Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
(повна назва інституту/факультету)

Кафедра телекомунікацій
(повна назва кафедри)

«На правах рукопису»
УДК _____

До захисту допущено
В.о. завідувача кафедри

_____ Явіся В.С.___
(підпис)
(ініціали, прізвище)
“___”_____2018_р.

Магістерська дисертація
на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка,
(код і назва)

спеціалізація Апаратно-програмні засоби електронних комунікацій

на тему: Методика забезпечення інформаційної безпеки IoT

Виконала: студентка _2_ курсу, групи ТЗ-71мп
(шифр групи)

Вовк Анастасія Віталіївна _____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник __доцент, в.о. обов'язки зав. кафедри телекомунікацій, кандидат технічних наук Явіся В.С. _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018_ рік

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

Спеціалізація Апаратно-програмні засоби електронних комунікацій

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____Явіся В.С.
(підпис) (ініціали, прізвище)
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

_____Вовк Анастасії Віталіївні _____
(прізвище, ім'я, по батькові)

1. Тема дисертації: Методика забезпечення інформаційної безпеки IoT

науковий керівник дисертації: Явіся Валерій Сергійович, доцент, в.о. обов'язки зав. кафедри телекомунікацій, кандидат технічних наук,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «_06_» «_11_» 2018р. № _4095-с_

2. Строк подання студентом дисертації _10 грудня 2018р. _____

3. Об'єкт дослідження: Інтернет речей(IoT).

4. Предмет дослідження: методика(алгоритм) для забезпечення максимального захисту IoT.

5. Перелік завдань, які потрібно розробити: аналіз роботи IoT, його архітектур, топологій та протоколів; огляд систем для практичного застосування IoT; розляд можливих загроз, на прикладі «розумного дому»; розгляд способів захисту IoT; розробка алгоритму на основі існуючих та власних способів забезпечення інформаційної безпеки IoT задля забезпечення безперервної роботи мереж.

6. Орієнтовний перелік ілюстративного матеріалу: основні елементи мережі IoT, протоколи IoT, топологія мережі, компоненти «розумного дому», класифікація атак, алгоритм забезпечення безпеки.

7. Дата видачі завдання _1 вересня 2017р._____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Базова архітектура IoT	13.01	
2	Протоколи архітектури, стандартизація	01.03	
3	Проблеми реалізації, практичне застосування IoT	01.05	
4	Елементи, загрози «розумного дому»	13.07	
5	Атаки IoT	24.08	
6	Безпека зв’язку, захист програмного коду	15.09	
7	Хостовий захист, управління IoT, аналітика безпеки	26.11	
8	Методика забезпечення інформаційної безпеки IoT	01.12	

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

Обсяг роботи: 100; кількість ілюстрацій 23, кількість бібліографічних найменувань за переліком посилань 20.

Метою даної роботи є забезпечення інформаційної безпеки Інтернету речей для захисту даних від можливих подразників шляхом вибору оптимального алгоритму способів(методів) захисту. Ціллю данного аналізу є створення алгоритму забезпечення безпеки. Практичні задачі, що вирішено в проекті: аналіз роботи IoT, його архітектур, топологій та протоколів; огляд систем для практичного застосування IoT; розляд можливих загроз, на прикладі «розумного дому»; розгляд способів захисту IoT; розробка алгоритму на основі існуючих та власних способів забезпечення інформаційної безпеки IoT задля забезпечення безперервної роботи мереж.

Ключові слова: Інтернет речей, технологія ZigBee, Z-wave, стандарт IEEE 802.15.4, аутентифікація, безпека IoT.

ANNOTATION

The amount of work: 100; number of pictures 23; number of bibliographic items on the list links 20.

The purpose of this work is to provide information security of the Internet things to protect data from possible stimuli by choosing the optimal algorithm of methods of protection. The purpose of this analysis is to create an algorithm for security. Practical tasks solved in the project: analysis of the work of IOT, its architectures, topologies and protocols; review of systems for the practical application of IOT; feasibility of possible threats, as an example of a "smart home"; consideration of ways to protect IOT; development of algorithm on the basis of existing and own methods of providing IT security information in order to ensure the continuity of networks operation.

Keywords: Internet of things, ZigBee technology, Z-wave, IEEE 802.15.4 standard, authentication, IOT security.

Зміст

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI	– Artificial intelligence (штучний інтелект)
AmI	– Ambient Intelligence (розумне оточення)
API	– Application **p**rogramming **i**nterface
BLE	– Bluetooth Low Energy
CoAP	– Constrained Application Protocol (Протокол обмеженого застосування)
CPU	– Central processing unit (центральний процесор)
DOD AG	– Destination oriented directed acyclic graph
DTLS	– Datagram Transport Layer Security
DSSS	direct sequence spread spectrum
ETSI	– European Telecommunications Standards Institute
EPC	– Electronic Product Code
EST	– Enrollment over Secure Transport
ECC	– Elliptic Curve Cryptography
FHSS	– Frequency-hopping spread spectrum (псевдовипадкове перестроювання робочої частоти)
FFD	– Full function device
GPS	– Global Positioning System (система глобального позиціонування)
GSI	– Global Standards Initiative
IEEE	– Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки)
IoT	– Internet of Things (інтернет речей)
IoT-A	– Internet of Things - Architecture
IP	– Internet Protocol (address)
ISM	– Industrial, scientific and medical (частотний діапазон)
LED	– Light-emitting diode (світлодіод)
LPWAN	– Low-power Wide-area Network
MAC	– Media access control (address)
MQTT	– Message Queue Telemetry Transport
M2M	– Machine to machine (комунікація машина-до-машини)
mDNS	– multicast Domain Name System

NASA	– National Aeronautics and Space Administration
NID	– Network Identificator
NFC	– Near Field Communication («Зв’язок на невеликих відстанях)
OCSP	– Online Certificate Status Protocol
PLC	– Power-line communication, зв'язок по ЛЕП
QoS	– Quality of service
RAM	– Random Access Memory (оперативна пам’ять)
RFID	– Radio frequency identification (радіочастотна ідентифікація)
RPL	– Routing Protocol
RFD	– Reduced-function device
SDP	– Session Description Protocol
SCEP	– Simple Certificate Enrollment Protocol
SoC	– System-on-a-chip (система на кристалі)
SW	– Software (програмне забезпечення)
TCP	– Transmission Control Protocol
TLS	– Transport Layer Security
USB	– Universal Serial Bus
USN	– Ubiquitous Sensor Networks
UPnP	– Universal Plug and Play
V2I	– Vehicle to Infrastructure
V2V	– Vehicle to Vehicle
VICS	– Vehicle Information and Communication System
Wi-Fi	– Wireless Fidelity
WPA	– Wi-Fi Protected Access
WPAN	– Wireless personal area network
МСЕ-Т	Міжнародного союзу електрозв'язку

ВСТУП

Інформаційні технології (IT) перебувають на границі повної і точної автоматизації та прискоренню різноманітних бізнес-завдань, щоб розширити можливості бізнесу, партнерів, працівників та споживачів, щоб накопичувати бізнес-переваги, що широко розповсюджуються та підтримуються інформаційними технологіями. IT позиціонується як найкращий бізнес-фахівець. IT постійно розвивається, щоб робити краще та більше. На сьогодні IT, крім того, що є найбільшим стимулом для простих та складних бізнес-операцій, активно проникає в кожний відчутний галузевий сегмент, щоб активно забезпечувати нові та найважливіші бізнес-пропозиції, орієнтовані на клієнта. Коротше кажучи, IT здатний як спростити, так і посилити результати бізнесу та прогнози значно. Цілком очевидно, що стратегічно обгрунтована асоціація та узгодження між бізнесом та інформаційними технологіями пов'язані з послідовним підйомом для створення та підтримки в режимі реального часу, адаптивної, складної та швидкої діяльності. Поглиблено усвідомлюючи видатний внесок IT у підтримку ділових кіл на конкурентному ринку, компаніями-виконавцями та підприємцями важко докладати зусиль, щоб заробити більше грошей, щоб заробити, конкретизувати та забезпечити наступні покоління IT діловими послугами та рішеннями для своїх клієнтів у всьому світі та споживачів, розробляти дієві і добре передбачені механізми та методи для розуміння потреб людей та забезпечувати їх усіма якостями обслуговування (QoS) та якістю досвіду (QoE), вбудованими через розумне прийняття і адаптацію всіх видів вишуканих досягнень IT-сфери. Виконавці та інші зацікавлені сторони постійно шукають нові можливості для отримання більших доходів. Існують тектонічні зрушення в IT, що в свою чергу сприяють полегшенню роботи в буденності людей.

Передбачається і проголошено, що наступна епоха буде повністю забезпечена знаннями. Це буде суспільство кероване знаннями. Бази даних дозволять прокласти шлях до баз знань, а також будуть спеціалізованими двигунами для створення та збереження системи самоконтролю. Системи та

мережі знань будуть використовуватися для автономної комунікації. Машини з експериментальними системами та експертні системи стануть нашими випадковими та компактними супутниками. Зростаючий набір більш розумних систем буде оточувати та підтримувати нас у наших класних кімнатах, будинках, офісах, мотелях, кав'ярнях, аеропортах, тренажерних залах та інших життєвих сферах. Вони легко зв'яжуться, співпрацюватимуть, підтверджуватимуть і співвідноситимуть, розуміючи наші психічні, соціальні та фізичні потреби та доставляючи їх у надзвичайно ненав'язливий, безпечний та спокійний спосіб. Тобто, правильна інформація та необхідні послуги будуть задумані, побудовані та надані потрібній людині в потрібний час і в потрібному місці. Найважливішими факторами для цієї тектонічної та спокійної модернізації та міграції стануть сильно фізичні артефакти та активи, механічні та електричні машини, інструменти, обладнання, посуд, електронні пристрої, шлюзи зв'язку та IT-системи. Кожна звичайна, випадкова і дешева річ приєднається до основних обчислень у світ обізнаних, пов'язаних та пізнавальних обчислень.

Технології мінімізації, віртуалізації, автоматизації швидко розвиваються з метою створення зникаючих, одноразових, доступних, зв'язаних, надійних, орієнтованих на людину пристроїв. Це сервісні можливості для створення високоякісних послуг.

Початковий веб-сайт (веб-1.0) був просто для читання (простий веб-сайт), після чого веб 2.0 об'єднав читання і написання (соціальна мережа), тепер очікують веб-3.0 для читання, написання та для пов’язування декількох веб-контентів, програм, служб та даних (семантична мережа), а майбутнє, безумовно, за веб-версією 4.0 для передбачуваної ери знань (smart web). Тобто, кожна важлива річ у нашому середовищі - це веб-доступ до взаємодії з даними, додатками, службами, вмістом тощо. Хмарна інфраструктура постійно вдосконалюється, щоб бути централізованою та базовою платформою для інтелектуальної мережі. Отже, майбутній Інтернет - це IoT.

IoT - це все, що забезпечує надзвичайний зв'язок між різними об'єктами в галузях промисловості. Як уже згадувалося раніше, низка перспективних та позитивних тенденцій в інформаційному просторі заклали міцну і стійку основу для візуалізації майбутніх перспектив ідеї IoT. У двох словах, переважна тенденція полягає в тому, щоб розповсюджувати всі види непередбачених та дешевих продуктів та артефактів у нашому повсякденному середовищі, щоб вони були доступними для IT, об'єднавши їх в спеціальний спосіб, використовуючи різноманітні комунікаційні технології на необхідній основі, щоб використовувати їх окремі можливості як в індивідуальному, так і в колективному порядку для того, щоб рішуче і повноцінно розуміти різні потреби людей в даному конкретному середовищі, а також вирішувати, розповсюджувати та надавати визначені послуги та інформацію відповідним людям в потрібний час і потрібному місці.

