALYTICS
SOCIAL SCIENCES
Electrical, Sensor
Mechanical
Systems
Embedded Programming
Connectivity & IT
Application Programming
Statistics
Machine Learning
Data Modeling
Community
Privacy & Security
Laws & Ethics

Рис.1. RFID-мітка SIMATIC RF620T, що відповідає стандартам ISO 18000-6C EPC CLASS 1 GEN. По центру задано штрих-код, праворуч - Data Matrix

Рис. 2. Універсальний зчитувач RFID, штрих-кодів, кодів Data Matrix

1. Класифікація способів ідентифікації об'єктів IoT

Контактні

- магнітна карта
- чіп-карта

Безконтактні

Оптичні:

- штрих код
- Data Matrix
- OCR

Радіочастотні:

- RFID
- RTLS

2. MAC-адреса

MAC-адреса (від англ. Media Access Control - управління доступом до середовища, також Hardware Address) - унікальний ідентифікатор, який присвоюється кожній одиниці активного обладнання або деяким їх інтерфейсів в комп'ютерних мережах Ethernet.

При проектуванні стандарту Ethernet було передбачено, що кожна мережева карта (так само як і вбудований мережевий інтерфейс) повинна мати унікальний шестибайтний номер (MAC-адресу), «прошитий» в ній при виготовленні. Цей номер використовується для ідентифікації відправника і одержувача фрейму; і передбачається, що при появі в мережі нового комп'ютера (або іншого пристрою, здатного працювати в мережі) адміністратору не доведеться налаштовувати MAC-адресу цього комп'ютера вручну.

Унікальність MAC-адрес досягається тим, що кожен виробник отримує в координаційному комітеті IEEE Registration Authority діапазон з 16777216 (224) адрес і, в міру вичерпання виділених адрес, може запросити новий діапазон. Тому за трьома старшими байтам MAC-адреси можна визначити виробника. Існують таблиці, що дозволяють визначити виробника по MAC-адресі; зокрема, вони включені в програми типу arpalert.

У широкомовних мережах (таких, як мережі на основі Ethernet) MAC-адреса дозволяє унікально ідентифікувати кожен вузол мережі і доставляти дані тільки цьому вузлу. Таким чином, MAC-адреси формують основу мереж на канальному рівні моделі OSI, яку використовують протоколи більш високого (мережевого) рівня. Для перетворення MAC-адрес в адреси мережевого рівня і назад застосовуються спеціальні протоколи (наприклад, ARP і RARP в мережах IPv4, і NDP в мережах на основі IPv6).

Більшість мережевих протоколів канального рівня використовують 1 з 3 просторів MAC-адрес, керованих IEEE (або MAC-48, або EUI-48, або EUI-64). Адреси в кожному з цих просторів, теоретично, повинні бути глобально унікальними. Але не всі протоколи використовують MAC-адреси; і не всі протоколи, що використовують MAC-адреси, потребують подібної унікальності цих адрес.

Адреси на кшталт MAC-48 найбільш поширені; вони використовуються в таких технологіях, як Ethernet, Token ring, FDDI, WiMAX і інших. Вони складаються з 48 біт; таким чином, адресний простір MAC-48 налічує 2^{48} (або 281 474 976 710 656) адрес. Згідно з підрахунками IEEE, цього запасу адрес вистачить щонайменше до 2100 року.

EUI-48 від MAC-48 відрізняється лише семантично: в той час як MAC-48 використовується для мережевого обладнання - EUI-48 застосовується для інших типів апаратного і програмного забезпечення.

Ідентифікатори EUI-64 складаються з 64 біт і використовуються в FireWire, а також в IPv6 (в якості молодших 64 біт мережевої адреси вузла).

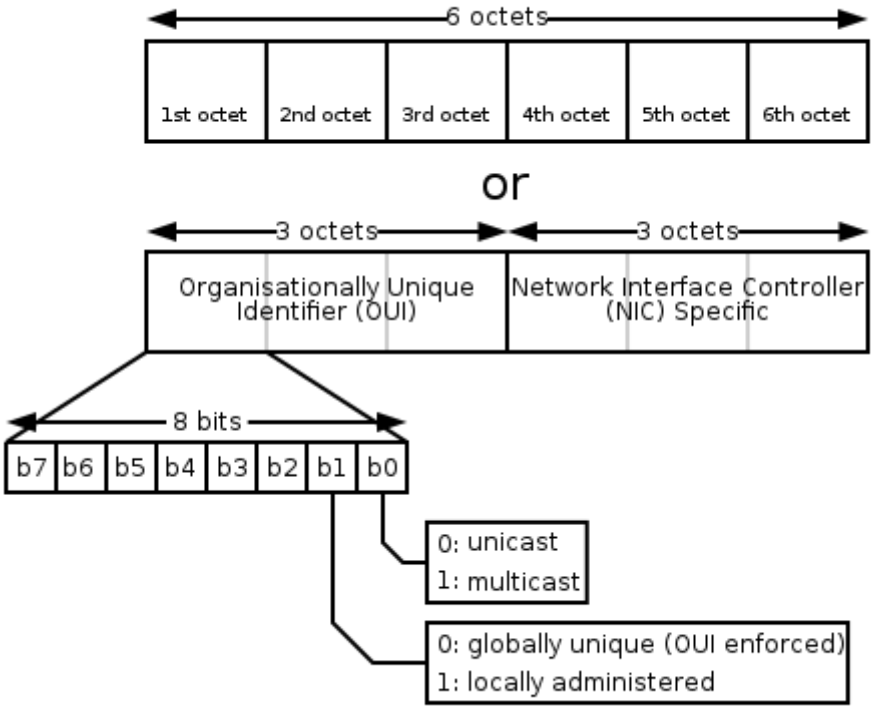


Рис. 3.

Стандарти IEEE визначають 48-розрядний (6 октетів) MAC-адресу, який розділений на чотири частини.

Перші 3 октети (в порядку їх передачі по мережі; старші 3 октети, якщо розглядати їх у традиційній біт-реверсній шістнадцятирічному запису MAC-адрес) містять 24-бітний унікальний ідентифікатор організації (OUI) [1], або код MFG (Manufacturing, виробника), який виробник отримує в IEEE. При цьому, в найпершому октеті використовуються тільки 6 старших розрядів, а два молодших мають спеціальне призначення:

- Нульовий біт - вказує: для одиночного (0) або групового (1) адресата призначений кадр;
- Перший біт - вказує, чи є MAC-адреса глобально (0) або локально (1) адміністрованою.

Наступні три октети - вибираються виробником для кожного екземпляра пристрою (за винятком мереж системної мережевої архітектури SNA).

Таким чином, глобально адмініструєма MAC-адреса пристрою є глобально унікальною і зазвичай «зашита» в апаратуру.

Адміністратор мережі має можливість, замість використання «зашитого», призначити пристрою MAC-адресу на свій розсуд. Така локально адмініструєма MAC-адреса вибирається довільно і може не містити інформації про OUI. Ознакою локально адміністрованої адреси є відповідний біт першого октету адреси.

