Мобільна платворма відеоспостереження стану та об’єктів навколишнього середовища розумного дому

аналіз стану розробок систем моніторингу навколишнього середовища рд

розділ 1 – аналіз об’єкту

Вступ

1. Розділ 1. Розумні будинки. Концепції, технології
   1. Інтернет речей
      1. Концепція. Визначення
      2. Архітектура і використовувані технології
      3. Переваги і недоліки концепції Інтернет речей
   2. Розумні будинки
      1. Визначення і архітектура “Розумних будинків”
      2. Дистанційне керування “Розумним домом”
   3. Системи спостереження
      1. Огляд (що використовується зараз)
      2. Значущість
      3. недоліки існуючих систем
   4. Постановка задачі
2. Розділ 2. Архітектура системи відеоспостереження
   1. постановка вимог (Вимоги до технічного забезпечення)
   2. Архітектура системи
   3. Засоби розробки
3. Розділ 3. Програмне забезпечення системи відеоспостереження
   1. Структура ПЗ
   2. Структура БД
   3. Структури даних
   4. Опис інтерфейсів
4. Розділ 4. Охорона праці

**Вступ**

Збереження інтересу до технології “розумного дому”, необхідність реалізації надійної системи спостереження.

**1. Розумні будинки: концепції, технології**

Створення «Інтелектуальних будівель» або «Розумних будинків» в останні  
роки набирає популярність у зв'язку з появою доступних і простих в установці модулів для їх створення. Спочатку, цей термін застосовувався для складних  
інженерних систем автоматизації, заснованих кабельно-дротовому з'єднанні. Але з появою концепції Інтернету речей (Internet of Things, IoT) «розумні будинки» стали використовувати бездротові інтерфейси зв'язку між компонентами, а також підключення до мережі Інтернет для дистанційного керування. Для того щоб спроектувати сервіс обслуговування систем даного типу, включаючи моніторинг та віддалене регулювання, необхідно вивчити основні принципи концепції «Інтернету речей», особливості архітектури «Інтелектуальних будівель», а також архітектуру хмарних обчислень.

**1.1 Інтернет речей**

Що таке Інтернет речей, з яких рівнів він складається і які технології використовує? Огляд концепції, її гідності і проблеми розвитку.

**1.1.1 Концепція. Визначення**

Термін вперше був сформульований в 1999 році Кевіном Ештоном(Англ. Kevin Ashton), працівником дослідницької групи в компаніїProcter & Gamble. Він запропонував запровадити радіочастотну ідентифікацію – RFID-мітки або маркери (Radio Frequency IDentification), для відстеження переміщення товарів компанії.

Зміст концепції Інтернету речей можна сформулювати наступним чином: для збільшення ступеня комфорту життя людей і надання складних комплексних послуг необхідно створення глобальної інфраструктури, що складається з безлічі речей (віртуальних і фізичних), які з'єднані між собою за коштами існуючих,що розвиваються і функціонально сумісних технологій інформаційноїкомунікації.

Фізичні речі в даній концепції - це речі реальногофізичного світу (датчики і різні пристрої), а віртуальні – речі інформаційного світу (наприклад, віртуальні гроші, і все, що матеріальну ціну, але не має фізичного носія). Кожна з таких речей може бути ідентифікована або інтегрована в мережу.

Якщо подивитися з практичної точки зору, то концепція Інтернету речей спрямована на автоматизацію процесів в різних сферах діяльності, виключення з них людини, і, як наслідок, підвищення ефективності економічних і суспільних процесів.

Засновник європейського ради по «Інтернету речей» Роб Ван Краненбург (бельг. Rob van Kranenburg) в своїх роботах пропонує цікаву виставу Інтернету речей у вигляді «чотиришарового пирога».

Перший шар включає в себе ідентифікацію об'єктів, наприклад, здопомогою датчиків або RFID-маркерів. На цьому етапі кожна Інтернет-річ отримує засіб зв'язку з навколишнім світом і унікальні дані.

Другий шар - обслуговування споживача або сервіс. тут об'єкти об'єднуються в мережі для виконання певної функції в рамках поставленого завдання. Найпоширенішими прикладами є системи моніторингу навколишнього середовища за допомогою бездротових сенсорних мереж і, звичайно, «Розумні будинки».