Проте на сьогоднішній день існує ряд проблем для реалізації Інтернету речей в нашу буденність. Однією з найголовніших проблем є безпека мережі, оскільки інформація передається ще й по бездротовому середовищу, котре є більш уразливим в наслідок використання відкритого простору. На даний момент це є гострою проблемою та своєрідним бізнесом.

Об’єктом дослідження є Інтернет речей(IoT).

Предметом дослідження є методика(алгоритм) для забезпечення максимального захисту IoT.

Проблема, що вирішується - забезпечення інформаційної безпеки IoT, збереження даних в умовах різноманітних атак, впливу навколишнього середовища, а також фізичного втручання в систему.

Мета – забезпечення інформаційної безпеки Інтернету речей для захисту даних від можливих подразників шляхом вибору оптимального алгоритму способів(методів) захисту.

Практичні задачі, на вирішення яких спрямовано проект:

- аналіз роботи IoT, його архітектур, топологій та протоколів;
- огляд систем для практичного застосування IoT;

- розгляд можливих загроз, на прикладі «розумного дому»;
- розгляд способів захисту IoT;
- розробка алгоритму на основі існуючих та власних способів забезпечення інформаційної безпеки IoT задля забезпечення безперервної роботи мереж.

Значимість проекту для розв’язання економічних і соціальних проблем - підвищення інформаційного захисту Інтернету речей в державних, військових, комерційних структурах в умовах інформаційних атак, негативного впливу навколишнього середовища, а також фізичного втручання та халатності робітників.

Отже, оскільки мережі IoT використовуються не тільки вдома, а і на підприємствах, а в майбутньому планується створення розумної планети, кожна ланка такої системи потребує захисту, тому що тільки комплексним захистом можна створити сильну захищену мережу, тому необхідно створити алгоритм для максимального захисту мережі IoT.

РОЗДІЛ 1. ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ IOT

1.1 Поняття «Інтернету речей»

Сама концепція IoT була сформована в 1999 році як результат розвитку засобів радіочастотної ідентифікації (RFID) (для взаємодії пристроїв між собою і оточенням). Однак, протягом першого десятка років інтернет речей залишався долею в значній мірі ентузіастів і вузьких фахівців. Значним поштовхом для розвитку інтернету речей послужив розвиток технологій, а також інтерес до даної тематики з боку більшості світових концернів. Що по суті є взаємодоповнюючими і взаємостимулюючими факторами.

На даний момент практично всі великі компанії зі світовим ім'ям усвідомили, що дана концепція буде затребувана в найближчі кілька років. З цієї причини в їх складі з'явилися робочі групи, що займаються даною проблематикою. Уряди країн в свою чергу також виділяють фінансові кошти на грантовій основі для розвитку даного напрямку науки і техніки[1].

Існує безліч трактувань цього поняття, розглянемо декілька, найбільш впливовий. Аналітична компанія Gartner трактує поняття «Інтернет речей» (Internet of Things) як мережу фізичних об'єктів, що містять вбудовану технологію, яка дозволяє цим об'єктам вимірювати параметри власного стану або стану навколишнього середовища, використовувати і передавати цю інформацію. Зауважимо, що в цьому визначенні, до речі, найбільш часто цитованому, слово «Інтернет» взагалі відсутній. Тобто, кажучи про мережу «Інтернет речей», не мають на увазі, що вона є частиною Інтернету. Більш того, згідно з висловом одного з фахівців з технології IoT Мета Трака (Matt Turck), керуючого директора компанії FirstMark Capital, «за іронією, незважаючи на назву" Інтернет речей ", самі речі часто пов'язані за допомогою M2M-протоколів, а не самого Інтернету». Втім, наявність або відсутність підключення до Інтернету - не єдина розбіжність у визначеннях. Згідно з тлумаченням фахівців з компанії Cisco Business Solutions Group (CBSG), IoT - це стан Інтернету починаючи з моменту часу, коли кількість «речей або об'єктів», підключених до Всесвітньої мережі, перевищує населення планети.

CBSG підкріплює свої висновки розрахунками. За даними компанії, вибухове зростання смартфонів і планшетних комп'ютерів довів число пристроїв, підключених до Інтернету, до 12,5 млрд в 2010 році, в той час як число людей, що живуть на Землі, збільшилася до 6,8 млрд; таким чином, кількість підключених пристроїв склало 1,84 одиниць на людину. Виходячи з цієї нескладної арифметики, Cisco Business Solutions Group фактично визначило саму точку настання ери «Інтернету речей». Десь між 2003-му і 2010-м роком кількість підключених пристроїв перевищила населення планети, що й ознаменувало перехід в стан «Інтернет речей». При цьому автори дослідження вважають, що кількість підключених пристроїв на одну людину з числа інтернет-користувачів в 2010 році становило 6,25 штук.

Якщо Cisco згадує в зв'язку з терміном IoT про вибухове зростання смартфонів, підключених до мережі, то IDC, наприклад, чітко говорить, що пристрої в концепції IoT повинні бути автономно підключені до Інтернету і передавати сигнали без участі людини. А тому смартфон, керований користувачами, до IoT-пристроїв віднесений бути не може.

Згідно IDC, «Інтернет речей» (IoT) - це провідна або бездротова мережа, що з'єднує пристрої, які мають автономне забезпечення, керуються інтелектуальними системами, забезпеченими високорівневою операційною системою, автономно підключені до Інтернету, можуть виконувати власні або хмарні додатки і аналізувати зібрані дані. Крім того, вони мають здатність захоплювати, аналізувати і передавати (приймати дані) від інших систем.

Очевидно, що якщо аналітики оперують поняттям «обсяг ринку IoT», то спиратися на настільки розпливчасте визначення, як «якийсь новий стан Інтернету», неможливо. При цьому про IoT, як про такий собі переході Інтернету в нову якість, говорять не тільки фахівці з CBSG. Показовую тут є схема зі статті корейського автора Sunsig Kim, опубликована в 2012 році. Тут стан IoT представляється як точка переходу - це наступний щабель, в порівнянні з технологією M2M(рис. 1). Так і навпаки, в публікаціях ряду

авторів, включаючи IDC, можна прочитати, що M2M - це технологія, яка, будучи попередницею технології IoT, в даний час є її складовою частиною.

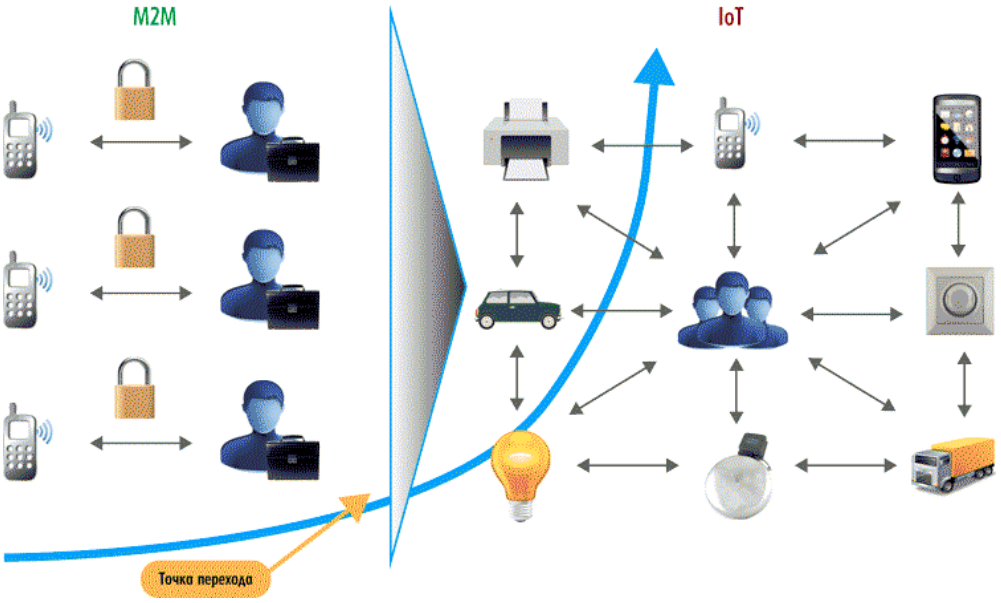

Рис. 1.1 Перехід від технології M2M до технології IoT

Тобто, Інтернет речей - це не просто безліч різних приборів і датчиків, об'єднаних між собою провідними та безпровідними каналами зв'язку та підключення до мережі Інтернет, а це більш тісна інтеграція реального та віртуального світу, в якому спілкування здійснюється між людьми та пристроями. Передбачається, що в майбутньому "речі" стануть активними учасниками бізнесу, інформаційних та соціальних процесів, де вони зможуть взаємодіяти і спілкуватися між собою, обмінюючись інформацією про навколишнє середовище, реагуючи та впливаючи на процеси, що відбуваються в навколишньому світі, без втручання людини[2][3].

Прихід парадигми IoT передбачає різноманітні програми для передбачуваної більш розумної планети. Отримані результати з додатків усіх подій у космосі IoT - це ряд інтелектуальних та інтерактивних робочих середовищ і розумніших середовищ, таких як розумні будинки та офіси. Наприклад, Японська залізниця (JR) створює розумні залізничні станції, щоб підвищити зручність, вибір, комфорт і свободу мандрівників. Спритне середовище, як правило, складається з масиву нескінченно малих і інтелектуальних електронних речей, здатних сприймати контекст, діяти та

реагувати, виходячи з подій у середовищі. Крім того, цілі безперебійної мобільності, сумісності та взаємодії динамічно досягаються серед пристроїв, що беруть участь у роботі в середовищі. Крім того, розміщені пристрої можуть з'єднуватись та взаємодіяти з будь-якими іншими пристроями, що надходять в навколишнє середовище, шляхом формування дрібних, на вимогу, важливих та спеціальних мереж для досягнення конкретних завдань. Тому дотепер невідомі і непередбачені програми раціонального поєднання проникливих систем та датчиків можуть створюватися динамічно в режимі реального часу та надаватися будь-якому користувачеві на вимогу. Виняткові характеристики цих пристроїв - це самоорганізація, самовідновлення, самооптимізація, самоконфігурування та саморегулювання. Точніше кажучи, вони можуть повернутись до початкового стану, якщо є якісь серйозні перешкоди або катастрофа, і вони здатні автоматично створювати проникливі мережі з іншими поблизу. Іншими критичними активами та артефактами є різні типи високошвидкісних серверних машин, пристроїв зберігання даних та мережевих рішень. Знамениті складові в будь-яких інтелектуальних зонах включають в себе фізичні засоби, механіку, електроніку, обладнану смарт-марками, штрих-кодами, тегами, наклейками, точками, пилом, плямами, маяками, світлодіодними ліхтарями тощо.

Переваги IoT, як і бездротових сенсорних мереж:

- здатність до самовідновлення та самоорганізації;
- здатність передавати інформацію на значні відстані при малій потужності передатчиків(шляхом ретрансляції);
- низька вартість вузлів та їх маленькі розміри;
- простота встановлення, відсутність необхідності в прокладці кабелю (завдяки бездротовій технології живлення від батареї);
- можливість встановлення таких мереж на вже існуючих та об’єктах, що введені в експлуатацію без проведення додаткових робіт;
- низька вартість технічного обслуговування.