Для того щоб дізнатися MAC-адресу мережевого пристрою, в різних операційних системах використовуються наступні команди:

- • Windows - ipconfig /all - більш детально розписує - яка MAC-адреса до якого мережевого інтерфейсу відноситься;
- • Windows - getmac /v - менш детально розписує - яка MAC-адреса до якого мережевого інтерфейсу відноситься;

Зміна MAC-адреси

Існує поширена думка, що MAC-адресу «жорстко вшитий» в мережеву карту і змінити його не можна (або тільки за допомогою програматора) - але насправді MAC-адресу легко змінюється програмним шляхом, так як значення, вказане через драйвер, має більш високий пріоритет, ніж «зашите» в плату. Однак все ж існує обладнання, в якому зміну MAC-адреси зробити неможливо без вибору програм (зазвичай це телекомунікаційне обладнання; наприклад, приставки для IP-TV (STB)).

У деяких пристроях, оснащених веб-інтерфейсом управління, можлива зміна MAC-адреси під час налаштування: більшість маршрутизаторів дозволяють дублювати MAC-адресу мережевої плати, через яку він підключений до комп'ютера.

В ОС «Windows» зміну MAC-адреси можна здійснити вбудованими засобами ОС: у властивостях мережевої плати, у вкладці «Додатково», для редагування є властивість «Мережевий адреса» (англ. «Network Address», у деяких виробників мережевих плат це властивість називається «Locally Administered Address») - дозволяє примусово привласнити потрібний MAC-адресу.

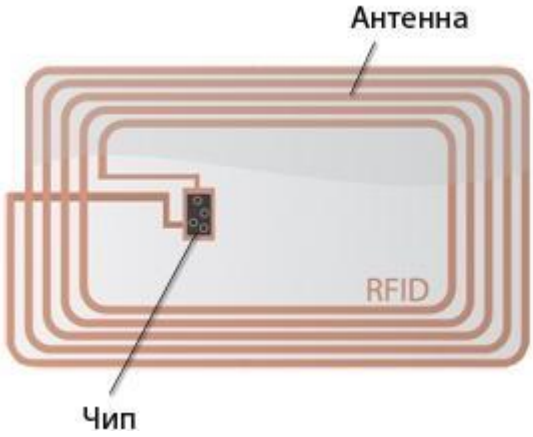
3. Радіочастотна ідентифікація (RFID): принцип роботи та застосування

RFID (Radio Frequency Identification) — це спосіб забезпечення зберігання та передачі інформації зі зручного носія-мітки в потрібне місце, з допомогою спеціальних пристроїв. Такі мітки-ідентифікатори дозволяють полегшити розпізнавання різних об'єктів: товарів в магазині, рухомих засобів при транспортуванні, допомагають визначати їх місце розташування, можуть ідентифікувати людей і тварин, не кажучи вже про широкі можливості ідентифікації документів і майна.

Що таке RFID-мітка

RFID-мітка приймає від антени електромагнітну хвилю. Хвиля активізує її, і стають можливими як запис даних на мітку, так і зчитування даних з мітки. Антена служить таким чином багатофункціональним каналом зв'язку між прийомопередавачем і міткою, повністю забезпечує процеси передачі і отримання даних.

Антени різних форм і розмірів можуть вбудовуватися в сканери, ворота, турнікети, - різні засоби для роботи з RFID-мітками, з метою забезпечення доступу до інформації, що зберігається в мітках товарів, предметів, людей, транспорту і т. д. - все, що переміщується через зону дії антени сканера, і має на собі RFID-мітки.



Антена може безперервно працювати і постійно зчитувати мітки у великій кількості, весь час опитуючи їх, або може включатися на деякий час за сигналом від оператора. Антена з прийомопередавачем і декодером часто знаходяться в одному загальному корпусі, щоб сигнал від антени відразу б демодулировался, розшифровувався і передавався б через стандартний інтерфейс на ПК для подальшої обробки отриманих даних.

Запис інформації на RFID-мітки

На мітку інформація може бути записана різними способами, в залежності від конструкції мітки. Так, RFID-мітки можуть бути наступних типів:

R/O – мітки тільки для читання (Read Only), коли дані заносяться на стадії виготовлення мітки, і більше не змінюються;

VIRUS – мітки для одноразової запису і подальшого багаторазового зчитування (Write Once Read Many), такі мітки на виробництві не

заносять ніяких даних, інформація записується користувачем один раз, потім може багаторазово зчитуватися;

- R/W - мітки для багаторазового запису і подальшого багаторазового зчитування інформації (Read/Write).

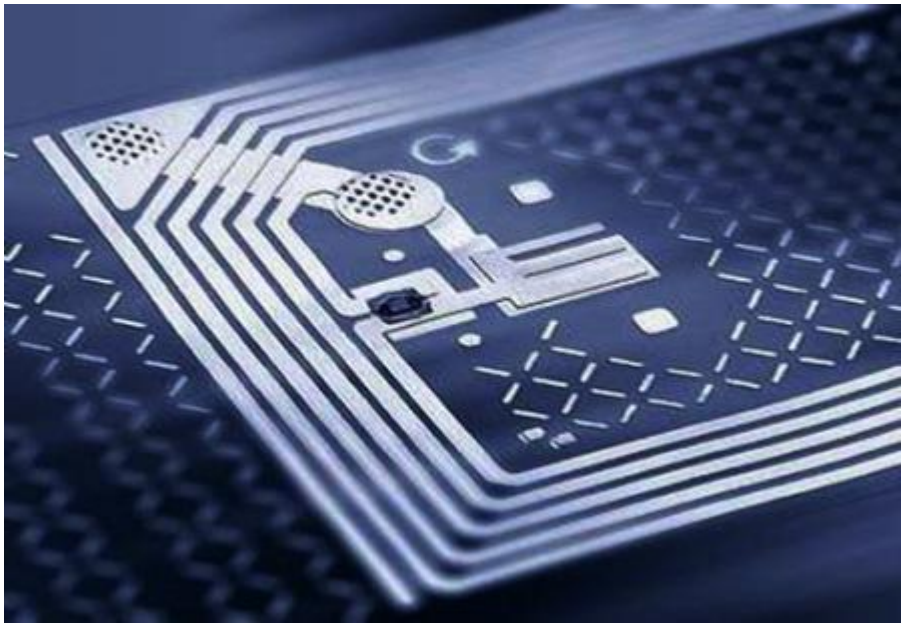
Пасивні і активні RFID-мітки

Пасивна RFID-мітка здатна працювати без власного джерела енергії, вона отримує енергію для живлення тільки від сигналу сканера. Такі мітки менше за розміром ніж активні, легше по вазі, дешевше у виробництві, і відрізняються довгим терміном експлуатації — це їх головне достоїнство.