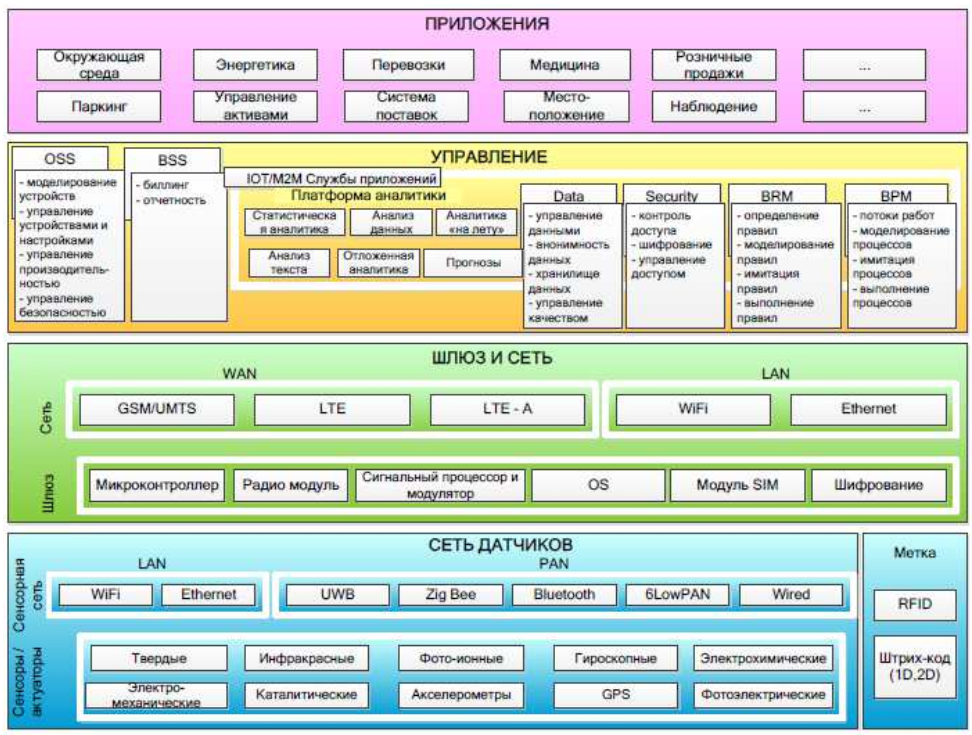
Третій шар заснований на тенденції урбанізації міського життя, так звані «Розумні міста», які мають на увазі дослідження і збір інформації на конкретній території (кварталі, районі тощо) і надання всієї необхідної інформації її мешканцям.

Четвертий і найвищий рівень - це сенсорна планета, коли всі існуючі мережіо б'єднуються в глобальну інформаційну інфраструктуру.

Іншими словами, Інтернет речей - це мережа мереж.

**1.1.2 Архітектура і використовувані технології**

Архітектуру Інтернету речей можна, можливо розділити на чотири функціональних рівня (рис. 1), розглянемо кожен з них  
детальніше.

Рисунок 1 – Архітектура IoT. Поділ на функціональні рівні

Самим нижнім в структурі Інтернету речей, але в той же час і самим важливим, є рівень сенсорів. Якщо зіставити з поданням Роба ванн Краненбурга, то він є першим шаром«Пирога».Грунтується цей рівень на модулях з підключаються датчиками і сенсорами, а також інших об'єктах, що забезпечують збір інформації,наприклад, на RFID-мітках згадуваних раніше або штрихкодах. Такіо б'єкти можуть інтегруватися один в одного і в інші фізичні об'єкти, інавіть в тіло людини.

Широкі дослідження в області сенсорів проводить Інститут інженерів електротехніки та електроніки - IEEE (англ. Institute of Electricaland Electronics Engineers). На даний момент анонсований стандарт обміну інформацією IEEE 802.15.6-2012, що дозволяє передавати інформацію в малопотужній бездротовій мережі в безпосередній близькості до людського тілу без перешкод.

Для передачі інформації всередині домашніх або офісних мереж використовуються менш чутливі і більш енергоємні стандарти обміну,найбільш відомими з яких є Ethernet, Wi-fi і Zig Bee.