Приклад функціонування інтернету речей: розглянемо, як працює «розумна» кавоварка. Сьогодні середньостатистичний любитель пробуджуючого напою включає пристрій, засипає зерна в спеціальний відсік, наливає воду в контейнер, вибирає потрібний режим і отримує чашку кави. Але це не IoT, а тільки автоматизація процесу.

Щоб домогтися максимальної «самостійності», система повинна ставити на контроль кілька дій:

- вести облік залишків кави;
- планувати час покупки;
- формувати список:
  - оптимізувати покупки (якщо цукор теж закінчується, список оновлюється);
  - погоджувати план з користувачем;
  - в разі схвалення відправити повідомлення (перед походом в магазин);
  - в разі зміни плану перенести покупку;
  - навчатися (якщо господар переконаний, що зерна поєднуються тільки з тростинним цукром, і категорично не налаштований йти в магазин в п'ятничний вечір, значить, програма запам'ятовує цю інформацію і використовує її в подальшому).

Концепція інтернету речей заснована на так званих мультиагентних технологіях, які дозволяють співвідносити реальний світ з віртуальним. Для кожного учасника фізичного світу (машини або людини) встановлюється програмний агент - об'єкт з віртуального світу з задатками, який відповідає за інтереси реального учасника в інтернет-реальності. Віртуальний світ копіює наше життя, але філософія набагато простіше: учасники (далі - агенти) слідують заздалегідь встановленим правилам.

Агенти приймають дані з зовнішнього світу, обробляють їх і планують дії, які передають в реальний світ. Тобто в прикладі з кавоваркою агент кавових зерен скооперується з агентом цукру, їх запити потраплять до агента покупок,

який повідомить людині про необхідність поповнення запасів або навіть замовить доставку - з оглядкою на час і обставини.

Це складно, але цілком можливо завдяки існуванню універсального машинозчитуючого способу представлення знань(онтологію). Людина може задати логічні правила і сформулювати важливі концепції для агентів. Найдоцільніше створити окрему онтологію для кожної сфери застосування і прописати правила взаємодії між ними[4].

1.2 Базова архітектура

Оскільки IoT являє собою сенсорну мережу розглянемо загальну архітектуру сенсорної мережі.

Стандартизацією сенсорних мереж займається багато міжнародних організацій, серед яких ISO, IEC, ITU-T, IEEE та інші. Так дослідницька група по сенсорних мережах SGSN (Study Group on Sensor Networks) об’єднаного технічного комітету ISO/IEC JTC 1 (Joint Technical Committee 1) визначила базову архітектуру сенсорної мережі та її основні інтерфейси.

Сенсорний вузол складається з (рис. 1.2):

- апаратного забезпечення;
- базового програмного забезпечення;
- прикладного програмного забезпечення.

В складі архітектури визначені чотири базових інтерфейси:

1. Інтерфейс між базовим і прикладним програмними забезпеченнями сенсорного вузла.
2. Інтерфейс між базовим програмним і апаратним забезпеченнями сенсорного вузла (сенсори, актуатори та/або комунікаційний вузол і так далі).
3. Бездротові або дротові інтерфейси між вузлами мережі.

4. Інтерфейс між сенсорною мережею та зовнішнім середовищем (провайдери послуг, користувачі).

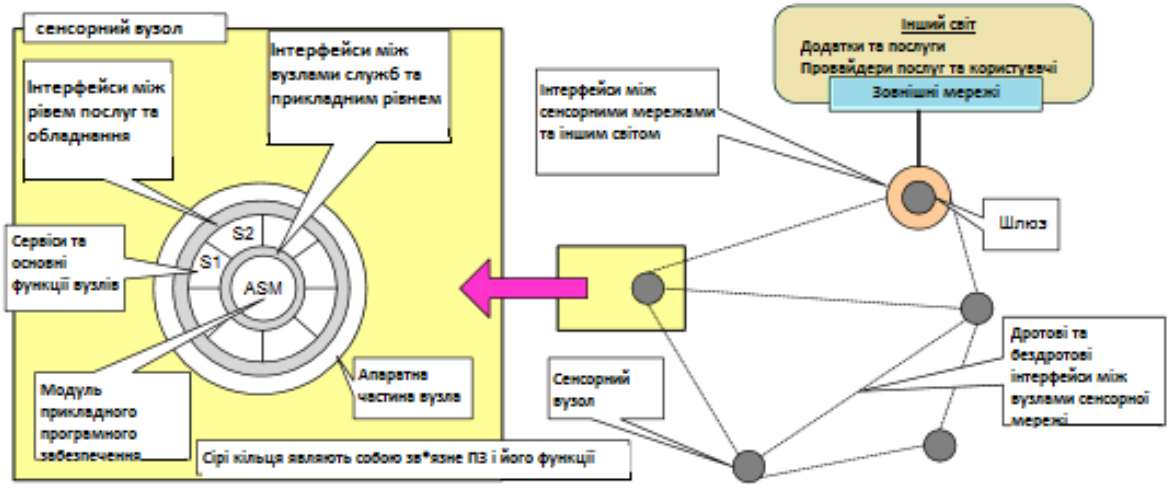

Рис. 1.2 Основні елементи та інтерфейси

Дані мережі складаються з мініатюрних обчислювальних пристроїв з датчиками, актуаторами і трансиверами (прийомопередавачами), що працюють в заданому діапазоні радіочастот. Такий вузол БСМ називають сенсорним вузлом або просто сенсором. Сенсорний вузол являє собою плату розміром зазвичай не більше одного кубічного дюйма. На платі розміщуються процесор, пам'ять - флеш і оперативна, цифро-аналогові і аналого-цифрові перетворювачі, радіочастотний приймач, джерело живлення і різні датчики, актуатори. Таким чином, апаратна частина вузла бездротової мережі може бути розділена на наступні чотири підсистеми (рис. 1.3):

1) комунікаційна підсистема - забезпечує бездротовий зв'язок з іншими вузлами в сенсорній мережі і містить радіо приймач;

2) обчислювальна підсистема - забезпечує обробку даних і функціональність вузла і складається з мікроконтролера MCU, до складу якого входять процесор, оперативна SRAM, незалежна EEPROM і флеш-пам'ять, аналого-цифровий перетворювач ADC, таймер, порти входу/виходу;

3) сенсорна підсистема - забезпечує з'єднання сенсорного бездротового вузла із зовнішнім світом, до складу якої можуть входити аналогові і цифрові сенсори, актуатори;

4) підсистема електроживлення - забезпечує енергетичне постачання всіх елементів бездротового сенсорного вузла і включає пристрої генерації і акумулювання енергії, а також регулювання напруги.

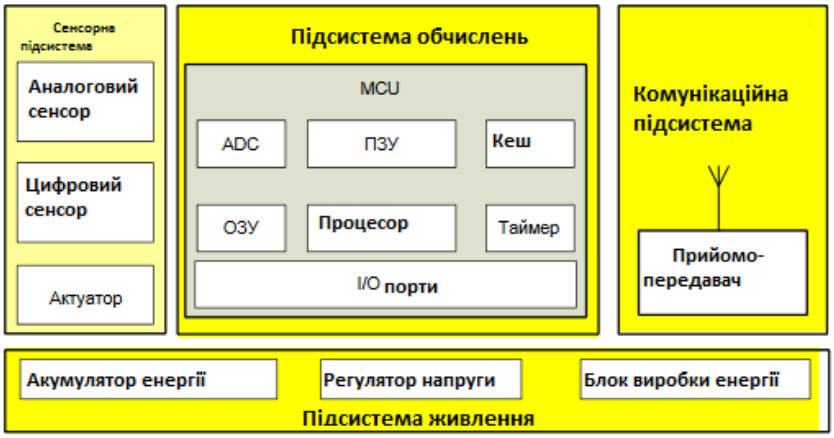

Рис. 1.3 Апаратна частина вузла сенсорної мережі

Датчики можуть бути найрізноманітнішими. Частіше використовуються датчики температури, тиску, вологості, освітленості, вібрації, розташування, рідше - магнітоелектричні, хімічні (наприклад, що вимірюють вміст CO, CO_2, рівень радіаційного фону), звукові і деякі інші. Набір застосовуваних датчиків залежить від функцій, які виконуються бездротовими сенсорними мережами.

Отримані від датчика електричні сигнали часто не готові для обробки, тому вони проходять через стадію перетворення. Наприклад, сигнал часто вимагає підсилення для збільшення амплітуди, можливе застосування фільтрів для усунення небажаного шуму в певних діапазонах частот і т.п. Перетворений сигнал трансформується за допомогою аналого-цифрового перетворювача (АЦП) в цифровий сигнал. В результаті сигнал виходить в цифровій формі і він готовий до подальшої обробки в процесорі і зберігання в пам'яті мікроконтролера. При наявності виконавчих механізмів можлива також передача керуючих впливів від вузлів мережі до зовнішнього середовища через актуатор. Живлення сенсорного вузла здійснюється зазвичай від невеликої батареї.

Крім розміру, є й інші жорсткі обмеження для вузлів БСМ, вони мають:

- споживати дуже мало енергії;

- працювати з великою кількістю вузлів на малих відстанях;

- мати низьку вартість виробництва;

- бути автономними і працювати без обслуговування;

- адаптуватися до навколишнього середовища[5].

Багаторівнева архітектура мережі IoT складається з:

1. Рівень об'єктів, також відомий як рівень пристроїв, містить фізичні пристрої, які використовуються для збирання та обробки інформації з екосистеми IoT. Фізичні пристрої включають різні типи датчиків, такі як ті, які зазвичай базуються на технологіях мікроелектромеханічних систем (MEMS). Датчики можуть бути оптичними, датчиками світла, датчиками, що реагують на жести та близькість, датчиками дотику та відбитків пальців, датчиками тиску та ін. Методи стандартизованого підключення і відтворення повинні використовуватися рівнем об'єктів, щоб інтегрувати та налаштовувати неоднорідні типи датчиків, що належать до пристроїв системи IoT. Дані пристрою, які збираються на цьому рівні переносяться на рівень абстракції об'єкта за допомогою безпечних каналів.

2. Рівень передачі даних, які збираються з об'єктів і передаються на рівень керування сервісом за допомогою безпечних каналів передачі. Передача даних може відбуватися за допомогою будь-якої з таких технологій:

- RFID
- 3G
- GSM
- UMTS
- Wi-Fi
- Bluetooth low energy
- Infrared
- ZigBee

У цьому шарі також присутні спеціалізовані процеси для обробки таких функцій, як хмарне обчислення та керування даними.

3. Рівень управління сервісом діє як проміжне програмне забезпечення для системи IoT. Цей шар надає конкретні послуги своєму запиту

на основі адрес і імен. Забезпечує гнучкість програмістів IoT у роботі над різними типами неоднорідних об'єктів незалежно від їхніх платформ. Цей шар також обробляє дані, отримані від транспортного рівня. Після обробки даних приймаються необхідні рішення щодо надання необхідних послуг, які потім виконуються за допомогою мережевих протоколів.

4. Рівень додатків забезпечує різноманітні види послуг, які вимагає замовник. Тип послуги, що запитується клієнтом, залежить від конкретного випадку використання, прийнятого замовником. Наприклад, якщо розумний дім є розглянутим випадком використання, тоді клієнт може вимагати певні параметри, такі як нагрівання, вентиляція та кондиціонування(HVAC), а також значення температури та вологості.