Умовний недолік пасивної RFID-мітки — необхідно мати пристрій зчитування достатньо великої потужності. Активна мітка відрізняється наявністю вбудованої батареї або потребою в приєднуваної батареї.

Такі мітки взаємодіють з антеною сканера на більшій відстані ніж пасивні мітки, оскільки їм потрібно менше потужності від антени в процесі роботи — це головна перевага активних міток, вони відрізняються дальністю прочитування в 2-3 рази більшою, ніж пасивні мітки, до того ж активна мітка може рухатися з високою швидкістю через зону дії сканера, і все одно встигне спрацювати.

Як пасивні, так і активні мітки за можливостями запису/зчитування, одноразової/багаторазовою, - можуть широко відрізнятися незалежно від способу живлення.

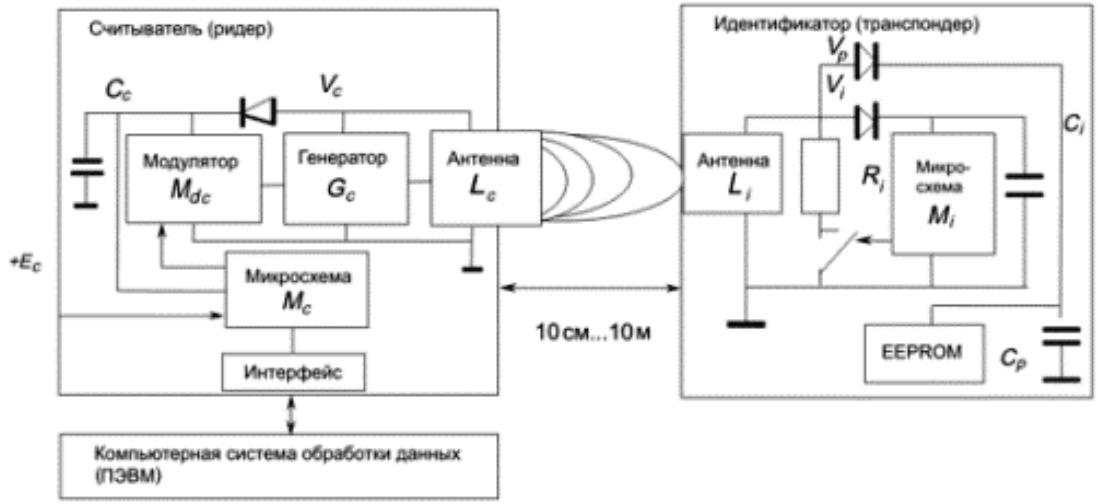


Будова RFID-мітки

Приймач, передавач, антена і блок пам'яті — ось основні частини RFID-мітки. Все окрім антени поміщається в корпус маленької мікросхеми — чіпа, тому з вигляду може здатися що мітка складається лише з многовитковой антени і чіпа. В активних мітках є ще одна частина джерело живлення, літієва батарейка наприклад.

Сама мітка зазвичай містить в собі антену, приймач, передавач, і пам'ять для зберігання даних. Енергію мітка отримує з радіосигналу антени зчитувача або від власного джерела живлення, після отримання зовнішнього сигналу, мітка відповідає

власним сигналом, у якому міститься певна ідентифікаційна інформація. Таким чином RFID-мітки — це свого роду етикетки, тільки більш розумні.



Переваги RFID-міток перед графічними ідентифікаторами

Штрих-код друкується один раз на стадії виробництва та упаковки, а інформація на RFID-мітки може бути не тільки повністю змінена, але і доповнено. Мітки можуть зчитуватися відразу у великій кількості завдяки механізму антиколізії, чого важко досягти для графічних кодів.

Незважаючи на те що матричні коди здатні вміщати відносно великі обсяги даних, які їм потрібні великі площі для нанесення кодів, наприклад, щоб штрих-кодом записати 50 байт, знадобиться аркуш формату А4, в той час як RFID-мітка з чіпом площею всього 1 квадратний сантиметр легко вмістить 1000 байт.

Запис на мітку досить швидкий, а графічні коди потрібно спочатку набирати, потім друкувати і наклеювати, та ще й зберегти цілісність зображення.

З RFID-ідентифікаторами все простіше, достатньо на стадії виробництва «імплантувати» мітку в упаковку (не обов'язково зовні), потім безконтактним способом записати дані, і мітка буде вічною (не менше 1000000 взаємодій з антеною сканера), прихованої всередині виробу мітці не страшні ні бруд, ні пил.

До того ж дані записані на мітку, цілком або частково, можна при необхідності захистити від зчитування або перезапису паролем — це надійний спосіб захисту від підробок. При цьому зчитування відбувається при будь-якому положенні мітки в зоні дії сканера — це зручніше ніж графічний код, який потрібно рівно піднести до сканера.

Частоти в залежності від області застосування

Там де потрібна висока швидкість зчитування, наприклад для контролю автомобілів у русі, вагонів на залізниці, в системах збору відходів — використовують високі частоти 850-950 МГц і 2,4-5 ГГц. Високочастотні сканери монтуються у ворота або шлагбауми, а RFID-мітка (транспондер) встановлюється, наприклад, на лобовому склі автомобіля. Дальність взаємодії мітки зі сканером становить від 4 до 8 метрів, що створює сприятливі умови для людей, оскільки зчитувальний пристрій розташовується поза межами їх досяжності.

В даний час дуже популярний середньочастотний діапазон 10-15 МГц. Він використовується в транспортних і інших аналогічних програмах, де потрібно робота з перезаписуваними картами, смарт-картами і т. д. Багато нинішні смарт-карти працюють як RFID-мітки середньохвильового діапазону.

Діапазон низьких частот 100-500 Кгц діє на невеликій відстані між сканером і об'єктом, не більше 50 см, іноді менше 10 див.

Велика антена компенсує невелику дальність взаємодії, проте перешкоди від високовольтних ліній, комп'ютерів і навіть енергозберігаючих ламп можуть перешкодити роботі системи. Але все одно у багатьох системах управління доступом (склади, прохідні) низькі частоти для роботи з безконтактними RFID-картами застосовуються. Крім того, низькочастотний діапазон використовується для безконтактної ідентифікації тварин і металевих предметів, таких наприклад як пивні кеги.

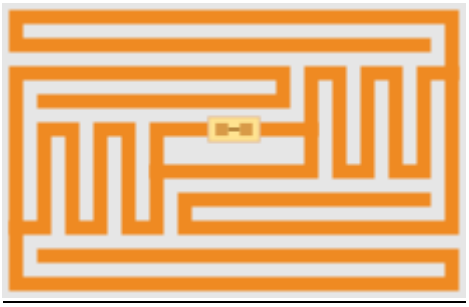
Радіочастотна ідентифікація

RFID (англ. *Radio frequency identification*) — радіочастотна ідентифікація.

Просвічена наскрізь наклейка на товар, яка містить радіомітку.

Пасивний RFID ключ в вигляді картки

Різноманітні пасивні RFID наліпки та вкладки для ідентифікації товарів в магазинах.