Велика частина датчиків неінформативна сама по собі, але, об'єднуючись в мережеві структури, вони несуть значний потік корисної інформації. Для об'єднання і передачі інформації в світ більшості датчиків потрібна наявність шлюзу або агрегатора сенсорів. Залежно від завдання об'єднання об'єктів і роду самих об'єктів, можливе використання одного з нижчеописаних типів мереж.

1) Бездротові сенсорні мережі (WSN, Wireless Sensor Network) -самоорганізуються мережі датчиків і пристроїв. Як правило, пристроїв мережі з'єднані радіоканалом, тому цей тип мереж відрізняється низьким енергоспоживанням, малим радіусом покриття і низькою швидкістю передачі. Радіус покриття коригується ретрансляцією повідомлень (MultiHop Networking або Ad Hoc мережі). Основним стандартомпередачі є 6LoWPAN (англ. IPv6 over Low power Wireless Personal Area Networks), який дозволяє підключати сенсорні пристрої до широко поширених IP мереж.

2) Мережі ультра широкосмугового бездротового зв'язку на малих відстанях (UWB, Ultra-Wide Band) -використовуються для під'єднання периферійних пристроїв в мережах малого радіусу охоплення, наприклад,принтерів або мультимедійних систем в межах будинку. Характеризуються високою швидкістю передачі на малих відстанях.

3) Персональні мережі (PAN, Personal Area Network) — мережі,створювані «навколо» людей, об'єднують персональні комп'ютери, телефони і інші пристрої. У мережах даного типу використовуються специфікації мережевих протоколів верхнього рівня, такі як ZigBee і Bluetooth.

4) Локальні обчислювальні мережі (LAN, Local Area Network) -Ethernet і Wi-Fi; даний тип мереж на сьогоднішній момент відомий більшості людей, так як інтернет міцно увійшов в сучаснесуспільство.

5) Глобальні бездротові мережі (WAN, Wide Area Network) -мережі, що забезпечують зв'язок пристроїв з серверами / додатками безпосередньо, якщо не потрібне підключення до агрегатору. У категорію глобальних бездротових мереж входять GSM, GPRS і LTE.

Реалізації сервісу для обслуговування вимагає IoT забезпечити суміщення великої кількості мереж з різними протоколами доступу і технологіями передачі даних. Причому конфігурація таких мереж може бути різноманітною. Другий рівень - рівень шлюзів і мереж якраз і передбачає об'єднання різнорідних мереж в єдину мережеву інфраструктуру.  
Об'єднані мережі вимагають особливого відповідності встановленим стандартам якості передачі інформації: затримки не повинні перевищувати допустимих норм, пропускна здатність і безпеку передачі даних повинні так само відповідати стандартам. Користувачі повинні мати доступ до ресурсів незалежно і спільно без втрат продуктивності.

Наступний рівень - сервісний. Забезпечує управління бізнес-правилами і бізнес-процесами (BRM, Business Rule Management і BPM,  
Business Process Management відповідно). дозволяє автоматизувати  
операції, проведені над інформацією - збереження та аналіз, забезпечує  
підтримку операційної і бізнес діяльності (OSS / BSS, Operation Support  
System / Business Support System).

Самий верхній рівень - рівень додатків. Додатки діляться на «Горизонтальні», «Вертикальні», застосовні створювані для різних сфер під певну діяльності і спрямованість діяльності.

**1.1.3 Переваги і недоліки концепції Інтернету речей**

Переваги розвитку технологій Інтернету речей випливають з практичного застосування концепції: це автоматизація процесів в різних сферах діяльності, і,  
як наслідок, підвищення їх економічної ефективності. Інтернет речей покликаний зробити наше існування комфортніше, а виробництво більш вигідним. Навряд чи хтось не мріє про автоматично винесене сміття і підігрітий до часу приходу додому з роботи чай або свіжозварену каву зранку.

Але це лише мала частина можливостей Інтернету речей в сфері особистого користування. Для роботи в офісах колосальну користь може принести контроль клімату в приміщенні, адже комфортне робоче середовище покращує самопочуття, підвищує працездатність і навіть настрій. А повідомлення про незакриті після робочого дня вхідних дверей може вберегти від неприємностей. Автоматизація на виробництві так само допоможе уникнути непередбачених ситуацій, що особливо важливо на небезпечних хімічних і атомних підприємствах. Постійний контроль робочої зони і сигнал при перевищенні параметрами встановлених норм може допомогти уникнути катастрофи.

