

УДК 004.3'144-022.513:004.724:004.738.5

doi: 10.32620/akt.2023.6.09

О. О. ВДОВІЧЕНКО, А. Є. ПЕРЕПЕЛИЦІН

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна

ОРГАНІЗАЦІЯ ВЗАЄМОДІЇ ПРИСТРОЇВ З ДОСТУПОМ В ІНТЕРНЕТ НА ОСНОВІ МІКРОКОНТРОЛЕРІВ ІЗ ОБМЕЖЕНОЮ КІЛЬКІСТЮ РЕСУРСІВ

Предметом вивчення і дослідження в даній статті є технології і моделі дистанційної взаємодії вузлів, а також окремих малогабаритних складових компонентів вбудованих систем Internet of Things (IoT). **Метою** роботи є спрощення процесу налаштування кінцевим користувачем системи з пристроїв з можливістю зв'язку через Інтернет. **Завдання:** проаналізувати проблеми та вимоги при побудові IoT систем; виконати аналіз і класифікацію апаратних компонентів IoT систем; здійснити аналіз процесу комунікацій між окремими елементами IoT системи; дослідити протоколи зв'язку для IoT; проаналізувати існуючі сервіси взаємодії з пристроями з можливістю зв'язку через Інтернет; запропонувати моделі комунікації елементів IoT системи. Відповідно до поставлених завдань, були отримані наступні **результати**. Проаналізовані існуючі шляхи і проблеми зв'язку пристроїв з підключенням до Інтернет. Проаналізовані можливі технічні рішення і компоненти в системах IoT. Виконано класифікацію набору компонентів подібних систем. Запропоновано процес вибору компонентів для набору вихідних умов з урахуванням вимог ціни, необхідних зусиль на розгортання системи та можливості внесення змін до системи. Обговорюються проблеми побудови рішень з доступом в Інтернет з використанням дешевих мікроконтролерів з невеликим розміром пам'яті програми та врахуванням вимоги обмежених ресурсів. Детально описаний процес зв'язку з пристроєм. Проведено аналіз існуючих протоколів взаємодії між сервісом і таким пристроєм. Запропоновані моделі для опису можливих видів взаємодії окремих вузлів. **Висновки.** Проведений аналіз дозволив виділити п'ять типів компонентів для побудови IoT систем і співвіднести їх ціну, трудовитрати на підключення та можливість модифікації. Знайдено простий у використанні сервіс для роботи з мікроконтролерами з обмеженими ресурсами і сервіс для побудови системи розумного будинку з відкритим кодом та широкою підтримкою протоколів. Практичне значення даного дослідження полягає у можливості прийняти рішення про найбільш підходящий набір компонентів для конкретної розподіленої апаратної системи, а також можливості вибрати модель взаємодії, вибрати протокол комунікації і знайти або створити сервіс для реалізації зв'язку.

Ключові слова: сервіси взаємодії з пристроями; розумний будинок; Internet of Things; IoT; ThingSpeak; Home Assistant; мікроконтролери з обмеженими ресурсами.

Вступ

Розвиток можливостей зв'язку та збільшення кількості готових компонентів для побудови IoT систем, у тому числі з використанням супутникового Інтернет з'єднання, а також модулів для збирання таких рішень, актуалізують можливість організації взаємодії окремих елементів домашніх систем зручним для їх використання способом [1].

Можливість управління окремими модулями у складі розумного будинку суттєво спрощує процес комунікації [2]. При цьому стає актуальною можливість використання відтворюваних рішень для організації такої взаємодії як на стороні користувача, так і на стороні пристрою [3].

Набори окремих модулів для побудови таких систем досить популярні, добре описані [4], і при цьому недостатньо продуктивні, щоб підтримува-

ти складні протоколи зв'язку [5]. Існують способи взаємодії, що не потребують реалізації складних алгоритмів і надають можливість використання таких простих пристроїв на основі 8-бітних чипів.

Забезпечення необхідного рівня безпеки є однією з важливих вимог щодо побудови таких систем з управлінням через Інтернет [6].

Популярні набори сервісів для взаємодії апаратних рішень у складі елементів розумного будинку, у складі всього спектру IoT рішень, при взаємодії між собою або з центральним контролюючим пристроєм, використовують протоколи, які здійснюють взаємодію і спрощують контроль.

Існує велика кількість IoT рішень та інформації про них, у тому числі і про їх побудову [7]. Їх розгляд у узагальненому вигляді дозволяє знайти закономірності створення і розгортання таких систем на більш високому рівні абстракції із за-

стосуванням модельних підходів. Це надає можливість узагальнити ці рішення і спростити процес взаємодії із ними.

Аналіз і порівняння сервісів потрібні для вироблення стратегії вибору з погляду застосування сервісу для кожного окремого випадку. Для цього існує необхідність розглянути, які рішення бувають, акцентуючи увагу на способи взаємодії пристроїв у складі рішення.

Метою даної роботи є спрощення процесу налаштування кінцевим користувачем системи з пристроїв з можливістю зв'язку через Інтернет.

Для досягнення цієї мети необхідно виконати наступні завдання:

- 1) проаналізувати проблеми та вимоги при побудові IoT систем;
- 2) виконати аналіз і класифікацію апаратних компонентів IoT системи;
- 3) здійснити аналіз процесу комунікацій між окремими елементами IoT системи;
- 4) дослідити протоколи зв'язку для IoT;
- 5) проаналізувати існуючі сервіси взаємодії з пристроями з можливістю зв'язку через Інтернет;
- 6) запропонувати моделі комунікації елементів IoT системи.

1. Аналіз проблем та вимог при побудові IoT систем

Розробка вбудованих рішень передбачає розгляд набору вимог для конкретного пристрою. Такі вимоги включають конкретику про можливий набір апаратних компонентів для реалізації системи, протоколи взаємодії, габарити та інші вимоги. Також одними з найважливіших вимог є вартість і тимчасові витрати розробки, разом з технічними складностями побудови.