EPC RFID-мітка, використовується в торговій мережі Wal-Mart

Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом спеціальних міток, що несуть ідентифікаційну та іншу інформацію. Цей метод вже став основою побудови сучасних безконтактних інформаційних систем, і має стійку назву RFID-технології.

Особливості технології

- RFID-міткам не потрібен контакт або пряма видимість, дані з мітки можуть бути отримані на відстані.
- RFID-мітки читаються швидко і точно, що дозволяє виконувати велику кількість сканувань.
- RFID-мітки можна використовувати навіть в агресивних середовищах, через бруд, фарбу, пар, воду, пластмасу, деревину, а також використовувати імплантацію в тіло.
- Пасивні RFID-мітки мають фактично необмежений термін експлуатації, мають низьку собівартість.
- RFID-мітки можуть нести велику кількість інформації.
- RFID-мітки легко відстежити на порівняно невеликій відстані — метро, офіси, банки, магазини, зупинки.
- RFID-мітки можуть бути використані як для читання, так і для запису великого обсягу інформації.

Ідентифікація транспорту на в'їзді та виїзді з закритої території. Одна антена для активації радіомітки, інша для отримання закодованого сигналу. У випадку виявлення ідентифікатора в базі дозволених — ворота відкриваються.

Історія RFID міток

У 1946 році Лев Сергійович Термен винайшов для Радянського Союзу шпигунський пристрій, який дозволив накладати аудіоінформацію на випадкові радіохвилі. Звук викликав коливання діафрагми, яка трохи змінювала форму резонатора, модулюючи відбиту радіочастотну хвилю. І хоча пристрій представляв лише пасивний передавач (т.з. «жучок»), цей винахід зараховують до перших попередників RFID-технології.

Технологія, найближча до даної — система розпізнавання «свій-чужий», винайдена британцями в 1939 році. Вона активно застосовувалася союзниками під час Другої Світової Війни, щоб визначити, своїм або чужим є об'єкт в небі. Подібні системи досі використовуються як у військовій, так і в цивільній авіації. Ще однією віхою у використанні RFID-технології є робота Гарі Стокмана (Harry Stockman) під назвою «Комунікації за допомогою відбитого сигналу» (англ. «Communication by Means of Reflected Power») (доповіді IRE, стор. 1196–1204, жовтень 1948). Стокман відзначає, що «значні роботи з дослідження й розробки були зроблені до того, як були вирішені основні проблеми в зв'язку за допомогою відбитого сигналу, а також до того, як були знайдені сфери застосування даної технології».

Патент США Маріо Кардулло (Mario Cardullo) № 3,713,148 від 1973 («Пасивний радіопередавач з пам'яттю»), був, по суті, прабатьком сучасної RFID-технології. Вперше пасивний пристрій на відбитій енергії був продемонстрований в 1971 році владі Нью-Йорка і іншим потенційним покупцям як пристрій з 16 бітами пам'яті для стягування мита на дорогах. Патент Кардулло покриває використання радіохвиль, світла і звуку як засіб передачі інформації.

Оригінальний бізнес-план був представлений інвесторам в 1969 для використання у сфері транспорту (ідентифікація самохідних машин, автоматична платіжна система (система стягування мита), електронні номерні знаки, електронні платіжні відомості, водіння машин, моніторинг стану транспортних засобів), в банківській справі (електронні книги перевірок, електронні кредитні картки), у сфері безпеки (персональна ідентифікація, автоматичні ворота, спостереження) і в медицині (ідентифікація пацієнта, історії хвороби).

Перша демонстрація сучасних RFID-чипів (на ефекті зворотного розсіювання), як пасивних, так і активних, була проведена в Дослідницькій Лабораторії Лос Аламоса (англ. *Los Alamos Scientific Laboratory*) в 1973 році. Портативна система працювала на частоті 915 Мгц і використовувала 12 бітових міток.

Перший патент, пов'язаний власне з назвою RFID, був виданий Чарльзу Уолтону (Charles Walton) в 1983 році (патент США за № 4,384,288).

Класифікація RFID-міток

Існує декілька способів систематизації RFID-міток і систем:

- за робочою частотою;
- за джерелом живлення;
- за типом пам'яті.

За джерелом живлення

За типом джерела живлення RFID-мітки діляться на:

- Пасивні
- Активні
- Напівпасивні

Пасивні

Пасивні RFID-мітки не мають вбудованого джерела енергії. Електричний струм, що індукується в антені електромагнітним сигналом від зчитувача, забезпечує достатню потужність для функціонування кремнієвого CMOS-чипа, розміщеного в мітці, і передачі у відповідь сигналу.

Комерційні реалізації низькочастотних RFID-міток можуть бути вбудовані в стикер (наклейку) або імплантовані під шкіру.

У 2006 Hitachi виготовила пасивний пристрій, названий μ-Chip (мю-чип), розмірами 0,15×0.15 мм (не включаючи антену) і тонше за паперовий лист (7.5 мкм). Такого рівня інтеграції дозволяє досягти технологія «кремній-на-ізоляторі» (SOI). μ-Chip може передавати 128-бітовий унікальний ідентифікаційний номер, записаний в мікросхему на етапі виробництва. Цей номер не може бути змінений надалі, що гарантує високий рівень достовірності і означає, що цей номер буде жорстко прив'язаний (асоційований) з тим об'єктом, до якого приєднується або в який вбудовується цей чип. μ-Chip від Hitachi має типовий радіус зчитування 30 см (1 фут). У лютому 2007 року Hitachi представила RFID-пристрій, що має розміри 0,05×0,05 мм, і завтовшки, достатньою для вбудовування в лист паперу.

У наш час основна проблема RFID-пристроїв полягає в тому, що для них потрібна зовнішня антена, яка за розмірами перевершує чип у найкращому разі в 80 разів. Найменша вартість RFID-міток, які стали стандартом для таких компаній, як Wal-Mart, DOD, Target, Tesco у Великій Британії і Metro AG в Німеччині, становить приблизно 5 центів за мітку фірми SmartCode. До того ж, через розкид розмірів антен, і мітки мають різні розміри — від поштової марки до листівки. На практиці максимальна дистанція зчитування пасивних міток варіюється від 10 см (4 дюймів) (згідно зі стандартом ISO 14443) до декількох метрів (стандарти EPC і ISO 18000-6), залежно від вибраної частоти і розмірів антени. В деяких випадках антена може бути виготовлена друкарським способом.