Інтернет речей розвивається стрімко, але і без труднощів не обійтися. На сьогоднішній день є кілька причин уповільнення в розвитку настільки популярною концепції: дефіцит IPv4 адрес, зменшення енергоспоживання датчиків і відсутність загальноприйнятих стандартів.  
1) Дефіцит адрес IPv4:  
Кожен новий датчик потребує унікальномий IP-адресу. Адреси IPv4  
закінчилися ще в лютому 2010 року. Отже, постає питання про переході до протоколу нової версії з розширеним кількістю адрес - IPv6. Крім більшої кількості адрес, IPv6 спрощує управління мережами, так як в ньому існує функція авто-конфігурації адрес, а так само підключення по даному протоколу є більш безпечним, ніж підключення по IPv4.  
2) Енергоспоживання датчиків:  
Енергопостачання датчиків - дуже важливе питання, тому що реалізація  
основної ідеї концепції Інтернету речей вимагає їх автономності.  
Неможливо забезпечити батарейками величезна кількість модулів без  
шкоди для навколишнього середовища. Необхідний інший підхід. датчики повинні  
отримувати енергію з навколишнього середовища або виробляти її самостійно. Найпростіший спосіб отримання енергії — сонячні батареї, але він не придатний для всіх видів датчиків, лише для тих, що розташовуються близько до джерел світла. Великий крок у розвитку був зроблений вченими Американського хімічного товариства в 2010 році. Анонсовано наногенератор - гнучкий чіп, що виробляє енергію з людських рухів. Безсумнівно, вчені розроблятимуть все нові і нові способи отримання енергії.  
3) Стандарти:

У галузі стандартизації були досягнуті значні результати за останні кілька років, але проблеми безпеки, захисту особистої інформації і встановлення єдиної архітектури рішень як і раніше актуальні. Уже згадувана раніше міжнародна асоціація IEEE (Інститут інженерів електротехніки та електроніки) - одна з небагатьох організацій, що сприяють розвитку єдиних стандартів. Поточним рішенням є стандартизована передача пакетів IPv6 в різних видах мереж.

Починаючи з 2012 року, Європейська комісія по питань інформаційного суспільства проводить консультації по темі регулювання ринку пристроїв, що підключаються до приватних бездротових мереж. Така стурбованість викликана тим, що пристроями Інтернету речей збирається, зберігається і передається інформація особистого характеру, яку зловмисники можуть використовувати проти власників. Єврокомісія намагається знайти оптимальне рішення, що поєднує захист особистих даних і зручність використання модулів і їх взаємну сумісність.

Над створенням універсальних специфікацій і відповідної сертифікації в сфері «розумної» електроніки на даний момент працюють кілька організацій, в тому числі альянс Open Connectivity Foundation (OCF), що включає в себе Intel, Samsung Electronics і Dell.

Одним з рішень проблеми безпеки є апаратна підтримка напівпровідниковими компонентами протоколу TLS (Transport Layer Security - безпека транспортного рівня). даний протокол аналогічний криптографічного протоколу SSL (Sockets Layer — рівень захищених сокетів), так як використовує симетричне шифрування і  
асиметричну криптографію, але захищає дані на більш низькому рівні. Нещодавно SSL визнаний небезпечним і радиться замінювати TLS.

**1.2 Інтелектуальні будівлі**

Визначення «Розумний будинок», з чого складаються системи автоматизації  
будівель і чому на сьогоднішній день цей напрямок дуже популярний.

**1.2.1 Визначення і архітектура “Розумних будівель”**

Автоматизація будівель почала з'являтися ще в 60-70-х роках минулого століття, тоді і було сформульовано поняття «розумний будинок». спочатку воно формулювалося як «будинок для ефективного використання робочого простору », але на сьогоднішній день його сенс набагато ширше.

«Розумний будинок» для сучасної людини - не просто система раціонального використання робочого простору, це інтелектуальна система, яка об'єднує в собі як інженерні комунікації та системи безпеки, так і інформаційні системи будівлі. Такі об'єднані рішення покликані підвищити комфортність приміщень і забезпечити їх безпеку. У багатьох випадках приводом для установки систем розумного будинку є бажання підвищити ступінь комфорту за рахунок автоматизації рутинних або постійно повторюються.