Вартість включає в себе витрати на дослідження, проектування та розробку, що у свою чергу, визначає порядок і складність реалізації рішення в рамках виконуваної задачі. Також вартість включає витрати на побудову апаратних і програмних компонентів, що використовуються при розробці програмно-апаратних комплексів.

Під програмними компонентами маються на увазі всі бібліотеки, фреймворки і окремі елементи існуючих і доступних рішень, застосованих у складі проекту. Апаратні компоненти або блоки – це серійно вироблені елементи, плати, мікросхеми, призначені для суміщення та використання у складі різних пристроїв.

Також важливою проблемою слід вважати завдання уніфікації інтерфейсів. Іншими словами, проблема сумісності з популярними рішеннями для управління та розгортання IoT рішень.

Інтерфейси повинні бути сумісними в рамках програми, комутації пристроїв між собою та в рамках взаємодії з користувачем. Наявність загальних стандартів дозволяє поєднувати, додавати, змінювати та сполучати компонентну та програмну базу різних рішень у рамках одного рішення. Такий підхід є економічно доцільним і вважається правилом хорошого тону при проектуванні.

Необхідним при проектуванні та розробці є вибір апаратних та програмних компонентів з тривалим періодом розвитку та підтримки від виробника. Особливо це стосується компонентів із відкритим вихідним кодом. Це важливо врахувати, щоб уникнути проблем, що виникають на етапі розгортання. Наприклад, може бути не враховано досвід певного набору пристроїв, оточення або каналу зв'язку. Це може призвести до відсутності сумісності.

За наявності різних способів комунікації, наприклад SIM-карт, GSM-модулів чи Wi-Fi модулів, висока ймовірність виникнення несумісності на рівні частот, операторів чи даних для авторизації під час спроби підключення.

Вимоги функціональної безпеки відіграють важливу роль. При побудові пристроїв, відповідальних за критичні функції систем, постає завдання забезпечення функціональної безпеки. Прикладом може бути процес запобігання аварійним ситуаціям при функціонуванні системи розумного будинку. До них можна віднести пожежу, затоплення та інші небажані події. У бізнес-критичних рішеннях важливо уникнути також і фінансових втрат. Наприклад, збою в логістиці підприємства через порушення у роботі навантажувачів.

Вимоги інформаційної безпеки також важливі для критичних систем. Для будь-якої системи, пов'язаної з виробництвом, зберіганням та передачею інформації важливим є і завдання забезпечення інформаційної безпеки або кібербезпеки [8]. Враховуються як підзавдання забезпечення захисту каналів зв'язку, акаунтів так і розмежування прав доступу до різних елементів IoT інфраструктури [9]. Значимість цієї складової тим вища, чим ближче проект до завдання забезпечення розгортання для масового використання.

2. Аналіз і класифікація компонентів IoT системи

Важливим етапом при побудові IoT систем є вибір компонентної бази. Залежно від завдань системи, що розробляється, набір комплектуючих може змінюватись. Для вибору оптимального набору доцільно вивчити діапазон готових рішень для побудови апаратних систем.

Проведений аналіз показує існування широкого спектра рішень, що поділяються за вартістю, способом виготовлення та призначенням.

Цілком ексклюзивні рішення часто використовуються на етапі створення першого прототипу пристрою. Сюди входять авторські поодинокі екземпляри компонентів і плат, що реалізують вузький спектр функцій, достатній для побутових завдань. Вони не є масовими, і часто легко відтворюються через використання серійних компонентів, плат і контролерів. Подібні рішення можуть виступати як апробація методів і концепцій автора, а також частковою або тимчасовою заміною заводських рішень.

Стандартизовані набори модулів для швидкого прототипування досить популярні та впізнавані. Сюди входять набори із часто затребуваних плат та пристроїв, виконаних у модульному вигляді. Зважаючи на серійність і масовість виробництва, системи побудовані на їх основі значно виграють за собівартістю при збереженні рівня якості виконання. Найчастіше їх якість є близькою до заводських рішень.

Також, завдяки модульному виконанню та стандартизації корпусів досягається легка та передбачувана відтворюваність систем, побудованих на їх основі. Це, у свою чергу, уможлиблює дистанційне відтворення та тестування екземплярів системи на етапі розробки.

Завдяки поширеності, зменшуються і тимчасові витрати на розробку, що поряд з можливістю попереднього складання та вбудованих механізмів захисту модулів, дозволяє уникнути багатьох помилок, здатних викликати збої при роботі готової системи.

На додаток до вищепереліченого, у подібних наборах присутня солідна розподілена інформаційна база в мережі Інтернет, що фіксує досвід користувачів і надає рекомендації як для користувачів, так і для виробників.

Рішення, що випускаються серійно, є основною частиною готових IoT рішень. Є оптимізованим, часто виконаним в єдиному корпусі комплексом підсистем високої точності для використання в промислових і комерційних системах.

Вони не завжди підходять для пробних збірок та перевірочних макетів, у зв'язку з тим, що поставляються у вигляді рішень з встановленим програмним забезпеченням та налаштуваннями, за рахунок чого мінімізуються часові витрати на складання та розгортання систем.

Монтажні рішення також є частиною ринку готових рішень IoT. Розглянутий тип пристроїв застосовується на етапі проектування та початку будівництва споруд. Монтуються дані пристрої

разом з елементами каркасу, фасаду, інтер'єру та екстер'єру. Здебільшого, дані рішення використовуються в завданнях моніторингу стану приміщення на предмет виникнення пожеж, несанкціонованого проникнення та задачах моніторингу систем енергозабезпечення, ліній комунікацій, водопостачання та водовідведення. Являють собою блок з елементом автономного живлення, переведений в сплячий режим до моменту виникнення події, що відстежується.