Виробничі процеси від Alien Technology під назвою Fluidic Self Assembly, від SmartCode — Flexible Area Synchronized Transfer (FAST) і від Symbol Technologies PICA направлені на подальше зменшення вартості міток за рахунок застосування масового паралельного виробництва. Alien Technology в наш час використовує процеси FSA і HiSam для виготовлення міток, тоді як PICA процес від Symbol Technologies знаходиться ще на стадії розробки. Процес FSA дозволяє проводити понад 2 мільйони IC пластин в годину, а PICA процес — понад 70 мільярдів міток в рік (якщо його допрацюють). У цих технічних процесах IC приєднуються до пластин міток, які у свою чергу приєднуються до антен, утворюючи готовий чип. Приєднання IC до пластин і надалі пластин до антен — просторово найчутливіші елементи процесу виробництва. Це означає, що при зменшенні розмірів IC монтаж (англ. *Pick and place*) стане найдорожчою операцією. Альтернативні методи виробництва, такі як FSA і HiSam, можуть значно зменшити собівартість міток. Стандартизація виробництва (англ. *Industry benchmarks*) приведе до подальшого падіння цін на мітки при їхньому широкомасштабному впровадженні.

Некремнієві мітки виготовляються з полімерних напівпровідників. В наш час їхньою розробкою займаються декілька компаній в усьому світі. Мітки, що виготовляються в лабораторних умовах і працюють на частотах 13.56 Мгц. були продемонстровані в 2005 році компаніями POLYIC (Німеччина) і Philips (Голландія). У промислових умовах полімерні мітки виготовлятимуться методом прокатного друку (технологія нагадує друк журналів і газет), внаслідок чого вони будуть дешевші, ніж мітки на основі ІС. Це може закінчиться тим, що для більшості сфер застосування мітки почнуть друкувати так само просто, як і штрих-коди, і вони стануть такими ж дешевими.

Пасивні мітки УВЧ (ультрависокочастотні дециметрові хвилі) і НВЧ (надвисокочастотні сантиметрові і міліметрові хвилі) діапазонів (860–960 МГц і 2,4-2,5 ГГц) передають сигнал методом модуляції відбитого сигналу частоти, що несе (англ. Backscattering Modulation модуляція зворотного розсіяння). Антена зчитувача випромінює сигнал частоти, що несе, і приймає відбитий від мітки модульований сигнал. Пасивні мітки ВЧ діапазону передають сигнал методом модуляції навантаження сигналу частоти, що несе (англ. Load Modulation модуляція навантаження). Кожна мітка має ідентифікаційний номер. Пасивні мітки можуть містити перезаписувану незалежну пам'ять EEPROM-типу. Дальність дії міток становить 1—200 см (ВЧ-МІТКИ) і 1-10 метрів (УВЧ і НВЧ-мітки).

Активні

Активні RFID-мітки володіють власним джерелом живлення і не залежать від енергії зчитувача, унаслідок чого вони читаються на дальній відстані, мають великі розміри і можуть бути оснащені додатковою електронікою. Проте, такі мітки найдорожчі, а у батарей обмежений час роботи. Активні мітки в більшості випадків надійніші (наприклад, здійснюють меншу кількість помилок), ніж пасивні, завдяки особливій сесії зв'язку між міткою і пристроєм зчитування. Активні мітки, володіючи власним джерелом живлення, також можуть генерувати вихідний сигнал більшого рівня, ніж пасивні, дозволяючи застосовувати їх в агресивніших для радіочастотного сигналу середовищах: воді (включаючи людей і тварин, які в основному складаються з води), металах (корабельні контейнери, автомобілі), для великих відстаней на повітрі. Більшість активних міток дозволяють передати сигнал на відстані в сотні метрів при тривалості життя батареї живлення до 10 років. Деякі RFID-мітки мають вбудовані сенсори, наприклад, для моніторингу температури товарів, які швидко псуються. Інші типи сенсорів в сукупності з активними мітками можуть застосовуватися для вимірювання вологості, реєстрації поштовхів/вібрації, світла, радіації, температури і газів в атмосфері (наприклад, етилену).

Активні мітки зазвичай мають набагато більший радіус зчитування (до 300 м) і обсяг пам'яті, ніж пасивні, і здатні зберігати більший обсяг інформації для відправки приймачем. В даний час, активні мітки роблять розмірами не більше звичайної пілюлі і продають за ціною в декілька доларів.

Напівпасивні

Напівпасивні RFID-мітки, також їх називають напівактивними, дуже схожі на пасивні мітки, але оснащені батареєю, яка забезпечує чип енергоживленням. При

цьому дальність дії цих міток залежить тільки від чутливості приймача зчитувача і вони можуть функціонувати на більшій відстані і з кращими характеристиками.

За типом використовуваної пам'яті

За типом використовуваної пам'яті RFID-мітки діляться на:

- RO (англ. *Read Only*) дані записуються тільки один раз, відразу при виготовленні. Такі мітки придатні тільки для ідентифікації. Ніяку нову інформацію в них записати не можна, і їх практично неможливо підробляти.
- WORM (англ. *Write Once Read Many*) окрім унікального ідентифікатора такі мітки містять блок одноразово записуваної пам'яті, яку надалі можна багато разів читати.
- RW (англ. *Read and Write*) такі мітки містять ідентифікатор і блок пам'яті для читання/запису інформації. Дані в них можуть бути перезаписані багаторазово.

Зчитувачі

Прилади, які читають інформацію з міток і записують в них дані. Ці пристрої можуть бути постійно підключеними до облікової системи, або працювати автономно. Залежно від частотного діапазону мітки, дистанція стійкого зчитування і запису даних може бути різна. Розрізняють стаціонарні та мобільні.

Стаціонарні

Стаціонарні зчитувачі кріпляться нерухомо на стінах, дверях, рухомих складських пристроях (штабеляторах, навантажувачах). Вони можуть бути виконані у вигляді замка, вмонтовані в стіл або закріплені поряд з конвеєром на шляху проходження виробів.

В порівнянні з мобільними, зчитувачі такого типу зазвичай мають більшу зону читання та потужність, і здатні одночасно обробляти значний потік інформації. Стаціонарні зчитувачі на виробництві інтегруються в інформаційну систему що дозволяє поетапно фіксувати переміщення маркованих об'єктів в реальному часі, або ідентифікувати положення мічених предметів в просторі.

Мобільні

Володіють порівняно меншою дальністю дії і часто не мають постійного зв'язку з програмою контролю і обліку. Мобільні зчитувачі мають внутрішню пам'ять, в яку записуються дані з прочитаних міток (потім цю інформацію можна синхронізувати з системою обліку) і, як і стаціонарні зчитувачі, здатні записувати дані в мітку (наприклад, інформацію про проведений контроль).