Цей рівень забезпечує різноманітні види інтелектуальних сервісів, які пропонуються різними гілками розвитку IoT. Деякі з провідних гілок IoT є:

- «розумні» міста;
- «розумна» енергія;
- «розумна» турбота про здоров’я;
- «розумні» будинки;
- «розумний» транспорт;
- «розумна» індустрія.

5. Бізнес рівень виконує загальне управління усіма діями та службами IoT. На цьому рівні використовуються дані, отримані від мережевого рівня, для створення різних компонентів, таких як бізнес-моделі, графіки та блок-схеми. Цей рівень також несе відповідальність за розробку, аналіз, впровадження, оцінку та моніторинг вимог системи IoT, здатний використовувати великий аналіз даних для підтримки прийняття рішень. А також на рівні виконується порівняння отриманих проти очікуваних результатів для підвищення якості послуг.

1.3 Протоколи архітектури

Рис. 1.4 Протоколи архітектури IoT

1.3.1 Протоколи інфраструктури

Протокол маршрутизації

RPL означає протокол маршрутизації для мереж низької потужності та втрат. Це протокол IPv6. Мережі з низьким рівнем втрат потужності включають в себе бездротові локальні мережі (WPAN), мережі низьковольтних лінійних зв'язків (PLC) та мережі бездротових датчиків (WSN). Ці мережі мають деякі характеристики:

- Можливість оптимізувати та заощадити енергію

- Можливість підтримувати схеми трафіку, відмінних від одноадресного спілкування

- Можливість запускати протоколи маршрутизації через шари каналів з обмеженими розмірами кадрів

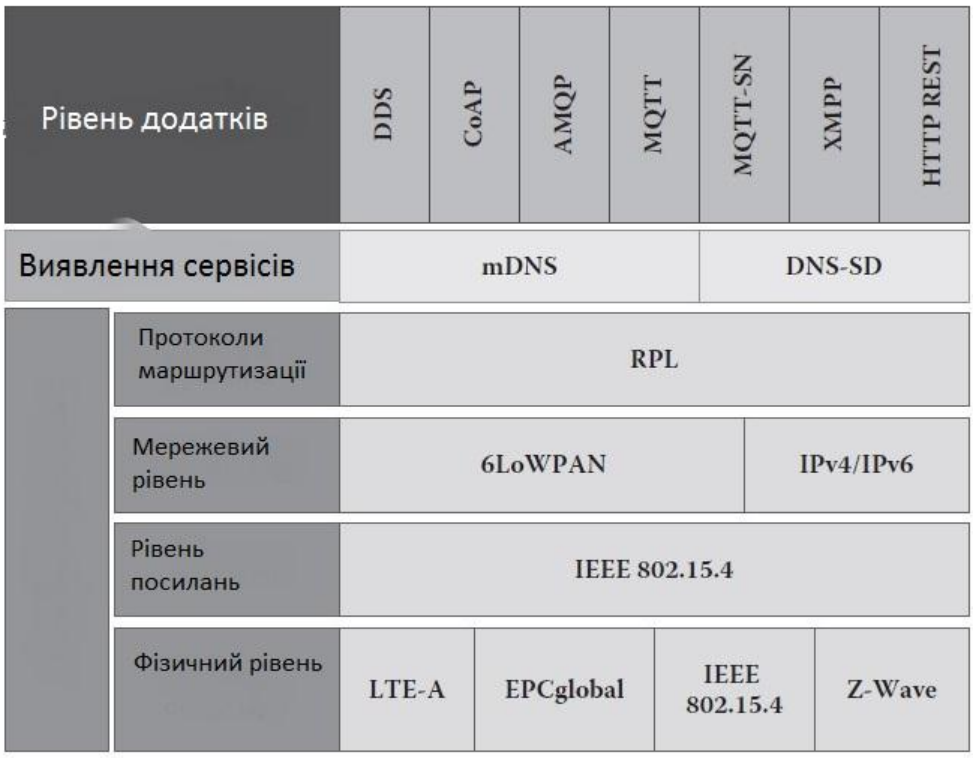

Рис. 1.5 Категорії протоколів IoT

RPL був розроблений, щоб підтримувати мінімальні потреби в маршрутизації шляхом створення високоточної топології над мережами з втратами. Цей протокол надає підтримку різноманітних типів моделей трафіку: багатоточкове, точка-багатоточка та точка-точка. Пристрої в мережі, що використовують цей протокол, підключаються один до одного таким чином, щоб у цьому з'єднання не було циклів. Для досягнення цього спочатку споруджується вузол, який називається цільовим орієнтованим ациклічним графіком (destination oriented directed acyclic graph, DODAG), який перенаправляється на одне призначення. Специфікації RPL звертаються до DODAG як до основи DODAG. Кожний вузол, який входить до складу DODAG, знає свій головний вузол, але не має інформації про його дочірні вузли. RPL підтримує щонайменше один шлях від кожного вузла до кореневого і до бажаного батьківського. Це зроблено для підвищення продуктивності пошуку швидшого шляху. Топологія DODAG, що використовується в RPL, зображена на рис. 1.6.

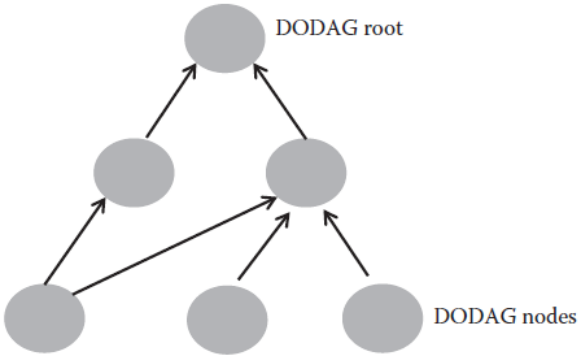

Рис. 1.6 Топологія DODAG

Маршрутизатори RPL працюють в одному з двох режимів роботи (MOP): режим не зберігання або зберігання. У режимі не зберігання повідомлення маршруту RPL рухаються у бік нижчих рівнів на основі маршрутизації джерела IP, тоді як у режимі зберігання маршрутизація вниз здійснюється на основі адресі призначення IPv6.

IEEE 802.15.4

Цей протокол був створений для того, щоб вказати підрівні для MAC та фізичного рівня, насамперед, для низькошвидкісних бездротових приватних мереж. Враховуючи різноманітні переваги, пропоновані цим протоколом, такі як низьке енергоспоживання, низька швидкість передачі даних, а також низька вартість та висока пропускна здатність повідомлень, вона дуже підходить для використання в системах IoT як протокол зв'язку. Цей протокол також забезпечує надійне з'єднання і може обробляти величезну кількість вузлів (приблизно близько 65K вузлів). Ідеально підходить для забезпечення зв'язку, оскільки забезпечує високий рівень безпеки, шифрування та служби автентифікації. Єдиною негативною стороною цього протоколу є те, що вона не забезпечує жодної з QoS(quality of service) гарантій.

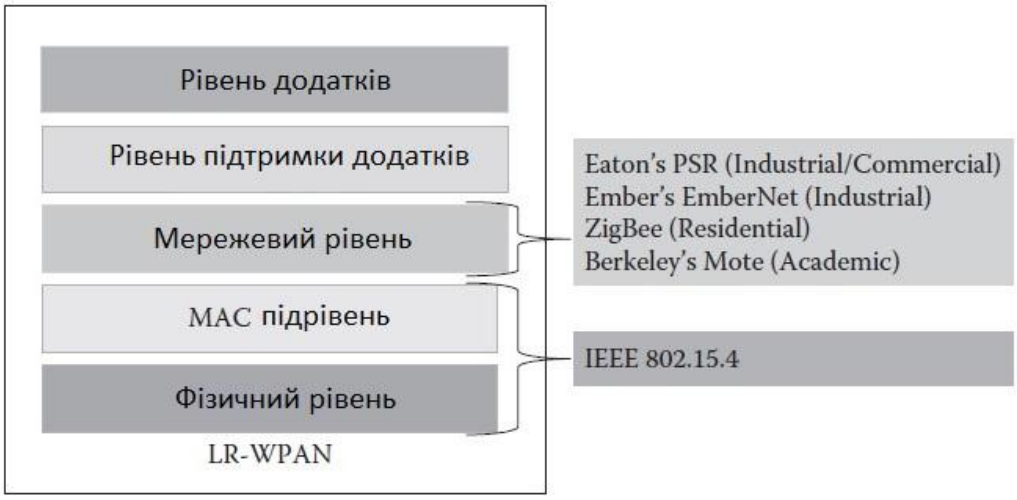

Рис. 1.7 Архітектура IEEE 802.15.4.

Цей протокол ґрунтується на ZigBee та інших протоколах, що використовуються в IoT-комунікації. IEEE 802.15.4 підтримує передачу у трьох частотних діапазонах, використовуючи метод DSSS(direct sequence spread spectrum). На основі частотного каналу, передача даних відбувається в три рази швидкість передачі даних:

- 250 kbps at 2.4 GHz
- 40 kbps at 915 MHz
- 20 kbps at 868 MHz

Цей протокол підтримує два типи вузлів мережі:

- Повнофункціональні пристрої (FFD)

- Знижено функціональні пристрої (RFD)

FFD можуть працювати як координатор персональної зони (PAN) або просто як звичайний вузол. Координатор має можливість створювати, керувати та підтримувати мережу. FFDs можуть зберігати таблицю маршрутизації у своїй пам'яті і можуть забезпечити MAC. Вони також можуть спілкуватися з іншими пристроями, використовуючи одну з наступних топологій:

- зірка;

- однорангова;

- кластерне дерево.

RFD - це дуже прості вузли, і вони мають обмежені ресурси. Вони можуть спілкуватися тільки з вузлом координатора, використовуючи тільки топологію зірки.

Топологія зірок: містить принаймні один FFD та кілька інших RFD. FFD, призначений для роботи в якості координатора PAN, повинен бути розташований у центрі мережі. Цей FFD несе відповідальність за управління та контроль усіх інших вузлів, які є частиною мережі (рис. 8).

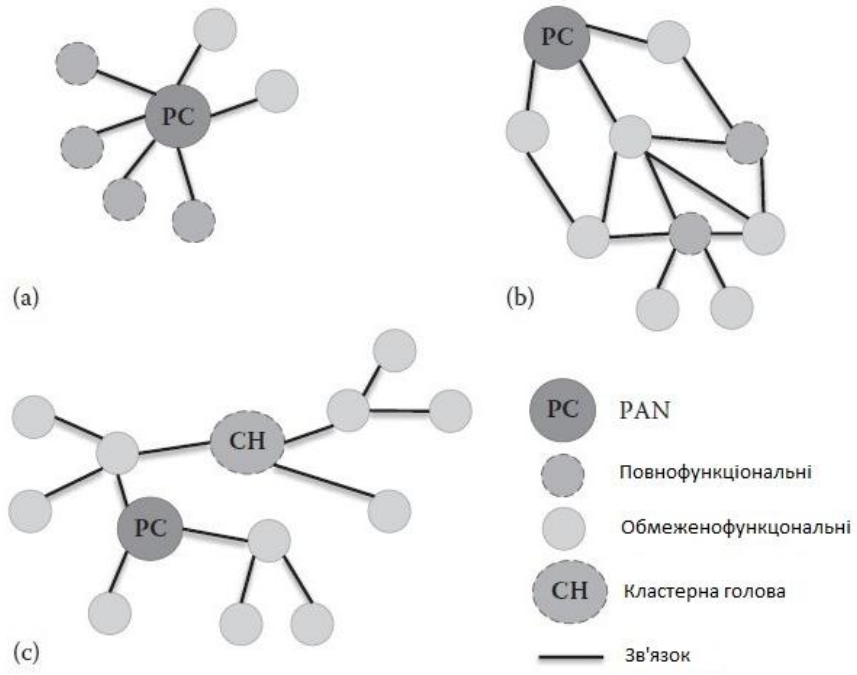

Рис. 1.8 Види топологій

Топологія однорангової мережі: вона містить координатора PAN, а інші вузли зв'язуються між собою в тій самій мережі або через проміжні вузли до інших мереж.