Ексклюзивні професійні пристрої є найдорожчими з усіх готових рішень IoT. Цей клас систем являє собою пристрої малого тиражу, розроблені на замовлення за допомогою виробничих потужностей. Вирізняються високою якістю виконання, матеріалів та високою собівартістю. Для таких систем виробником та постачальником передбачається програма підтримки та обслуговування, що мінімізує ризики, пов'язані з функціональною та інформаційною безпекою.

Співвіднесення компонентів за набором ознак показує можливість об'єднання груп пристроїв залежно від категорії зіставлення. Частина з них мають схожі властивості в заданій категорії.

Результати аналізу компонентів представлені в таблиці 1. Для виділених категорій в рамках класифікації проведено порівняння компонентів за ціною, необхідними трудовитратами з боку користувача на розгортання і налаштування екземпляра такої системи та можливості внесення змін до програмної або апаратної складової пристрою.

Таблиця 1
Співвіднесення категорій компонентів IoT пристроїв за критерієм вартості, кількості умов для налаштування та модифікованості

Категорія	Ціна	Потрібні зусилля	Підтримка модифікації
Поодинокі прототипи	Низький	Максимальний	Будь-які зміни
Модулі «своїми руками»	Мінімальний	Залежить від завдання	Будь-які зміни
Готові пристрої	Середній	Низький	Залежить від пристрою
Інтегровані пристрої	Високий	Мінімальний	За виробником, сервісним центром
Високоякісні професійні пристрої	Максимальний	Мінімальний	Тільки від виробника

Отримані результати аналізу дозволяють зробити вибір компонентів для конкретної IoT систем на підставі заданих вимог. Можна зробити висновок, що найбільш раціональними рішеннями на етапі розробки системи є готові модулі. Вони дозволяють вносити модифікації і при цьому мають найменшу вартість та доступність у готовому вигляді у багатьох регіонах для паралельної розробки рішення групою з різних країн.

3. Аналіз процесу комунікацій між елементами IoT системи

Взаємодія апаратних компонентів може здійснюватися між координатором та виконавчим пристроєм [10]. При розгляді взаємодії елементів у складі діючої системи у складі розумного будинку важливо визначити ролі окремих апаратних компонентів [11]. У узагальненій моделі взаємодії обчислювально-керівне рішення може виступати в ролі координатора з доступом в Інтернет.

Щодо внутрішньої структури системи Координатор може бути виконаний у вигляді вузла або групи вузлів у складі системи розумного будинку з частковим або повним доступом до периферії.

Під периферією розуміються виконавчі пристрої та датчики, які обмінюються даними з координатором за допомогою інших інтерфейсів. Це можуть бути місцеві дротові інтерфейси, інфрачервоні канали, оптичні в інших діапазонах, звукові, в тому числі ультразвукові, та радіоканали.

Винятком є Інтернет, зважаючи на те, що є необхідність розмежовувати канали обміну інформацією з координатором за допомогою використання різних наборів інтерфейсів. В цьому випадку завдання взаємодії з Інтернетом реалізується повністю координатором такої домашньої системи.

Крім координатора, у схемі взаємодії компонентів з Інтернетом є і сам сервіс взаємодії IoT рішень. Він забезпечує та обслуговує комунікацію всієї системи. Розгляд цих сервісів становить великий інтерес.

Взаємодія елементів IoT системи та сервісу дозволяє забезпечити дистанційну взаємодію системою для вирішення завдань моніторингу або керування. Для управління та відображення органів керування системою необхідний відповідний елемент у складі моделі системи. На практиці у якості такого елемента може виступати комп'ютер або телефон, який використовується для моніторингу та керування системою. Даний елемент через Інтернет пов'язаний за допомогою програмних інтерфейсів, як із сервісами взаємодії, так і з Координатором для обміну даними та управління.

Під взаємодією в рамках системи розуміється вертикальне сполучення у складі Інтернет з координатором за допомогою сервісу взаємодії IoT. У такому випадку при обслуговуванні безлічі систем, сервіс виступає централізованим монітором, у той час як пристрій моніторингу займає вторинне місце.

У такому випадку пристрій моніторингу призначений для збору статистики або вторинної інформації про роботу системи.

У класичному випадку, сервіс виступає у ролі посередника при взаємодії пристрою керування та моніторингу з координатором.

В обох випадках сервіс, крім обчислювального розвантаження, дозволяє більш гнучко керувати підключеннями в межах системи, розвантажуючи пристрій-координатор. Це значно знижує енергоспоживання вузлів.

Також, на відміну від варіанта без використання сервісу, для забезпечення з'єднання немає необхідності у виділеній адресі кожного координуючого вузла. Натомість достатньо забезпечити підтримку набору протоколів взаємодії з сервісом. Використання протоколів значно полегшує структуру самого пристрою та процедуру взаємодії з ним.

При взаємодії пристрою з сервісом через протокол і дотриманні вимог до складності реалізації спілкування з користувачем, яке здійснюється програмно, здійснюється грамотний процес комунікації, минаючи більшість проблем, пов'язаних з апаратною реалізацією та питань енергоспоживання. Сервіс здійснює взаємодію з величезною кількістю екземплярів подібних рішень. Це знижує в рази енергоспоживання на одиницю такого екземпляра в порівнянні з рішеннями, що реалізують ці функції без використання сервісу.

Значна частина сервісів вже призначена саме для взаємодії з елементами розумного будинку, IoT рішеннями та надають пряму підтримку таких рішень.

Загальна структура і взаємодія елементів описуваної системи представлені рисунку 1.



Рис. 1. Комунікація елементів IoT через Інтернет

4. Аналіз протоколів зв'язку для IoT

REST (Representational State Transfer) є одним із можливих протоколів [12]. Часто зустрічаються сервіси, які здійснюють взаємодію через REST. Він передає репрезентативний статус або стан інформаційного ресурсу. Під цим же ім'ям можна розуміти в цілому архітектурний стиль взаємодії розподілених компонентів у мережі.