Основні переваги RFID-технології

- для RFID не потрібний контакт або пряма видимість;
- RFID-мітки читаються швидко і точно (наближаючись до 100%-ої ідентифікації);

- RFID може використовуватися навіть в агресивних середовищах, а RFID-мітки можуть читатися через бруд, фарбу, пар, воду, пластмасу, деревину;
- пасивні RFID-мітки мають фактично необмежений термін експлуатації;
- RFID-мітки несуть велику кількість інформації і можуть бути інтелектуальними;
- RFID-мітки можуть бути не тільки для читання, але і з записом інформації;

Недоліки та критика RFID-технології

- В деяких випадках мітки не деактивуються повністю, є можливість повторного спрацьовування
- Мітку можна виявити на товарі і в багатьох випадках пошкодити або відірвати
- З огляду на легку можливість маскування, можуть використовуватись для шпигунства без згоди власника товару
- У випадку оплати товару карткою банку технічно залишається можливість асоціювання імені власника з товаром
- В індивідуальних випадках категорична відмова від імплантації з огляду на страх втрати приватності індивідом
- Технічно можливо збирати приватну інформацію - національність та інші дані з паспортів, куплену літературу і п.т.
- RFID-мітки відносно легко ввести в оману. Для цього необхідно щоб мітка пройшла в радіусі дії несанкційованого зчитувача, часто мобільного, який збереже інформацію з мітки у себе. Після цього достатньо прийти до точки доступу і протранслювати зчитану інформацію системі за допомогою спеціального транслятора. Ускладнює ситуацію й те, що у виготовленні транслятора не виникає ніяких складностей і його схеми є широко розповсюджені в мережі Інтернет.

Застосовування RFID систем

Використання кліпси в вусі для ідентифікації тварин в господарствах та фермах

RFID-системи застосовуються в різноманітних випадках, коли потрібен оперативний і точний контроль, відстеження і урахування численних переміщень різноманітних об'єктів. Типові застосування:

- електронний контроль за доступом і переміщеннями персоналу на території підприємств;

керування виробництвом, товарними і митними складами (особливо значними), магазинами, видачею і переміщенням товарів і матеріальних цінностей;

- автоматичний збір даних і при необхідності нарахування оплати на залізницях, платних автомобільних дорогах, на вантажних станціях і терміналах;
- контроль, планування і керування рухом, інтенсивністю графіка і вибором оптимальних маршрутів;

- громадський транспорт — керування рухом, оплата проїзду й оптимізація пасажиропотоків;
- системи електронних платежів для усіх видів транспорту, включаючи організацію платних доріг, автоматичний збір плати за проїзд і транзит, платні автостоянки;
- забезпечення безпеки (у комплексі з іншими технічними засобами аудіо- і видеоконтролю).

захист і сигналізація на транспортних засобах.

- покращення обліку й руху матеріалів у системі логістики, зокрема на складах.

Принцип роботи RFID систем

Система складаються з трьох основних компонентів:

- зчитувача "рідера",
- транспондера (так званою "міткою" або "тегом", від англ. *tag*)
- комп'ютерної системи опрацювання даних

Зчитувач має приймально-передавальний пристрій - він посилає сигнал до мітки та приймає відповідний сигнал від мітки. Мікропроцесор (пасивної мітки), який віддає сигнал живиться за рахунок індукційного струму з котушки або антени, в якій виробляється струм, коли мітка проходить через електромагнітне поле. Мітки можуть мати більш складну реалізацію з мікропроцесором, що перевіряє і декодує дані, а не просто відповідає ідентифікатором, а також пам'ять, що зберігає дані для наступної передачі, якщо це необхідно.

Основні компоненти тега — інтегральна схема, що керує зв'язком із зчитувачем і антена. Чип має пам'ять, що береже ідентифікаційний код або інші дані. Тег виявляє сигнал від ридера і починає передавати дані, збережені в його пам'яті, обернено в зчитувач.

Немає ніякої потреби в контакті або прямої видимості між зчитувачем і міткою, оскільки радіосигнал легко проникає через неметалеві матеріали. Таким чином, теги навіть можуть бути сховані усередині тих об'єктів, що підлягають ідентифікації.

Галузі застосування RFID системи

Галузь застосування системи визначається її частотою. RFID-системи діляться на:

1. Високочастотні (850–950 Mhz і 2.4-5 Ghz), що використовуються там, де потрібна велика відстань і висока швидкість зчитування, наприклад контроль залізничних вагонів, автомобілів, системи збору відходів. Наприклад, ридери встановлюють на шлагбаумах, а транспондер закріплюється на вітровому або бічному склі автомобіля. Велика дальність дії дає можливість безпечної установки ридерів поза межами досяжності людей.
2. Проміжні частоти (10MHz—15MHz) — там, де повинні бути передані великі кількості даних.

3. Низькочастотні (100–500 Khz). Використовуються там, де припустимо невеличка відстань між об'єктом і рідером. Звичайна відстань зчитування становить 0,5 метра, а для тегів, умонтованих у маленькі «кнопочки», дальність читання, як правило, ще менше — близько 0,1 метра. Велика антена рідера може якоюсь мірою компенсувати таку дальність дії невеличкого тега, але випромінювання високовольтних ліній, моторів, комп'ютерів, ламп і т.і., заважає її роботі. Більшість систем керування доступом, безконтактні картки, керування складами і виробництвом використовує низьку частоту.

4. Система позиціонування в режимі реального часу RTLS

RTLS (скор. Від англ. Real-time Locating Systems - система позиціонування в режимі реального часу) - автоматизована система, що забезпечує ідентифікацію, визначення координат, відображення на плані місцезнаходження контрольованих об'єктів в межах території, охопленій необхідною інфраструктурою. RTLS накопичує, обробляє і зберігає інформацію про місцезнаходження і переміщеннях людей, предметів, мобільних механізмів і транспортних засобів з метою моніторингу технологічних і бізнес-процесів, сигналізації про відхилення від регламентів, а також з метою ретроспективного аналізу тих чи інших процесів і ситуацій.

Основні характеристики
До основних характеристик RTLS можна віднести:

Точність позиціонування - точність визначення координат об'єкту, що контролюється. Для різних технологій RTLS характерна точність позиціонування становить від декількох десятків метрів (для WiFi) до декількох сантиметрів (для ультразвукових).

Достовірність позиціонування - в реальних умовах точність позиціонування в значній мірі залежить від впливу перешкод і багатопроменевого загасання (відбитих сигналів), тому говорячи про точність позиціонування RTLS зазвичай вказують і вірогідну характеристику достовірності. Наприклад, «точність позиціонування 1 метр з достовірністю 90%», тобто точність буде забезпечуватися в 90% вимірювань.

Періодичність опитування - для забезпечення позиціонування в режимі реального часу проміжок часу між вимірами повинен бути таким, щоб об'єкт, рухаючись з характерною для нього швидкістю, встигав проходити відстань не більш подвоєною точності позиціонування. Наприклад, щоб забезпечити позиціонування в реальному часі з точністю один метр людини, що має характерну швидкість пересування 1,5 метра в секунду (5,4 км / год), виміри треба проводити з періодичністю не менше одного разу кожні 1,3 секунди. Це дозволяє будувати досить точні для практичних цілей траєкторії руху об'єкта навіть при різких змінах швидкості та напрямку руху.

Важливе значення мають також:

надійність і живучість (здатність самовідновлюватися при виході з ладу будь-якого вузла);

малі габарити і вага, а також низьке енергоспоживання міток (з метою економії заряду акумуляторів).