Топологія кластерного дерева: це особливий тип одноранговох топології. Він складається з координатора PAN, кластерної голови та нормальних вузлів.

IPv6 over Low-Power Wireless Personal Area Networks(6LoWPAN)

Архітектура сітки 6LoWPAN зображена на діаграмі, яка наведена на рисунку 1.9.

Вихідна лінія до Інтернету забезпечується точкою доступу (AP, access point), яка в цьому випадку є маршрутизатором IPv6. Різні типи пристроїв,

таких як ПК та сервери, можуть бути підключені до AP. Компоненти мережі 6LoWPAN підключаються до мережі IPv6 за допомогою маршрутизатора 6LoWPAN. Нижче наведено функції, які виконує «edge» маршрутизатор:

- Це дозволяє обмінюватися даними між пристроями 6LoWPAN та Інтернетом (або іншою IPv6 мережею).

- Це дозволяє обмінюватися даними між пристроями, що входять до мережі 6LoWPAN.

- Це допомагає генерувати та підтримувати мережу 6LoWPAN.

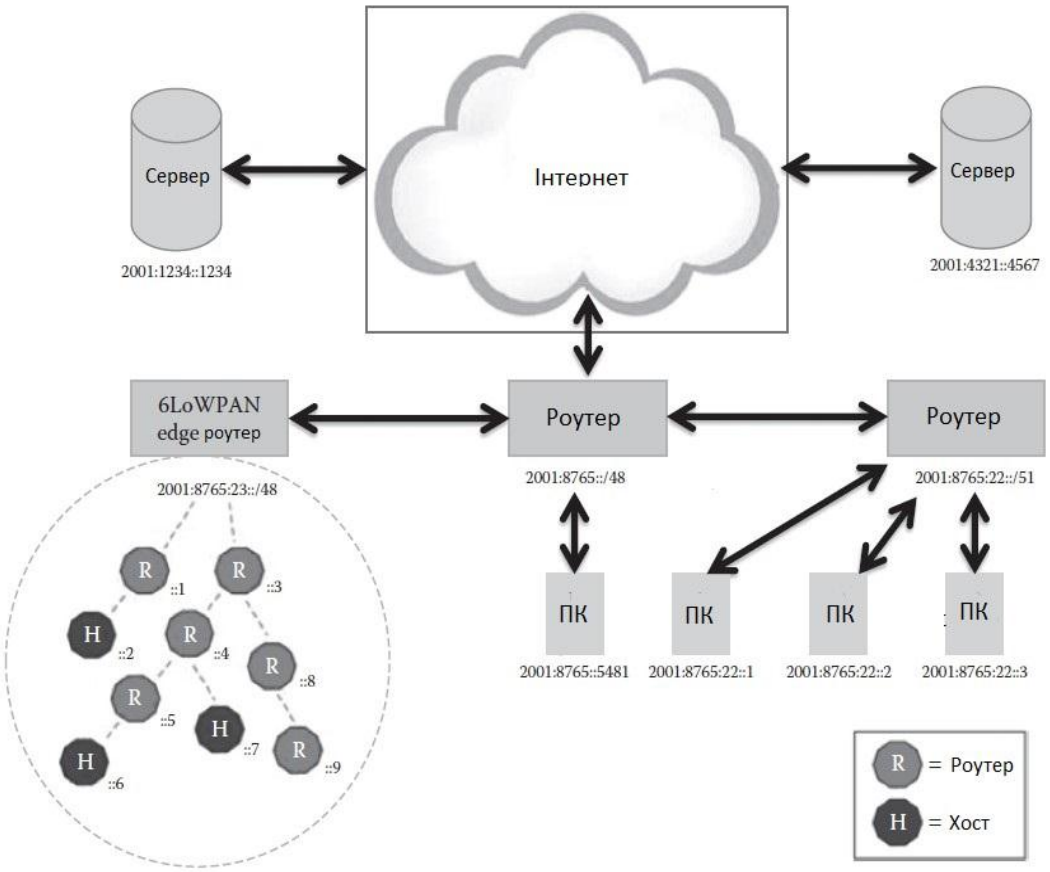

Рис. 1.9 Архітектура 6LoWPAN

Оскільки мережі 6LoWPAN можуть спілкуватися з IP-мережами, вони підключаються до IP-мереж просто за допомогою IP-маршрутизаторів.

«Edge» маршрутизатори, які використовуються для підключення мереж 6LoWPAN до інших IP-мереж, передають IP-датаграми між різними носіями, що використовуються в IP-мережах. Медіа, що використовується в мережі IP, може бути Ethernet, Wi-Fi, 3G або 4G. Оскільки «edge» маршрутизатори, що використовуються в мережевих датаграмах мережі 6LoWPAN для інших IP-

мереж із використанням мережевого рівня, вони не підтримують стан прикладного рівня. Це, в свою чергу, знижує робоче навантаження на «edge» маршрутизаторі з точки зору потужності обробки, що дозволяє використовувати дешеві вбудовані пристрої з простим програмним забезпеченням.

Bluetooth Low Energy

Bluetooth Low Energy (BLE) спочатку працював як частина базової специфікації Bluetooth 4.0. BLE використовує радіоприймач малої дальності з мінімальною потужністю і працює довгий час. Його діапазон охоплення становить близько 100 метрів, що приблизно в 10 разів перевищує звичайний Bluetooth. Затримка BLE в 15 разів менша за звичайну Bluetooth. BLE працює, використовуючи потужність від 0,01 мВт до 10 мВт. Ці характеристики роблять BLE ідеальним протоколом для використання пристроями IoT.

EPCglobal

RFID (радіочастотна ідентифікація) пристрої - бездротові мікрочіпи, які використовуються для позначення об'єктів для автоматичної ідентифікації. Електронний код продукту (EPC) - це унікальний ідентифікатор, що зберігається в тезі RFID, що допомагає ідентифікувати та відслідковувати елементи в сценарії керування ланцюжком постачання. EPCglobal - це організація, що розробила EPC, а EPCglobal також готує та підтримує стандарти, пов'язані з RFID та EPC. RFID може бути використана як ключова технологія для пристроїв IoT з наступних причин:

- Відкритість;
- Масштабованість;
- Надійність;
- Підтримка ідентифікаторів об'єктів та відкриття сервісів.

Тег RFID має дві основні компоненти: електронний мікросхеми для зберігання ідентичності об'єкта та антени, що дозволяє чіпу спілкуватися з системою читання тегів. Зв'язок між тегом і читачем тегів відбувається за допомогою радіохвиль. Два основних компоненти системи RFID:

- радіоприймач;

- читач тегів.

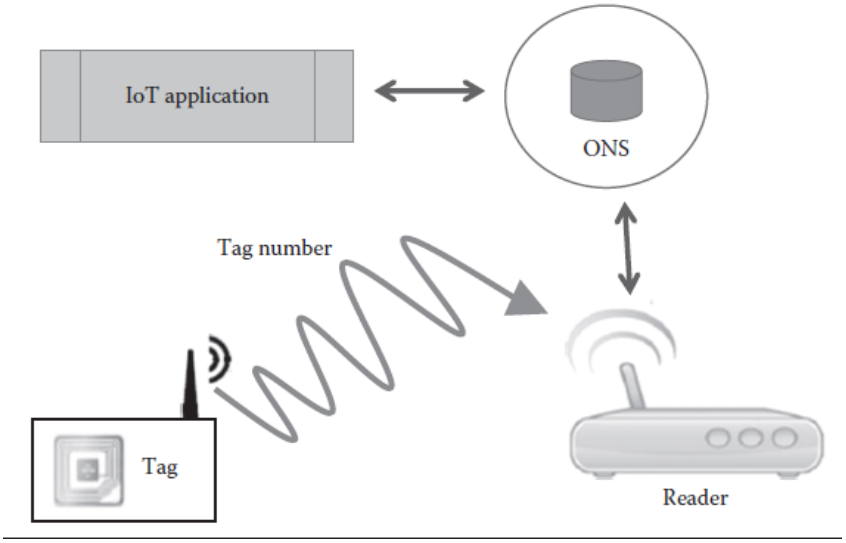

Рис. 1.10 Компоненти RFID системи

Z-Wave

Z-Wave - це протокол бездротового зв'язку з малою потужністю, який використовується переважно для домашніх мереж (HAN, home area networks). Він має широке застосування в розробці програм дистанційного керування для розумних будинків, а також інших невеликих комерційних областей. Z-Wave була розроблена компанією ZenSys, а пізніше вдосконалена альянсом Z-Wave. Z-Wave працює переважно в частотному діапазоні біля ГГц, що зазвичай становить близько 900 МГц.

Цей протокол використовує топологію мережевої сітки з малою потужністю. Кожен вузол або пристрій, що входить до складу мережі, має можливість надсилати та отримувати команди керування через стіни та поверхи будинку, і вони використовують проміжні вузли для маршрутизації даних навколо перешкод, які можуть бути присутніми в будинку. Складається мережа з контролерів та підпорядкованих пристроїв.

ZigBee

Протокол ZigBee був обрамлений альянсом ZigBee. Наступні особливості ZigBee роблять його дуже придатним для застосування IoT:

- Низьке енергоспоживання

- низька вартість

- Підтримка великої кількості вузлів мережі (<= 65K вузлів)

Крім особливостей, перерахованих вище, ZigBee має децентралізовану топологію мережі, яка дуже подібна до Інтернету. Цей протокол має можливість, яка дозволяє вузлам знаходити нові маршрути, якщо один маршрут не працює в мережі. Ця функція робить його дуже надійним бездротовим протоколом.

Специфікація ZigBee використовує нижні шари стека протоколу IEEE 802.15.4 і визначає власні верхні шари від мережі до програми.

1.3.2 Протоколи виявлення сервісів

multicast Domain Name System (mDNS)

mDNS - це служба, яка може працювати як унікальний DNS-сервер. Цей підхід дуже гнучкий через те, що простір імен DNS можна використовувати локально без будь-якої додаткової конфігурації. mDNS - це вигідний вибір для вбудованих пристроїв на базі Інтернету з наступних причин:

- Для керування пристроями не потрібна ручна настройка або адміністрування.
- Можна запустити без будь-якої додаткової інфраструктури.
- Високий рівень відмовостійкості через здатність функціонувати, навіть якщо відбудеться несправність інфраструктури.