Протокол MQTT (Message Queue Telemetry Transport) є лідером по частоті використання у спеціалізованих системах, після HTTP (Hypertext Transfer Protocol). Це спрощений мережевий протокол на основі черг TCP/IP запитів у форматі видавець-підписник. З назви зрозуміло, що будуватиметься черга і всередині пристрою, і на стороні сервісу, щоб просто обмінюватися повідомленнями [13]. Цей протокол взаємодії підтримується більшістю сервісів взаємодії IoT пристроїв.

XMPP (Extensible Messaging and Presence Protocol) також часто використовується для взаємодії пристроїв. Використовується у спеціалізованих системах для швидкого обміну повідомленнями та, що важливо, інформацією про присутність. Тобто, пристрій залишається на зв'язку, крім випадків, коли розривається канал, і не має можливості з ним взаємодіяти. Це дозволяє значною мірою економити ресурси при взаємодії з пристроями та спрощує перевірку їх наявності та активності у мережі.

AMQP (Advanced Message Queuing Protocol) у нинішньому вигляді є відкритим стандартом, орієнтованим на обробку повідомлень. Підтримується приблизно у третині систем для практичного застосування. Поширеність підтримки вимагає наявності бібліотеки для різних пристроїв.

CoAP (Constrained Application Protocol) це важливий і часто використовуваний протокол. Він являє собою спрощений HTTP для інтернету речей. Зустрічається в половині застосовуваних рішень і сервісів, які дозволяють здійснювати обмін. Встановлює канал обміну між кінцевим пристроєм, користувачем або споживачем даних, якщо цей пристрій виробляє дані.

Різні протоколи взаємодії, до яких можна віднести і HTTP, HTTPS, FTP, Web Sockets, та інші протоколи взаємодії, яких існує багато. Якщо ми говоримо в цілому про такі сервіси, ми розуміємо, що існує досить потужний, широкий спектр компаній виробників, і рішень які також знаходять широке застосування при побудові сервісів для взаємодії елементів розподілених апаратних систем. Якщо йде мова про спеціалізовані протоколи під такі сервіси, слід звернути увагу на перші п'ять елементів у складі поточного списку.

5. Аналіз сервісів взаємодії з пристроями

При безпосередньому розгляді стандартних та добре відомих компаній, які дозволяють будувати деякі сервіси для обробки та взаємодії з IoT рішеннями, можна назвати деякі відомі корпорації, серед яких є Microsoft, Amazon, Google, IBM та Cisco [14].

Microsoft Azure IoT це один із сервісів з найкращим захистом з точки зору організації каналу для роботи з IoT пристроями. Тобто, він має один з максимальних ступенів захисту. Також він є масштабованим і містить досить прості кроки, пов'язані з його розгортанням. Також це досить популярний сервіс, який надає повноцінну підтримку, і надає вичерпну можливість пройти кроками, пов'язаними з цими процесами, у тому числі саме розгортання. Документація доступна та надана на високому рівні. При цьому варто відзначити його високий рівень захисту. Тобто, всі міри захисту там реалізовані дуже на високому рівні.

AWS IoT, тобто це Amazon рішення, які включають і хмарні рішення, хмарні ресурси, в тому числі рішення FPGA as a Service. Останнє вважається окремим напрямком реалізації апаратури та доступу до апаратних рішень на рівні хмари.

В рамках цього дослідження сервісів для організації взаємодії з IoT рішенням слід зазначити, що AWS IoT має переваги підтримки необмеженої кількості пристроїв під час своєї роботи. При цьому має багаторівневий захист і, власне, даних, і можливості управління конкретними пристроями, а також взаємодії з цими пристроями. Також надає елементи штучного інтелекту, які дозволяють здійснювати роботу з такими пристроями та роботу з аналізом даних від таких пристроїв, якщо це завдання моніторингу. У цьому випадку елементи штучного інтелекту можуть бути інтегровані з користувацькими рішеннями, для того, щоб працювати з конкретними даними, з конкретним пристроєм, і знижувати витрати часу оператора, у разі, якщо він потрібний для обробки таких даних.

Google Cloud Platform. Це рішення, яке працює над питаннями безпеки на рівні взаємодії та платформи в цілому. Також Google безпечно зберігає дані через механізм, пов'язаний із зберіганням користувацьких даних, або тих даних, які надходять від пристрою, що захищаються на рівні самої компанії Google.

Однією з важливих особливостей такого рішення є те, що заявлено кінець (або період зміни) способу взаємодії з цим сервісом, але колосальну кількість інформації можна використовувати і далі.

Якщо потрібно вибрати пристрій-виробник, то потрібно розглянути дві платформи, або Google Cloud Platform, або IBM Watson IoT. Це дві компанії, що дозволяють зберігати колосальну кількість даних.

Рішення IBM Watson IoT, на відміну від Google, це повністю платне рішення і власне, за рахунок цього воно надає, підтримує та застосовує такі послуги. Таке рішення є високо безпечним і, власне, позиціонує себе як рішення з найвищим рівнем безпеки. Але додатковою особливістю цього рішення є набір інструментів для аналізу, та детального аналізу даних, які надходять від використаного пристрою у рамках взаємодії.

Рішення Cisco IoT Cloud Connect передбачають інтеграцію з мережевими системами. Більшістю споживачів таких рішень є компанії, які займаються зв'язком і в цьому випадку забезпечується безпечна організація таких взаємодій. Такі рішення від Cisco надають у реальному часі та дозволяють здійснювати моніторинг стану таких рішень. Загалом споживачами таких рішень можуть бути, у тому числі, і мережі стільникового зв'язку, та інші провайдери, які використовують роботу окремих рішень, які вимагають віддаленого доступу та взаємодії.