До складу більшості типів RTLS зазвичай входять:

Активна мітка RTLS - радіоелектронний пристрій, які прикріплюються до контрольованих об'єктів і взаємодіють зі зчитувачами RTLS. Зчитувачі отримують

сигнал від активних міток і вирішуючи тріангуляційну задачу визначають координати об'єкта.

Інфраструктура RTLS - базові станції обладнання забезпечує реперні точки з фіксованими координатами, об'єднаних мережею передачі даних і в деяких типах RTLS мережею синхронізації. Базова станція (БС) - пристрій, який взаємодіє з мітками в процесі визначення координат останніх. Базові станції мають фіксовані координати, щодо яких визначаються координати міток. Базові станції розташовуються так, щоб в будь-якій точці контрольованої території мітка могла «бачити» мінімум три базові станції.

Серверне програмне забезпечення - програмне забезпечення, що забезпечує управління процесом вимірювань, розрахунок координат об'єктів, обробку та накопичення даних.

Методи позиціонування

Мітки в RTLS позиціонуються щодо базових станцій з відомими координатами. Координати обчислюються за допомогою:

трилатерации - обчислення координат за результатами вимірювання відстані від мітки до трьох БС,

мультілатерації (також відомої як гіперболічне позиціонування) - обчислення координат за результатами вимірювання відстаней від мітки до трьох або більше БС

тріангуляції - обчислення координат шляхом вимірювання кутів напрямку від мітки до трьох БС.

Для підвищення точності і достовірності позиціонування використовуються складні алгоритми, що враховують наявність перешкод, обмежувачів руху (стін, бар'єрів), аттракторов (зручних, надають найменший опір шляхів), також в мітки може бути інтегрована інерціальна система навігації.

Суть процесу

Контрольовані системою об'єкти - люди, обладнання, транспортні засоби, рухомі механізми, інструменти, вантажі, цінні і небезпечні предмети та ін. Забезпечуються мітками RTLS. Контрольована системою територія обладнується інфраструктурою RTLS. В процесі роботи мітки обмінюються з вхідними в інфраструктуру БС пакетами даних і в ході обміну вимірюють відстані до них (або кути напрямку на БС). Серверне програмне забезпечення:

обчислює координати міток;

накопичує отримані дані;

сигналізує про знаходження об'єктів в заданих або заборонених зонах, рух об'єктів по заданих маршрутах або відхилення від них, порушеннях швидкісного режиму;

візуально відображає на екранах операторів місцезнаходження обраних об'єктів і траєкторії їх руху за заданий відрізок часу

5. Оптичні ідентифікатори

Штриховий код (штрихкод [1]) - графічна інформація, що наноситься на поверхню, маркування або упаковку виробів, що надає можливість зчитування її технічними засобами - послідовність чорних і білих смуг, або інших геометричних фігур.

Способи кодування інформації

Лінійні

Лінійними (смуговими кодами) називаються штрих-коди, що читаються в одному напрямку (по горизонталі). Найбільш поширені лінійні символіки:

EAN (EAN-8 складається з 8 цифр, EAN-13 - використовуються 13 цифр)
UPC (UPC-A, UPC-E)
Code56
Code128 (UPC / EAN-128)
Codabar
«Interleaved 2 of 5»

Лінійні символіки дозволяють кодувати невеликий об'єм інформації.

Двомірні

Приклад коду Data Matrix, що кодує текст: «Wikipedia, the free encyclopedia»

Двовимірний штрих-код на медичному рецепті

Двомірні символіки були розроблені для кодування великого обсягу інформації. Розшифровка такого коду проводиться в двох вимірах (по горизонталі і по вертикалі).

Двомірні коди поділяються на багаторівневі (stacked) і матричні (matrix). Багаторівневі штрих-коди з'явилися історично раніше, і являють собою поставлені один на одного кілька звичайних лінійних кодів. Матричні ж коди більш щільно упаковують інформаційні елементи по вертикалі.

В даний час розроблено безліч двовимірних штрих-кодів, що застосовуються з тією чи іншою широтою поширення

DataMatrix - двовимірний матричний штрихкод, який представляє собою чорно-білі елементи або елементи декількох різних ступенів яскравості, зазвичай у формі квадрата, розміщені в квадратної або прямокутної групі. Матричний штрихкод призначений для кодування тексту або даних інших типів. Найчастіше в промисловості і торгівлі застосовуються бітові матриці, що кодують від декількох байт до 2 кілобайт даних. При бажанні можна роздрукувати на принтері матриці ємністю в сотні кілобайт і потім зчитувати їх з досить високою точністю за допомогою фотоапаратів, матриці яких містять мільйони пікселів. Прообразом штрихкодів у вигляді матриць є перфокарти.

Зчитування за допомогою мобільного телефону (проект Semacode)

Зчитувачі коду Data Matrix і самі коди

Один з варіантів бітових матриць, «Data Matrix», був розроблений компанією RVSI / Acuity CiMatrix (нині частина концерну Siemens AG). Код застосовується для маркування в електроніці, автомобілебудуванні, харчовій промисловості, авіакосмічної та оборонної промисловості, енергетичному машинобудуванні. [1]

Також дані коди застосовуються в рекламної та розважальної сферах. За допомогою DataMatrix можна закодувати як текст, так і інші типи даних - веб-посилання, адреси електронної пошти, номери телефонів і SMS.

Маркування на твердих поверхнях

Друк наклейок з серійними номерами в процесі виробництва

Універсальний промисловий зчитувач

Технічна специфікація

Символи DataMatrix утворені з модулів, розташованих в межах шаблону пошуку. Ними можна зашифрувати до 3116 кодів таблиці ASCII (включаючи надлишкову інформацію). Символ складається з областей даних, які містять модулі у вигляді періодичного масиву. Кожна область даних обмежена шаблоном пошуку і

оточена з усіх чотирьох сторін межами вільної зони. (Зауваження: модулі можуть бути круглими або квадратними, конкретна форма стандартом не закріплена).

Data Matrix ECC 200

ECC 200 - це новітня версія DataMatrix, що використовує коди Ріда-Соломона для запобігання помилок і відновлення стертою інформації. ECC 200 уможливлює відновлення всієї послідовності закодованої інформації, коли символ містить 30% пошкоджень, припускаючи, що матриця все ще розташована в точності правильно. DataMatrix має частоту появи помилок менше, ніж 1 на 10 мільй відсканованих символів.

Символи мають парну кількість рядів і парна кількість стовпців. Більшість символів квадратні розмірами від 10x10 до 144x144 модулів. Однак деякі символи прямокутні і мають розміри від 8x18 до 16x48 модулів (тільки парні значення). Всі символи, що підтримують виправлення помилок ECC 200, можуть бути пізнані по верхньому правому кутовому модулю, має один колір з фоновим.

Додаткові можливості, що відрізняють ECC 200 символи від більш ранніх стандартів:

зворотний порядок читання символів (світле зображення на темному тлі)
специфікація набору символів
прямокутні символи
структурне приєднання (з'єднання до 16 символів для кодування більшої кількості інформації) [2]

Форма Data Matrix

Data Matrix код в горизонтальному і квадратному виконанні

Data Matrix код в горизонтальному і квадратному виконанні з посиланням на сторінку сайту https://tamali.net/barcode/2d/datamatrix/, за допомогою якої він був виготовлений.