DNS Service Discovery

Цей протокол допомагає клієнтам знаходити набір необхідних послуг, які присутні в мережі за допомогою стандартних DNS-повідомлень. Цей протокол також допомагає підключати пристрої без зовнішнього адміністрування або конфігурації. Виявлення служби DNS (DNS-SD) зазвичай використовує mDNS для надсилання пакетів DNS до певних адрес мультимовлення за допомогою UDP. Робота сервісу - це двоетапний процес:

1. Пошук назв вузлів необхідних служб
2. Об'єднання IP-адреси з іменами хостів, використовуючи mDNS.

Universal Plug and Play

Universal Plug and Play (UPnP) - це набір мережевих протоколів, який був розроблений форумом UPnP. Основні особливості UPnP, що робить його придатним для сервісного виявлення пристроїв IoT, є наступні:

- Можливість підключення пристрою UPnP до мережі динамічно (автоматично) та отримання IP-адрес інших пристроїв і одночасно передавати свої можливості на інші пристрої

- Конфігурація та адміністрування з нуля[6].

1.4 Стандартизація IoT

Питаннями стандартизації та практичного впровадження окремих складових Інтернету речей (M2M, RFID, всепроникні сенсорні мережі та ін.) займаються багато міжнародних організацій, неурядові асоціації, альянси виробників і операторів, партнерські проекти. В цілому для Інтернету речей, як нового напрямку розвитку інфокомунікацій, в даний час визначені найзагальніші концептуальні та архітектурні рішення. Найближчим часом основною проблемою буде гармонізація різних стандартів з метою формування єдиної і несуперечливої нормативної бази для практичної реалізації Інтернету речей[7].

В рамках діяльності сектора стандартизації телекомунікацій Міжнародного союзу електрозв'язку (МСЕ-Т) є три глобальні ініціативи GSI (Global Standards Initiative). Під глобальної ініціативою розуміється комплекс робіт, виконуваних паралельно різними дослідницькими комісіями МСЕ відповідно до скоординованих планом робіт. Одна з таких ініціатив присвячена стандартизації Інтернету речей - IoT-GSI (Global Standards Initiative on Internet of Things). Дві інші глобальні ініціативи - по стандартизації мереж наступних поколінь NGN-GSI і систем телебачення на основі протоколу Інтернет IPTV-GSI - також базуються на використанні IP-технологій, як і IoT-GSI.

IoT-GSI будує свою роботу на основі зусиль МСЕ-Т в таких областях, як мережеві аспекти ідентифікаційних систем (Network Identificator, NID),

всепроникні сенсорні мережі (Ubiquitous Sensor Networks, USN), межмашинного зв'язок (M2M), WEB речей (WoT) і т.п. В рамках серії МСЕ-Т Y.2xxx, присвяченій мереж наступного покоління NGN, вже затверджені перші рекомендації, присвячені спеціально Інтернету речей: Y.2060 «Огляд Інтернету речей», Y.2063 «Основа WEB речей» і Y.2069 «Терміни та визначення Інтернету речей »і ін.

В Рекомендації Y.2060 приведена еталонна модель IoT, яка дуже схожа на модель NGN і також включає чотири базових горизонтальних рівня (рис. 1.5):

–рівень додатків IoT;

–рівень підтримки додатків і послуг;

–мережевий рівень;

–рівень пристроїв[8].

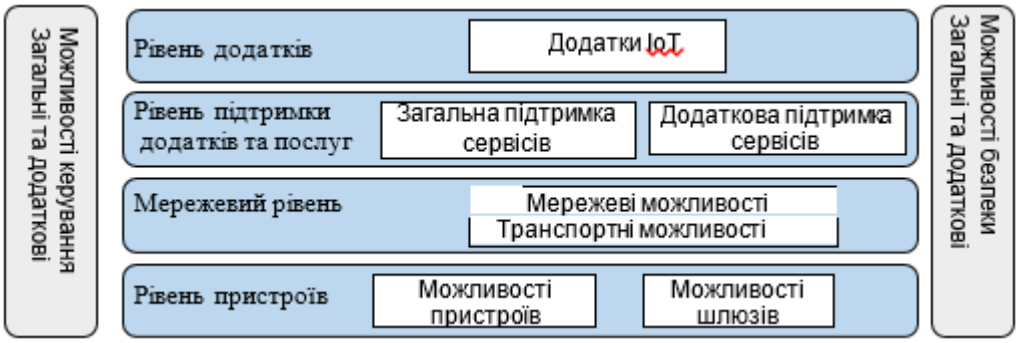

Рис. 1.11 Еталонна стандартизація IoT згідно МСЭ-Т Y.2060

Рівень додатків IoT в Рекомендації Y.2060 детально не розглядається. Рівень підтримки додатків і послуг включає загальні можливості для різних об'єктів IoT з обробки та зберігання даних, а також можливості, необхідні для деяких додатків IoT або груп таких додатків. Мережевий рівень включає мережеві можливості (функція управління ресурсами мережі доступу та транспортної мережі, управління мобільністю, функції авторизації, аутентифікації і розрахунків, AAA) і транспортні можливості (забезпечення зв'язності мережі для передачі інформації додатків і послуг IoT). Нарешті, рівень пристроїв включає можливості пристрою і можливості шлюзу. Можливості пристрою припускають прямий обмін з мережею зв'язку, обмін

через шлюз, обмін через бездротову динамічну ad-hoc мережу, а також тимчасові зупинки і відновлення роботи пристрою для енергозбереження. Можливості шлюзу припускають підтримку безлічі інтерфейсів для пристроїв (шина CAN, ZigBee, Bluetooth, WiFi і ін.) і для мереж доступу/транспортних мереж (2G / 3G, LTE, DSL і ін.). Іншою можливістю шлюзу є підтримка конверсії протоколів, в разі, якщо протоколи інтерфейсів пристроїв і мереж відрізняються один від одного.

Існує також два вертикальних рівня - рівень управління і рівень безпеки, що охоплюють всі чотири горизонтальних рівня. Можливості вертикального рівня експлуатаційного управління передбачають управління наслідками відмов, можливостями мережі, конфігурацією, безпекою та даними для білінгу. Основними об'єктами управління є пристрої, локальні мережі та їх топологія, трафік і перевантаження на мережах. Можливості вертикального рівня безпеки залежать від горизонтального рівня. Для рівня підтримки програм та послуг визначені функції AAA, антивірусний захист, тести цілісності даних. Для мережевого рівня - можливості авторизації, аутентифікації, захисту інформації протоколів сигналізації. На рівні пристроїв - можливості авторизації, аутентифікації, контроль доступу і конфіденційність даних.

Основною метою проекту Європейського інтеграційного проекту IoT-A (Internet of Things - Architecture), учасниками якого є різні компанії, є розробка еталонної архітектурної моделі Інтернету речей з описом основних складових компонентів, яка б дозволила інтегрувати різнорідні технології IoT в єдину взаємопов'язану архітектуру.

Функціональна модель IoT-A (рис. 1.12) дещо відрізняється від моделі MCE, хоча вона теж є ієрархічною, але складається вже з семи горизонтальних рівнів, що доповнюються двома вертикальними (управління і безпеки), які беруть участь у всіх процесах[9][10].

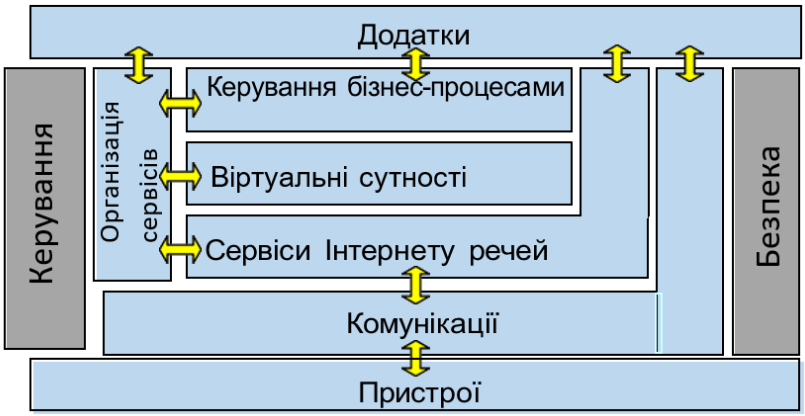

Рис. 1.12 Функціональна модель IoT-A

1.5 Проблеми реалізації IoT

При практичній реалізації IoT існує ряд проблем:

1.5.1 Проблема енергоспоживання.

Обмеження по енергоспоживанню пов'язаний з тим, що сенсори працюють від джерела живлення з обмеженим лімітом енергії (зазвичай батарейка). Чим рідше вони будуть замінюватися або заряджатися, тим нижчу вартість буде мати їх обслуговування. Також енергоспоживання є важливим обмеженням при використанні сенсорів, доступ до яких є ускладнений, отже, джерело живлення не може бути замінено або заряджено. Для зменшення енергоспоживання зазвичай передбачається відключення передавачів сенсорних вузлів, коли немає необхідності передачі інформації. На мережевому рівні використовуються оптимальні шляхи передачі інформації від сенсорного вузла до координатора (базової станції), з огляду на число проміжних вузлів, необхідну енергію і доступну енергію. Крім мережевого протоколу на споживання енергії впливає конструкція вузлів (наприклад, маленький розмір пам'яті, ефективність перемикань між завданнями), програмне забезпечення, механізми захисту і навіть робочі додатки.

1.5.2 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.

1.5.3 Проблема 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. Нещодавно в цій області був досягнутий великий успіх. Вчені анонсували придатний до комерційного використання наногенератор - гнучкий чіп, що перетворює в електроенергію людські рухи тіла (навіть одного пальця).

1.5.4 Проблема стандартизації

В області стандартів було досягнуто значного прогресу, проте попереду 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 великий і, що людство обов'язково знайде рішення для всіх перерахованих проблем. Це лише питання часу[11].

1.5.5 Проблема самоврядування

IoT, як і інші сенсорні мережі часто мають працювати у віддалених областях і в жорстких умовах, без можливості їх обслуговування і ремонту. Тому, сенсорні вузли повинні конфігуруватися самостійно, взаємодіяти з іншими вузлами, адаптуватися до поломок, змін навколишнього середовища без втручання людини.

1.5.6 Проблема децентралізованого управління

Алгоритми побудови багатьох IoT будуються за централізованим принципом. При децентралізованому управлінні сенсорні вузли повинні обмінюватися інформацією з сусідніми вузлами, щоб згенерувати рішення про комутацію вузлів, без глобальної інформації про всю мережі. Внаслідок цього децентралізовані алгоритми можуть бути неоптимальними, але більш ефективними щодо енергії, ніж централізовані. Наприклад, при централізованому управлінні базова станція може «опитувати» всі сенсорні вузли, приймати від них інформацію, повідомляти кожному вузлу свій маршрут передачі інформації. При частій зміні мережі втрати будуть значні. Децентралізований підхід дозволяє кожному вузлу робити власне рішення, при наявності невеликої інформації (список сусідніх пристроїв, що включає інформацію про відстань до базової станції). В даному випадку втрати на управління будуть значно зменшені.

1.5.7 Проблема конструкції

Головною метою IoT є створення маленьких, дешевих і ефективних пристроїв. Через вимоги до низького споживання енергії типовий сенсорний вузол має невеликі швидкості виконання операцій і обсяги інформації, що зберігається. Також через це небажано використання деяких пристроїв, таких як GPS-приймачі. Обмеження за розмірами впливає на структуру протоколів і алгоритмів, реалізованих в бездротових сенсорних мережах. Наприклад, таблиця всіх маршрутів в мережі може бути занадто великою і не помістится в пам'яті вузла. Тому тільки невелика частина інформації (наприклад, список сусідніх вузлів) може зберігатися в пам'яті вузла.