Інші відомі постачальники сервісів надають схожі можливості для IoT. На додаток до набору описаних рішень, часто використовується набір сервісів, який надається іншими відомими компаніями. Виділяють відомі Oracle, Eclipse IoT та інші, наприклад Salesforce IoT рішення, IRI рішення, Particle та ThingWorx.

ThingSpeak особливо цікавий для організації взаємодії з пристроями, де використовується мікроконтролер з дуже обмеженою кількістю ресурсів [15, 16]. Цей сервіс є одним з найбільш популярних для Arduino, і він став відомим за рахунок досить простого способу взаємодії з ним. Достатньо створити акаунт, отримуючи власний обліковий запис ThingSpeak або використовувати свій обліковий запис від MathWorks, компанії, яка інтегрована з рішеннями в складі ThingSpeak. Ця компанія надає інструментарій набору MathLab для аналізу даних та візуалізації, тобто, побудови графіку і різних діаграм за даними деяких IoT рішень, від датчиків, тобто від пристроїв, які підключені до цього сервісу.

У більшості випадків, якщо йдеться про моніторинг стану пристрою, процес використання цього сервісу з графічним відображенням безперервних даних є дуже зручним і інформативним. Інструментарій надається на основі Free підписки, тобто на основі безкоштовного плану, який доступний всім для реєстрації.

Цей сервіс надає можливість реєстрації окремих вузлів для користувача і надає можливість відстеження розташування певних подій та інформування.

Сервіс KAA розробляється і підтримується компанією CyberVision і пропонує глобальну інфраструктуру для побудови різних сервісів. Тобто, є можливість реалізації різних протоколів. Наприклад, реалізація протоколу REST, і надання, набору мов для реалізації зв'язків клієнт-сервер, на Java та C і C++ у складі ToolKIT.

Zetta це сервер орієнтований сервіс на NodeJS. Це рішення реалізоване за допомогою протоколів REST та WebSockets. Сервіс розглядає пристрій як REST-інтерфейс та дозволяє взаємодіяти з ним. Підтримує практично всі пристрої, Raspberry Pi та їх модифікації. Також сумісні з Arduino рішення на основі ARM, теж безумовно підтримуються цим сервісом.

Distributed Service Architecture це архітектура розподілених служб, яка представляє взаємодію складових частин IoT як певний набір або стан повнозв'язкових мереж. Це досить складна система для реалізації та використання, але вона представляє інтерес з точки зору розглядуваних властивостей сервісів.

Сервіс DeviceHive являє собою вулик пристроїв, де сервіс займається аналізом великих даних. Загалом для їх роботи потрібен пристрій, який підтримує варіацію ядра Ubuntu. Здійснює взаємодії шляхом створення проміжного шлюзу для взаємодії між вузлом та сервісом.

Сервіс GE Predix реалізує платформу як послугу (PaaS) для побудови рішень на основі промислових IoT рішень. Це платний сервіс, який має досить довгу історію та вважається успішною IoT платформою, яка пропонує можливості, пов'язані з підтримкою та моніторингом даних у реальному часі.

Home Assistant це платформа, яка позиціонує себе як сервіс масового використання. Вона надає набір інструментів для розгортання та створення свого сервісу. Це рішення заслуговує уваги, тому, що підтримує більшість протоколів і може знайти застосування там, де віддають перевагу рішенням з відкритим кодом. Можливість розширення цього сервісу, а також контроль над даними роблять його одним із найбільш привабливих для побудови рішень із домашньою автоматизацією.

Open Connectivity Foundation або **IoTivity** це розробка компанії Intel, Samsung, Qualcomm, Microsoft та Electrolux. Претендує на лідерство в напрямку організації обміну даними з пристроями через використання набору протоколів, включно з протоколами REST та CoAP.

Open HAB це один із сервісів для побудови та взаємодії рішень у якості елементів розумного будинку з відкритим кодом. Вимогою до роботи з рішенням є використання JVM. Тобто щоб запускатися рішення на основі сервісу необхідна віртуальна машина Java.

OpenIoT це також рішення на основі Java, яке здійснює взаємодію з кінцевими пристроями із можливістю побудови сенсорної мережі та об'єднання набору датчиків.

Open Remote – це сервіс, який призначений для автоматизації та застосовується підключення безлічі інтерфейсів. У складі такого сервісу включена підтримка досить складних протоколів самої взаємодії з кінцевими датчиками. Це OneWare, EnOcean, xPL та X10.

OpenThread це сервіс, орієнтований на пристрої, які підключені через IPv6 і використовуються в цьому випадку рішення на основі архітектури ARM. У тому числі можлива підтримка AVR рішень, Microchip, Qualcomm та інші.

PlatformIO – це рішення на основі Python і включає середовище розробки для генерації складових елементів проекту, набору бібліотек і надає підтримку і можливість взаємодії з більш ніж двома сотнями апаратних рішень у вигляді окремих макетних плат на основі Arduino сумісних та ARM рішень. Дозволяє здійснити інтеграцію з Eclipse, Qt Creator та іншими засобами розробки.

6. Запропоновані моделі взаємодії окремих вузлів у складі IoT

На абстрактному модельному рівні під час розгляду рішень із погляду їхньої взаємодії в рамках системи можна виокремити кілька категорій пристроїв, під'єднаних до мережі Інтернет.

Пристрої моніторингу та телеметрії, описуються моделлю, в рамках якої потік даних спрямований більшою мірою від пристрою до зовнішніх вузлів.

Це пристрої виробники, які здійснюють моніторинг і телеметрію рішень за допомогою Інтернет. Прикладом можуть виступати розумні термометри, датчики і сигналізація. У цьому разі модель взаємодії подається як вертикаль, спрямована в хмару, зважаючи на наявність ієрархії у взаємодії пов'язаних блоків, а саме сторона, що приймає, і сторона, що продукує.

Керувальні пристрої та актуатори описуються моделлю, в рамках якої мається на увазі двонаправлений потік даних між комбінацією пристроїв. Ці пристрої передбачають наявність наборів дій для керування виконавчими пристроями та периферією.