Реалізація розумного будинку ділиться на дві частини: апаратну і програмну. На рисунку 2 представлена ​​одна з можливих і найбільш часто використовуваних схем апаратного забезпечення розумного будинку. Апаратна частина, як правило, складається з контролера, модулів розширення і кінцевого обладнання.

Контролером може виступати ПК, планшет, смартфон, на які встановлюється програмне забезпечення для управління системами розумного будинку всередині домашньої (робочої) мережі або через мережу Інтернет.

Модулями або платами розширення називають спеціальні пристрої з підключеними датчиками різного типу і керованими частинами системи.

В категорію кінцевого обладнання входять датчики для відстеження  
різних параметрів середовища і стану пристроїв, які необхідно  
регулювати.

Програмне забезпечення може бути реалізовано багатьма способами:  
від звичайного пульта управління до складного синхронізованого комплексу програмного забезпечення, що встановлюється на будь-який кількість гаджетів і ПК власника інтелектуальної будівлі і повністю автоматичних систем, що включають в себе елементи інтелектуалізації.

**1.2.2 Дистанційне керування “Розумним домом”**

Розвиток бездротових інтерфейсів зв'язку та розширення концепції Інтернету речей призвело до виходу систем розумних будинків за межі приміщень і будівель, в яких вони встановлені. Взаємодія автоматизують комплексів з мережею Інтернет дало можливість управляти ними в режимі віддаленого доступу.

Дистанційне керування має ряд переваг перед управлінням виключно автоматичним і через системи, що працюють не далі установленного радіусу. Перш за все, це підвищення рівня безпеки і комфорту.

Основна перевага — підвищення комфорту використання простору будинку або офісу, що і є основною ідеєю для створення розумного будинку. При наявності функції віддаленого управління користувач може включити, вимкнути або налаштувати потребує покупець пристрою (освітлення, побутові прилади та інші системи), де б він не перебував. Наприклад, підігріти чай перед приходом додому з роботи або заздалегідь включити опалення, якщо за показаннями датчиків в приміщенні некомфортна температура.

Але головною перевагою варто вважати підвищення рівня безпеки. При відсутності людей в приміщенні можуть відбутися ситуації, що загрожують схоронності майна і самої будівлі. Для запобігання подібних інцидентів можливе підключення камер для спостереження за обстановкою в приміщенні або віддалений моніторинг з допомогою аналізу інформації, що надходить з різних датчиків, які використовуються в системах безпеки (датчики вогню, датчики відкриття / закриття дверей і т. д.). В тому числі, автоматичне відключення електроприладів та світла допоможе не тільки заощадити споживання електроенергії, а й зменшити ризик самозаймання електропроводки в порожньому приміщенні;

Система дистанційного керування в більшості випадків проста: користувач, з використанням гаджетів або ПК, відсилає команди системі через веб-додаток або зі сторінки веб-сайту, система аналізує отриману команду і за допомогою контролера виконує вказану дію.

Так як дистанційна робота з датчиками, камерами і іншим обладнанням передбачає зберігання, обробку і аналіз великої кількості інформації, і зручний доступ до результатів декількома користувачами, доцільне застосування хмарних обчислень. При такому підході в системі розумного будинку з'являється хмарний сервіс,  
дозволяє винести турботи про обслуговування серверної частини системи, з допомогою якої відбувається управління всією системою, за межі ведений користувача.

Для підключення хмари існує два варіанти. Перший - використання хмари в якості контролера. Всі пристрої підключаються безпосередньо до хмари і управляються з нього безпосередньо. Керуюча частина системи може бути повністю винесена за межі будівлі. Другий варіант - збір пристроїв на контролерах і підключення їх до хмари. В цьому випадку хмара буде керувати діями контролерів, передаючи інформацію між кількома модулями. контролер розміщується всередині будівлі, але все програмне забезпечення винесено на сервіс.

Обидва варіанти передбачають винесення аналізуючої частини системи в  
хмару, що дозволяє знизити вимоги до контролера, головна відмінність в  
тому, що в першому випадку управління пристроями автономно один від одного,  
а в другому через загальний контролер. Багато сучасні модулі працюють по власних протоколах передачі даних і, взаємодіють з Інтернет-сервісами тільки через своі API, що створює складності обміну інформацією між пристроями  
безпосередньо, а також заважає розширенню системи розумного будинку