Основною відмінністю Data Matrix від інших матричних штрих-кодів є можливість вибору форми зображення коду, яка може бути квадратної або прямокутної форми

QR-код

QR-код з посиланням на веб-сайт на білборді

Художній QR-код. Незважаючи на додаткову інформацію, цей код залишається читаним

QR-код (англ. Quick Response Code - код швидкого реагування; скор. QR code) - товарний знак для типу матричних штрих-кодів (або двовимірних штрих-кодів), спочатку розроблених для автомобільної промисловості Японії. Штрихкод - прочитується машиною оптична мітка, що містить інформацію про об'єкт, до якого вона прив'язана. QR-код використовує чотири стандартизованих режиму кодування (числовий, буквено-цифровий, двійковий і кандзі) для ефективного зберігання даних; можуть також використовуватися розширення [1].

Система QR-кодів стала популярною за межами автомобільної промисловості завдяки можливості швидкого зчитування і більшої місткості в порівнянні зі штрих-кодами стандарту UPC. Розширення включають відстеження продукції, ідентифікацію предметів, відстеження часу, управління документами і загальний маркетинг [2].

QR-код складається з чорних квадратів, розташованих у квадратної сітці на білому тлі, які можуть зчитуватися за допомогою пристроїв обробки зображень, таких як камера, і оброблятися з використанням кодів Ріда - Соломона до тих пір, поки зображення не буде належним чином розпізнано. Потім необхідні дані витягуються з шаблонів, які присутні в горизонтальних і вертикальних компонентах зображення [

QR-код розроблений і представлений японською компанією Denso-Wave [3] в 1994 році. Величезна популярність штрихкодів в Японії призвела до того, що обсяг інформації, зашифрованої в них, незабаром перестав влаштовувати промисловість. Японці почали експериментувати з новими сучасними способами кодування невеликих обсягів інформації в графічній картинці.

На відміну від старого штрихкоду, який сканують тонким променем, QR-код визначається датчиком або камерою як двовимірне зображення. Три квадрата в кутах зображення і менші синхронизирующие квадратики по всьому коду дозволяють нормалізувати розмір зображення і його орієнтацію, а також кут, під яким датчик розташований до поверхні зображення. Точки переводяться в двійкові числа з перевіркою по контрольній сумі.

Основна перевага QR-коду - це легке розпізнавання скануючим обладнанням, що дає можливість використання в торгівлі, виробництві, логістиці.

Максимальна кількість символів, які поміщаються в один QR-код:

цифри десяткової системи числення - 7089;
цифри десяткової системи числення і букви (латиниця) - 4296;
байти - 2953 (отже, близько 2953 літер кирилиці в кодуванні windows-1251 або близько 1450 літер кирилиці в utf-8);
ієрогліфи - 1817.

Хоча позначення «QR code» є зареєстрованим товарним знаком «DENSO Corporation», використання кодів не обкладається жодними ліцензійними відрахуваннями, а самі вони описані і опубліковані в якості стандартів ISO.

Мініатюрне видання А. С. Пушкіна «Євгеній Онєгін» в QR-коді [4]
Специфікація QR-коду не описує формат даних. Найбільш популярні програми перегляду QR-кодів підтримують такі формати даних: URL, закладка в браузер,

Email (з поміткою), SMS на номер (с темою), MeCard, vCard, географічні координати.

Також деякі програми можуть розпізнавати файли GIF, JPG, PNG або MID менше 4 КБ і зашифрований текст, але ці формати не отримали популярності.

Застосування
QR-коди найбільше поширені в Японії. Вже на початку 2000 року QR-коди набули такого широкого поширення в країні, що їх можна було зустріти на великій кількості плакатів, упаковок і товарів, там подібні коди наносяться практично на всі товари, що продаються в магазинах, їх розміщують в рекламних буклетах і довідниках. За допомогою QR-коду навіть організовують різні конкурси та рольові ігри. Провідні японські оператори мобільного зв'язку спільно випускають під своїм брендом мобільні телефони з вбудованою підтримкою розпізнавання QR-коду [5].

В даний час QR-код також широко поширений в країнах Азії, поступово розвивається в Європі і Північній Америці. Найбільше визнання він отримав серед користувачів мобільного зв'язку - встановивши програму-распознаватель, абонент може моментально заносити в свій телефон текстову інформацію, додавати контакти в адресну книгу, переходити по web-посиланнях, відправляти SMS-повідомлення і т. Д.

Як показало дослідження, проведене компанією comScore в 2011 році, 20 млн жителів США використовували мобільні телефони для сканування QR-кодів [6].

В Японії, Австрії і Росії QR-коди також використовуються на кладовищах і містять інформацію про небіжчика [7] [8] [9].

У китайському місті Хефей літнім людям були роздані значки з QR-кодами, завдяки яким перехожі можуть допомогти загубився старикам повернутися додому [10].

QR-коди активно використовуються музеями [11], а також і в туризмі, як уздовж туристичних маршрутів, так і у різних об'єктів. Таблички, виготовлені з металу, більш довговічні і стійкі до вандалізму.

Також в Бєлгороді (Росія) в кінці 2013 року був здійснений обласної проект з оснащення пам'ятників культури міста QR-кодами. Таким чином запуск інформаційного ресурсу «QR Бєлгород» дозволив зробити інформацію про історичний та культурний спадок регіону більш доступною для гостей і жителів області [12] [13].

Загальна технічна інформація
Найменший QR-код (версія 1) має розмір 21 × 21 піксель (без урахування полів), найбільший (версія 40) - 177 × 177 пікселів.

Існує чотири основних кодування QR-кодів:

Цифрова: 10 бітів на три цифри, до 7089 цифр.
Алфавітно-цифрова: підтримуються 10 цифр, літери від A до Z і кілька спецсимволов. 11 бітів на два символу, до 4296 символів
Байтовая: дані в будь-якої зручної кодуванні (за замовчуванням ISO 8859-1), до 2953 байт.
Кандзі: 13 бітів на ієрогліф, до 1817 ієрогліфів.
Також існують «псевдокодіровкі»: завдання способу кодування в даних, розбиття довгого повідомлення на кілька кодів і т. Д.

Для виправлення помилок застосовується код Ріда-Соломона з 8-бітовим кодовим словом. Є чотири рівня надмірності: 7, 15, 25 і 30%. Завдяки виправлення помилок вдається нанести на QR-код малюнок і все одно залишити його читаним.

Micro QR

Щоб в коді не було елементів, здатних заплутати сканер, область даних складається по модулю 2 зі спеціальною маскою. Коректно працює кодер повинен перепробувати всі варіанти масок, порахувати штрафні очки для кожної з особливими правилами і вибрати найбільш вдалу.