У разі керування пристроями, з акцентом на дані від навколишнього середовища, для двонаправленого потоку передбачається симетричний канал для зворотної взаємодії та виключення затримок під час обміну даними.

Для фізичних механічних пристроїв деякі критичні дії можуть спиратися на реакцію оператора, у зв'язку з чим, наявність затримок має бути зведена до мінімуму. Також до цієї категорії належать автономні пристрої з опціями керування, вибору функцій, режимів роботи і віддаленим запуском.

Прикладом може бути пристрій керування компонентами розумного будинку, на кшталт увімкнення чайника, запуску прання або двигуна окремо взятого автомобіля. У цьому разі модель взаємодії подається як двонаправлена вертикаль, зважаючи на наявність ієрархії у взаємодії пов'язаних блоків, а саме сторона, що задає, і сторона, що виконує.

Активний вузол описується новою моделлю, яка вважається джерелом і елементом інтелектуальної взаємодії одночасно. Таку модель не варто плутати з моделлю координатора розумного будинку. Найчастіше пристрій має в собі елементи штучного інтелекту і дозволяє здійснювати активні з'єднання.

Маються на увазі пристрої, здатні за власною ініціативою виходити в Інтернет, здійснювати окремі дзвінки та їхні групи без ініціації з боку оператора. Автономія дій таких пристроїв досить висока для формування запитів для людини, замість самої людини.

У цьому разі модель взаємодії визначає наявність як керуючих вузлів, так і однорангових відносно розглянутого пристрою. Це, своєю чергою, виводить систему із суворой вертикальної ієрархії взаємодії, передбачаючи й активність пристроїв на одному рівні.

Модель організації вузлів передбачає модель взаємодії, яка набуває характеру взаємодії рою і переходить із вертикальної ієрархії в горизонтальну, рівноправно обмінюючись даними між собою. Способи взаємодії варіативні та охоплюють усі системи, у яких пристрої можуть взаємодіяти на горизонтальному рівні.

Наявність головного вузла в цій моделі не заперечується. Це реалізується, коли присутній керуючий пристрій, що взаємодіє з іншими, при цьому інші елементи у взаємодії один щодо одного еквівалентні.

При цьому, присутність головного вузла стає опціональним варіантом. Система, що складається виключно з однорангових пристроїв, є застосовним такого випадку, і, також, використовується.

Висновки

В рамках роботи проведено дослідження проблем та пропонується рішення для дистанційної взаємодії вузлів, а також окремих малогабаритних складових компонентів вбудованих систем IoT. Проаналізовані існуючі шляхи і проблеми зв'язку пристроїв з підключенням до Інтернет, а також можливі технічні рішення і компоненти в системах IoT.

Розглядаються набори сервісів для взаємодії апаратних рішень у складі елементів розумного будинку, у складі всього спектра IoT під час взаємодії між собою або з центральним контролювальним пристроєм, який здійснює взаємодію і контроль.

Розглянуті категорії пристроїв за способом взаємодії один з одним, а також моделі взаємодії, виділені для них, можна використати надалі для ухвалення рішення щодо застосовності сервісу взаємодії для кожного окремого випадку і конкретного IoT рішення.

Запропонована класифікація набору компонентів подібних систем дозволяє здійснити процес вибору компонентів для набору вихідних умов з урахуванням вимог ціни, необхідних зусиль на розгортання системи та можливості внесення змін до системи, включаючи рішення з доступом в Інтернет з використанням дешевих мікроконтролерів з невеликим розміром пам'яті програми та врахуванням вимоги обмежених ресурсів. Також запропоновані моделі для опису можливих видів взаємодії окремих вузлів.

Таким чином, завдяки цьому дослідженню стає можливим прийняти рішення про найбільш підходящий набір компонентів для конкретної розподіленої апаратної системи, вибрати модель зв'язку, вибрати протокол і знайти або створити сервіс для реалізації зв'язку.

У рамках подальших досліджень необхідно розглянути проблеми, пов'язані з побудовою розподілених апаратних рішень. Для детального розуміння слід узяти до уваги весь набір вимог до сервісів взаємодії, що, своєю чергою, вимагає визначення переліку основних проблем під час їхньої побудови.

Внесок авторів: формулювання завдань дослідження – **А. Є. Перепелицин**; аналіз інформаційних джерел – **О. О. Вдовіченко, А. Є. Перепелицин**; аналіз протоколів взаємодії і рішень в складі хмарних сервісів – **А. Є. Перепелицин**; дослідження та формулювання моделей взаємодії окремих вузлів IoT – **О. О. Вдовіченко, А. Є. Перепелицин**; аналіз отриманих результатів, формулювання висновків та написання – **О. О. Вдовіченко, А. Є. Перепелицин**.

Усі автори прочитали та погодились з опублікованою версією рукопису.

Література

1. Исследование подходов к построению орбитальной вычислительной сети спутниковой системы Интернета Вещей [Текст] / М. Е. Ильченко, Т. Н. Нарытник, В. И. Присяжный, С. В. Капштык, С. А. Матвиенко // *Авіаційно-космічна техніка і технологія*. – 2019. – № 8. – С. 138–151. DOI: 10.32620/akt.2019.8.21.

2. Plakhteyev, A. Edge computing for IoT: An educational case study [Text] / A. Plakhteyev, A. Perepelitsyn, V. Frolov // *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018*. – 2018. – P. 130–133. DOI: 10.1109/DESSERT.2018.8409113.

3. Technologies of Embedded Systems Prototyping using Reconfigurable Nodes: Technical Solutions [Text] / A. Perepelitsyn, V. Duzhyi, O. Vdovichenko, & O. Zheltukhin // *Proceedings 2022 IEEE 12th International Conference on Dependable Systems, Services and Technologies, DESSERT 2022*. – 2022. – 6 p. DOI: 10.1109/DESSERT58054.2022.10018581.