1.5.8 Проблема безпеки

Віддалене розташування сенсорів і їх автоматична робота збільшує їх незахищеність до сторонніх вторгненнь і атак. При бездротовому з'єднанні досить легко для порушника перехопити пакети, що передаються сенсорним вузлом. Наприклад, найбільш велика загроза здійснення атаки «відмови в обслуговуванні» (denial-of-service), мета даної атаки порушити коректне

функціонування сенсорної мережі. Це може бути досягло за допомогою різних способів, наприклад, при подачі потужного сигналу, який заважає сенсорним вузлів обмінюватися інформацією («білий шум» або jamming attack). Є різні варіанти захисту систем від зловмисників, але для багатьох з них необхідні високі вимоги до апаратний ресурсів, що є важкодосяжним на жорстко обмежених по багатьох вимогах сенсорних вузлах. Отже, IoT вимагають нових рішень для створення ключів, їх поширення, ідентифікації та захисту вузлів[12].

1.6 Практичне Застосування IoT

1.6.1 «Розумна планета»

Окремі масштабні проекти в напрямку створення «розумної» планети, свого роду «інтернет речей», енергійно розвиваються в останні роки. Так, Національне управління США з аеронавтики і дослідженню космічного простору (National Aeronautics and Space Administration, NASA) за підтримки компанії Cisco створює систему глобального збору даних про Землю - «Шкіру планети» (Planetary skin). Планується розробити онлайнову платформу для збору і аналізу даних про екологічну ситуацію, що надходять від космічних, повітряних, морських і наземних датчиках, розкиданих по всій нашій планеті. Ці дані стануть надбанням широкої громадськості, урядів і комерційних організацій. Вони дозволять в режимі, близькому до реального часу, вимірювати, доповідати і перевіряти екологічні дані, своєчасно розпізнавати глобальні кліматичні зміни і адаптуватися до них. Розробка платформи почалася з серії пілотних проектів, включаючи проект Rainforest Skin (букв. - «шкіра тропічних джунглів»), в ході якого буде досліджено процес знищення тропічних лісів в світовому масштабі.

В рамках програми Planetary Skin розробляються системи підтримки прийняття рішень, що дозволяють ефективно управляти такими природними ресурсами, як біомаса, вода, земля і енергія, кліматичними змінами і пов'язаними з ними ризиками (такими як підйом рівня світового океану,

посухи та епідемії), а також розвитком нових екологічних ринків, утворених навколо вуглеводнів, води і біологічного різноманіття.

Концепцію «розумної планети» Smart Planet пропагує компанія IBM. Суть її полягала в тому, що завдяки технологіям IoT можна зробити планету розумнішою. Сьогодні вплив цієї ідеї вже помітно відчувається по всьому світу в різних секторах і галузях, а також у нашому повсякденному житті.

Компанії, що працюють в сфері енергетики і енергопостачання, знаходять кращі, більш ефективні способи вироблення і розподілу електроенергії. Міста впроваджують рішення для управління дорожнім рухом, що допомагають суспільству заощадити час і гроші і при цьому підвищити якість життя. Компанії, що виробляють споживчі товари, використовують інтелектуальні технології для створення і поставки більш якісних продуктів в більш короткі терміни і за нижчою ціною. Системи охорони здоров'я використовують інформацію для зменшення числа помилок, скорочення витрат і забезпечення більш індивідуалізованого обслуговування.

Технології IoT на базі сенсорних мереж широко використовуються в екології, наприклад, відстеження руху птахів, дрібних тварин і комах, моніторинг стану навколишнього середовища з метою виявлення її впливу на сільськогосподарські культури і худобу, виявлення лісових пожеж, повеней, забруднень та ін. Починати будувати «розумну планету» потрібно з побудови «розумних будинків», об'єднуючи їх потім в «розумні міста», і продовжувати цей процес до тих пір, поки «цифровою інтелектуальністю» не буде наділена вся планета.

1.6.2 «Розумне місто»

В останні роки в містах інтенсивно створюються інформаційні системи для автоматизації окремих сфер міського життя: безпеки міського середовища, транспорту, енергетики і ЖКГ, охорони здоров'я, освіти, державного і муніципального управління та ін. Принципи і технології IoT дозволяють створити повнозв'язне інтегроване рішення, необхідне для функціонування

міського середовища і доступне всім жителям міста, співробітникам міських служб, чиновникам і керівникам різних рівнів.

Слід визнати, що Інтернет речей поки що не проник глибоко в елементи міської інфраструктури та господарства, але вже сформував сферу впливу, в рамках якої грає практично революційну роль. Це в першу чергу транспорт, енергетика та комунальні послуги, екологія, контроль злочинності, інформаційне забезпечення жителів міста і інтерактивне управління домогосподарством.

Інтелектуальні мобільні пристрої і високошвидкісні територіально розподілені мережі для доступу до них, сенсори, що вбудовуються в міське середовище - все це забезпечує основу для створення всеосяжних міст (ubiquitous city), або u-міст, в яких об'єкти інфраструктури і люди тісно пов'язані. Уряду декількох країн вже прийняли масштабні програми створення інтелектуальних міст U-City.

Найбільш ефективні U-системи (пов'язані на основі Інтернету речей) - це комунальна, транспортна, паркувальна служби, а також служба боротьби з вуличною і побутової злочинністю. Це, по суті, ключові проблеми міського життя, які можна вирішити на основі єдиної системи моніторингу та контролю. Так, в корейському місті Eunpyeong New Town ефективно працює U-система в сфері торгівлі у вигляді порталу з інформацією про магазини, кафе і т.д., а також система контроля розташування дітей, призначена для батьків. За допомогою сайту Uber в Києві можна відстежити переміщення замовленої машини, виявити найближчих водіїв на онлайн-карті. Збір інформації від автобусів, обладнаних системою GPS або ГЛОНАСС, дозволяє створювати інтерактивні табло, онлайн-ресурси і додатки, які інформують жителів про те, скільки їм доведеться чекати автобуса. Наприклад, в Москві на Тверській вулиці встановлені п'ять перших «розумних» зупинок, забезпечених сенсорними панелями. Тепер пасажири можуть прокласти свій шлях на інтерактивній карті і дізнатися точний час прибуття автобуса чи тролейбуса. У Москві планується також оснастити парковки інтелектуальною системою,

яка дозволить автомобілістам отримувати інформацію про вільні паркувальні місця в режимі реального часу.

Інший цікавий приклад - розумні сміттєві контейнери. Сигнал про наповнення подається в централізовану систему управління, яка відстежує на карті всі сміттєзбиральні машини і включає наповнений контейнер в маршрут найближчого вантажівки. І це теж вже не фантастика: саме так працює сміттєзбиральна система в Дубліні і Барселоні.

Ідея використовувати в Інтернеті речей таку просту, що отримала повсюдне поширення технологію, як стільниковий зв'язок, знаходить все більше застосування в усьому світі. У майбутньому смартфони городян сформують мережу, що постійно розширюється, муніципальними датчиками. Зараз вчені експериментують з вбудованими датчиками в стільникові телефони для вирішення соціальних проблем (наприклад, збору даних по забрудненню повітря або рівню радіації) так, щоб звести до мінімуму або навіть нулю потребу в допомозі з боку городян.

1.6.3 «Розумна енергія»

В даний час найбільш опрацьованим варіантом застосування технологій IoT є «розумні мережі» (Smart Grids) в енергетиці. Робота такої мережі заснована на тому, що постачальник і споживач отримують об'єктивну картину по використанню енергоресурсів за рахунок моніторингу на всіх ділянках мережі і, як наслідок, отримують можливість оперативного управління. У разі аварій такі мережі здатні автоматично ідентифікувати проблемні ділянки і протягом короткого часу направляти електроенергію по резервними схемами, відновлюючи електропостачання. для споживачів. «Розумні» мережі означають можливості за гнучким регулювання споживання електроенергії, як у «ручному», так і в автоматичному режимі.

Управління енергомережею проводиться за допомогою наступних систем (рис.1.12):

- «Розумної» маршрутизації енергопотоків (Smart Routing) - системи контролю навантаження і якості, самовідновлення мереж в результаті аварійних подій, зберігання енергії та ін.;
- «Розумних» вимірювань (Smart Metering) - сучасні інтелектуальні прилади обліку (Smart Meter), системи інтелектуальної будівлі (Smart Home), «розумні» побутові прилади.

«Розумний» (або інтелектуальний) лічильник (Smart Meter) - прилад обліку енергоресурсів з розширеними можливостями, який дозволяє контролювати величину спожитих енергоресурсів і періодично передавати інформацію через телекомунікаційну мережу постачальника енергоресурсів або в центр обліку та розрахунків за житлові та комунальні послуги. «Розумні» лічильники можуть вимірювати витрату електроенергії, газу, води, тепла, а також володіти додатковими можливостями[15].

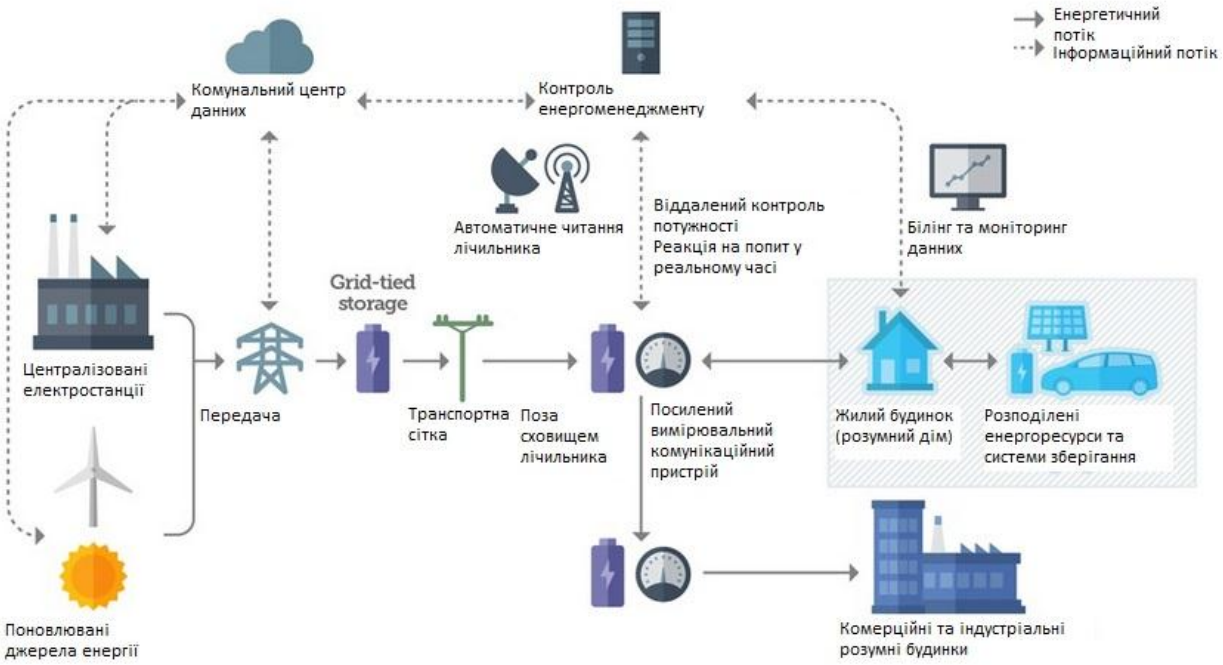

Рис. 1.13 Схема «розумної» мережі Smart Grid[13]

«Розумний» прилад обліку володіє наступними технічними особливостями:

1. Формує і зберігає поточні і архівні значення спожитих енергоресурсів. Обсяг архівних даних залежить від розміру пам'яті контролера приладу.