4. Vdovichenko, O. Technologies for building systems of remote lining of communication lines: a practical example of implementation [Text] / O. Vdovichenko, & A. Perepelitsyn // *Radioelectronic and Computer Systems*. – 2021. – No. 2. – P. 31–38. DOI: 10.32620/reks.2021.2.03.

5. Метод дистанційної діагностики, перепрограмування і реконфігурації вузлів вбудованої системи [Текст] / О. О. Вдовіченко, А. Є. Перепелицин, В. І. Дужий, О. В. Желтухін // *Авіаційно-космічна техніка і технологія*. – 2022. – № 6. – С. 66–75. DOI: 10.32620/akt.2022.6.08.

6. IoT Privacy and Security: Challenges and Solutions [Text] / L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider // *Applied Sciences*. – 2020. – Vol. 10, No. 12. – Article No. 4102. – P. 1–17. DOI: 10.3390/app10124102.

7. Lombardi, M. Internet of Things: A General Overview between Architectures, Protocols and Applications [Text] / M. Lombardi, F. Pascale, & D. Santaniello // *Information*. – 2021. – Vol. 12, No. 2. – Article No. 87. – P. 1–20. DOI: 10.3390/info12020087.

8. Technique for IoT malware detection based on control flow graph analysis [Text] / K. Bobrovnikova, S. Lysenko, B. Savenko, P. Gaj, O. Savenko // *Radioelectronic and Computer Systems*. – 2022. – No. 1. – P. 141–153. DOI: 10.32620/reks.2022.1.11.

9. Kolisnyk, M. Vulnerability analysis and method of selection of communication protocols for information transfer in Internet of Things systems [Text] / M. Kolisnyk // *Radioelectronic and Computer Systems*. – 2021. – No. 1 – P. 133–149. DOI: 10.32620/reks.2021.1.12.

10. Developing complex services in an IoT ecosystem [Text] / C. Akasiadis, G. Tzortzis, E. Spyrou, & C. Spyropoulos // *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015. – P. 52–56. DOI: 10.1109/WF-IoT.2015.7389026.

11. Formal Analysis of Trust and Reputation for

Service Composition in IoT [Text] / A. I. A. Ahmed, S. H. A. Hamid, A. Gani, A. Abdelaziz, & M. Abaker // *Sensors*. – 2023. – Vol. 23, no. 6. – Article No. 3192. – P. 1–14. DOI: 10.3390/s23063192.

12. Chang, C. E. *FPGA Prototyping of Web Service Using REST and SOAP Packages [Text]* / C. E. Chang, A. K. Mustapha, & F. Mohd-Yasin // *Chips*. – 2022. – Vol. 1, no. 3. – P. 210–217. DOI: 10.3390/chips1030014.

13. *Smart Node Networks Orchestration: A New E2E Approach for Analysis and Design for Agile 4.0 Implementation [Text]* / A. Bertoli, A. Cervo, C. A. Rosati, & C. Fantuzzi // *Sensors*. – 2021. – Vol. 21, no. 5. – Article No. 1624. – P. 1–25. DOI: 10.3390/s21051624.

14. Muhammed, A. S. *Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives [Text]* / A. S. Muhammed, D. Ucuz // *2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020*, – 4 p. DOI: 10.1109/ISDFS49300.2020.9116254.

15. De Nardis, L. *ThingsLocate: A ThingSpeak-Based Indoor Positioning Platform for Academic Research on Location-Aware Internet of Things [Text]* / L. De Nardis, G. Caso, M. G. Di Benedetto // *Technologies*. – 2019. – Vol. 7, no. 3. – Article No. 50. – P. 1–23. DOI: 10.3390/technologies7030050.

16. *ATmega8A Data Sheet [Online]*. – Microchip Technology Inc., 2020. – 324 p. – Available at: <https://ww1.microchip.com/downloads/en/DeviceDoc/ATmega8A-Data-Sheet-DS40001974B.pdf>. – 19.09.2022.

References

1. Ilchenko, M., Narytnyk, T., Prysyzhny, V., Kapshtyk, S., & Matvienko, S. *Issledovaniye podkhodov k postroyeniyu orbital'noy vychislitel'noy seti sputnikovoy sistemy Interneta veshchey [Research of approaches to the development of the orbital computing network for the satellite system of Internet of Things]*. *Aviacionno-kosmichna tehnika i tehnologia – Aerospace technic and technology*, 2019, no. 8, pp. 138-151. DOI: 10.32620/akt.2019.8.21.

2. Plakhteyev, A., Perepelitsyn, A., & Frolov, V. *Edge computing for IoT: An educational case study*. *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018*, 2018, pp. 130-133. DOI: 10.1109/DESSERT.2018.8409113.

3. Perepelitsyn, A., Duzhyi, V., Vdovichenko, O., & Zheltukhin, O. *Technologies of Embedded Systems Prototyping using Reconfigurable Nodes: Technical Solutions*. *Proceedings 2022 IEEE 12th International Conference on Dependable Systems, Services and Technologies, DESSERT 2022*, 2022, 6 p. DOI: 10.1109/DESSERT58054.2022.10018581.

4. Vdovichenko, O., & Perepelitsyn, A. *Technologies for building systems of remote lining of communication lines: a practical example of implementation*. *Radioelectronic and Computer Systems*, 2021, no. 2, pp. 31-38. DOI: 10.32620/reks.2021.2.03.

5. Vdovichenko, O., Perepelitsyn, A., Duzhyi, V., & Zheltukhin, O. *Method of remote diagnostics, reprogramming and reconfiguration of nodes of embedded system*. *Aviacionno-kosmichna tehnika i tehnologia – Aerospace technic and technology*, 2022, no. 6, pp. 66-75. DOI: 10.32620/akt.2022.6.08.

6. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. *IoT Privacy and Security: Challenges and Solutions*. *Applied Sciences*, 2020, vol. 10, no. 12, article no. 4102, pp. 1-17. DOI: 10.3390/app10124102.

7. Lombardi, M., Pascale, F., & Santaniello, D. *Internet of Things: A General Overview between Architectures, Protocols and Applications*. *Information*, 2021, vol. 12, no. 2, article no. 87, pp. 1-20. DOI: 10.3390/info12020087.

8. Bobrovnikova, K., Lysenko, S., Savenko, B., Gaj, P., & Savenko, O. *Technique for IoT malware detection based on control flow graph analysis*. *Radioelectronic and Computer Systems*, 2022, no. 1, pp. 141-153. DOI: 10.32620/reks.2022.1.11.

9. Kolisnyk, M. *Vulnerability analysis and method of selection of communication protocols for information transfer in internet of things systems*. *Radioelectronic and Computer Systems*, 2021, no. 1, pp. 133-149. DOI: 10.32620/reks.2021.1.12.

10. Akasiadis, C., Tzortzis, G., Spyrou, E., & Spyropoulos, C. *Developing complex services in an IoT ecosystem*. *2015 IEEE 2nd World Forum on Internet of Things, WF-IoT 2015*, 2015, pp. 52-56, DOI: 10.1109/WF-IoT.2015.7389026.

11. Ahmed, A. I. A., Hamid, S. H. A., Gani, A., Abdelaziz, A., & Abaker, M. *Formal Analysis of Trust and Reputation for Service Composition in IoT*. *Sensors*, 2023, vol. 23, no. 6, article no. 3192, pp. 1-14. DOI: 10.3390/s23063192.

12. Chang, C. E., Mustapha, A. K., & Mohd-Yasin, F. *FPGA Prototyping of Web Service Using REST and SOAP Packages*. *Chips*, 2022, vol. 1, no. 3, pp. 210-217. DOI: 10.3390/chips1030014.

13. Bertoli, A., Cervo, A., Rosati, C. A., & Fantuzzi, C. *Smart Node Networks Orchestration: A New E2E Approach for Analysis and Design for Agile 4.0 Implementation*. *Sensors*, 2021, vol. 21, no. 5, article no. 1624, pp. 1-25. DOI: 10.3390/s21051624.

14. Muhammed, A. S., & Ucuz, D. *Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives*. *2020 8th International Symposium on Digital Forensics and Security, ISDFS 2020*, 2020, 4 p. DOI: 10.1109/ISDFS49300.2020.9116254.

15. De Nardis, L., Caso, G., & Di Benedetto, M. G. *ThingsLocate: A ThingSpeak-Based Indoor Positioning Platform for Academic Research on Location-Aware Internet of Things*. *Technologies* 2019, vol. 7, no. 3, article no. 50, pp. 1-23. DOI: 10.3390/technologies7030050.

16. *ATmega8A Data Sheet*. Microchip Technology Inc., 2020. 324 p. Available at: <https://ww1.microchip.com/downloads/en/DeviceDoc/ATmega8A-Data-Sheet-DS40001974B.pdf>. (accessed 19.09.2022).

Надійшла до редакції 10.10.2023, розглянута на редколегії 20.11.2023

ORGANIZATION OF COMMUNICATION OF DEVICES WITH INTERNET ACCESS BASED ON MICROCONTROLLERS WITH LIMITED HARDWARE RESOURCES

Oleksandr Vdovichenko, Artem Perepelitsyn

The subject of study in this article and research are technologies and models of remote communication of nodes, as well as individual small-sized components of embedded IoT systems. The **goal** is to simplify the process of configuration by the end user of the system based on devices with the possibility of communication over Internet. The **task** is: to analyze the problems and requirements for the creation of IoT systems; to perform the analysis and classification of the hardware components of IoT systems; to analyze the process of communication between individual elements of IoT system; to perform research of the communication protocols for IoT; to analyze existing services for the organization of the communication of devices with the possibility of connection to the Internet; and to propose the models of the communication of the elements of IoT system. According to the tasks, the following **results** were obtained. The existing ways and problems of communicating of devices with Internet connection are analyzed. Possible technical solutions and components of IoT systems are analyzed. Classification of the set of components of such IoT systems is performed. The process of selecting the components based on the set of initial requirements, considering the parameters of the price, the necessary efforts for the customer to deploy the system, and the possibility of system modification, is proposed. The problems of creation of systems with Internet access using cheap microcontrollers with a small program memory and considering the requirements of limited resources are discussed. The process of communication of the service with the device and connected peripheral modules is described in detail. The analysis of existing protocols for communication between the service and IoT device is performed. Models that describe possible types of interaction of individual nodes of smart home system are offered. **Conclusions.** The performed analysis allowed to classify and highlight five types of components for the creation of IoT systems and to correlate their price, required efforts for installation, and the possibility of modification by the customer. A service for simple communication with microcontrollers with limited resources and an open source service for the creation of a secure smart home system with wide support of protocols are found. The practical significance of this study is the possibility to decide which set of components is the most suitable for a specific distributed hardware system, as well as the possibility to choose the model of interaction and to choose the communication protocol with finding or creation of the service for IoT communication.

Keywords: services for communication of devices; smart home; Internet of Things; IoT; ThingSpeak; Home Assistant; microcontrollers with limited resources.

Вдовіченко Олександр Олександрович – асп., асист. каф. комп’ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Перепелицин Артем Євгенович – канд. техн. наук, доц., доц. каф. комп’ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Oleksandr Vdovichenko – PhD Student, Assistant of Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine, e-mail: o.vdovichenko@csn.khai.edu, ORCID: 0000-0001-8695-1752, Scopus Author ID: 58090577500.

Artem Perepelitsyn – PhD, Associate Professor of Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine, e-mail: a.perepelitsyn@csn.khai.edu, ORCID: 0000-0002-5463-7889, Scopus Author ID: 56332607800.