2. Має вбудований годинник реального часу, які вимагають періодичної синхронізації з єдиного центру.

3. Володіє можливістю взаємодії з інформаційною системою, що управляє для формування балансу споживання, обліку допуску приладу.

4. Має стандартний цифровий інтерфейс для обміну даними з автоматизованою системою обліку споживання енергоресурсів та (або) телекомунікаційну частина для віддаленої передачі даних в центр обліку та розрахунків.

Основні вимоги, що пред'являються до «розумним» мереж, такі:

- можливість «самовідновлення» мережі після замикань, фізичних ушкоджень та ін .;

- можливість мотивування споживачів для активної участі в регулюванні мережі (за допомогою регулювання власного споживання);

- висока стійкість до шкідливих зовнішніх впливів (теракти, диверсії і т.п.);

- можливість надання електроенергії високої якості (в т.ч. з заданими параметрами) і скорочення втрат;

- інтеграція опцій виробництва і зберігання електроенергії;

- висока ефективність.

Розвиток технологій «розумних» мереж (Smart Grid) і «розумних» лічильників (Smart Metering) несе в собі перспективу того, що всі промислові і побутові енергоприймачі знайдуть здатність до взаємодії в інформаційній мережі, стануть керованими і будуть виконувати функції вимірювання власного споживання електроенергії і потужності. Це дасть реальний інструмент для енергозбереження та підвищення енергоефективності.

1.6.4 «Розумний транспорт»

Інтелектуальні транспортні системи ITS (Intelligent Transportation System) на базі технологій IoT дозволяють здійснювати автоматичну взаємодію між об'єктами інфраструктури і транспортним засобом V2I (Vehicle to Infrastructure) або між різними транспортними засобами V2V (Vehicle to Vehicle). Системи V2V здійснюють обмін даними по бездротовому зв'язку між машинами на відстані до декількох сот метрів. Системи V2I здійснюють обмін між транспортним засобом і центрами управління дорожнім рухом, операторами доріг і сервісними компаніями. Дані, передані об'єктами інфраструктури, інтегруються в загальну систему і передаються довколишніх транспортним засобам. Технології обох груп здатні значно збільшити безпеку і ефективність транспорту.

Як приклад використання технологій IoT в містах можна привести систему управління автомобільним трафіком (рис. 2.6), яка на основі аналізу пропускної здатності доріг не тільки самостійно управляє трафіком за допомогою перенастроювання світлофорів, а й постійно в реальному часі публікує дані про свій стан, які можуть бути доступні будь-яким іншим пристроям і сервісам, будь-то ГЛОНАСС/GPS-навігатор, мобільний телефон або спеціалізовані веб-сайти. Використання технології IoT в транспортній сфері дозволяє не тільки відслідковувати оповіщення про критичні ситуації, але також перенаправляти маршрути руху в режимі реального часу і навіть попереджати пасажирів і водіїв про альтернативні маршрути, транспортні засоби, придорожнє житло і пункти громадського харчування. Крім того, за допомогою встановлених на вулицях датчиків можна буде забезпечити публікацію інформації про їх завантаженість[10].

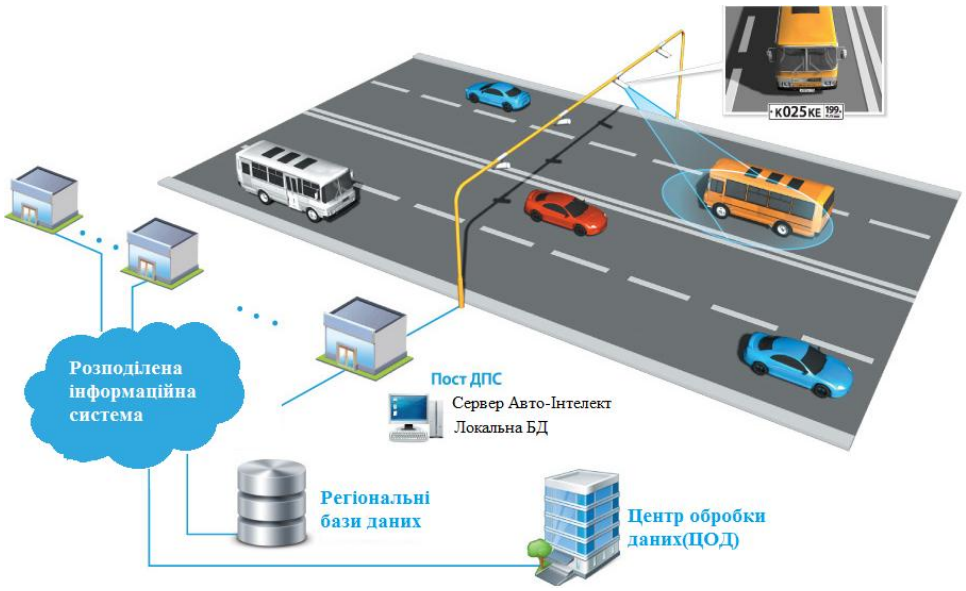

Рис. 1.14 Система інтелектуального керування транспортом[14]

Серед таких «розумних» транспортних систем IoT можна згадати:

- системи запобігання зіткнень;
- системи «бічної підтримки», що вказують водію на перетин дорожніх смуг або небезпечні маневри;
- системи нічного бачення;
- системи автоматичного управління машиною і руху в групах машин;
- системи, які контролюють стан водія (зокрема, що не дозволяють йому заснути);
- системи превентивного реагування на аварійну ситуацію (наприклад, системи, що здійснюють попереднє натягування ременів безпеки перед неминучим зіткненням).

Система інформування водіїв за допомогою вбудованих в машині пристроїв VICS (Vehicle Information and Communication System) збирає інформацію через сенсори, встановлені на об'єктах дорожньої інфраструктури (дорожньому полотні, камерах спостереження та ін.), З використанням «машин-зондів» (мобільних пунктів спостереження за дорожнім рухом), а також шляхом використання вже встановлених бортових систем, що дозволяють збирати інформацію про швидкість руху транспортного потоку, погоді і стан доріг. Ця інформація системою VICS обробляється і переводиться

в цифровий вигляд, а потім розсилається по бортовим навігаційним системам. Користувачі системи можуть отримувати інформацію в різних видах - у вигляді тексту, простої графіки, карт. Бортові системи динамічно обробляють дані і пропонують водієві оптимальний маршрут.

1.6.5 «Розумне виробництво»

Вважається, що винахід парової машини в XVIII столітті викликало першу індустріальну революцію. Наступний якісний стрибок стався в промисловості на початку XX століття при переході на конвеєрне виробництво. Потім, з 1960-х роках, процеси на підприємствах почали кардинально змінюватися завдяки впровадженню комп'ютерів. І ось зараз ми стаємо свідками стрімко наростаючою четвертої індустріальної революції, рушійною силою якої є Інтернет речей. За рахунок технологій IoT виробничі компанії зможуть оптимізувати все - від роботи складу до виконання безпосередньо виробничих завдань, якщо кожне промислове будівництво, транспортний засіб і навіть інструмент будуть забезпечені сенсорами і регулярно будуть відправляти звыт про свій стан, місцезнаходження та інші характеристики.

Наведемо конкретний приклад. Оскільки вимоги до якості і безпеки автомобілів неухильно ростуть, виробники зацікавлені в можливості контролювати роботу основних систем і деталей вже випущених і проданих машин. Іншими словами, автозавод хоче залишатися з ними в контакті, і завдяки Всесвітній мережі це можливо. В майбутньому будь-який автомобіль стане частиною Інтернету речей. Машина зможе зв'язуватися зі своїм виробником і, наприклад, повідомляти йому, що потребує дострокове техобслуговуванні. Сенсори в режимі онлайн будуть сповіщати, наприклад, про перегрів, вібрації, передчасному зносі певного вузла або, скажімо, про незвичні звуки.

Подібні інтелектуальні цифрові системи надалі встановлюватимуть на будь-яких машинах і верстатах, але перш за все на обладнанні таких системоутворюючих об'єктів, як, наприклад, електростанції. Кожен вузол

верстата або обладнання буде займатися самодіагностикою і через інтернет повідомляти про свій стан до відповідного експлуатаційного центру управління. Такі рішення будуть мати цілий ряд переваг для самих виробників. Так, компанії зможуть краще планувати випуск і поставку запчастин, вони отримають можливість відстежувати, наскільки часто ті чи інші вузли стикаються з певними проблемами, і своєчасно вносити необхідні інженерно-конструкторські зміни. До того ж вони зможуть цілеспрямовано інформувати клієнта про необхідність замінити той чи інший вузол.

Нарешті, виробники зможуть перевіряти, чи використовує клієнт якісні фірмові запчастини або вдається до дешевих підробок. Проблема ця досить гостро стоїть сьогодні перед багатьма компаніями і в цілому машинобудівної галуззю, яка зіткнулася з потоком контрафактної продукції. Для перевірки справжності запчастин в обладнання будуть, наприклад, вбудовувати чіпи, які знають, де в інтернеті знаходиться відповідна документація виробника. При заміні деталей вони перевірятимуть «Новачків» і звіряти отриману інформацію з рідною базою даних. Таким чином, машинобудівна продукція надалі буде існувати як би в двох іпостасях. Одна - реальна, «залізна», а інша - віртуальна, у вигляді набору цифрових даних.

Завдяки IoT стане можливим об'єднання всіх контрольно-вимірювальних приладів і датчиків на будь-якому виробництві в єдину інформаційну мережу. Крім ефективного витрачання енергії можна буде навіть швидко інтегрувати в систему альтернативні джерела екологічно чистої електрики - наприклад, сонячні батареї і вітряні генератори. Зниження виробничих витрат, ефективна витрата енергії, відмова від економічно нерентабельних активів – все це разом дозволить суттєво здешевити виробництво, а використання поновлюваних джерел електрики поліпшить екологічну обстановку.

Ще один сучасний прояв Інтернету речей - зв'язок між машинами (M2M) за допомогою SMS. В Європі цю технологію вже використовують в сільському господарстві для стеження в реальному часі за переміщеннями великої рогатої худоби. Крім стеження за переміщенням худоби, фермери отримують

автоматичні повідомлення про стан тварин. В стійлах і в полі встановлюються забезпечені SIM-картами пристрої для зв'язку M2M, а до тварин прикріплюються спеціальні датчики, що збирають інформацію і передають її на пристрій збору даних. Це пристрій негайно відправляє фермеру потрібну інформацію за допомогою SMS. За даними про стан тварин можна спостерігати не тільки через SMS, але і в онлайновому режимі через канал GPRS, що зв'язує системи моніторингу з центром обробки даних. У Європі таким додатком вже користуються близько 4 тисяч ферм.

1.6.6 «Розумна медицина»

«Розумна медицина» на базі Інтернету речей на практиці зазвичай реалізується у вигляді систем моніторингу здоров'я людей з використанням різноманітних біосенсорів, датчиків і систем віддаленої медичної допомоги. Можливі застосування систем моніторингу на базі сенсорних мереж в медицині:

1. *Моніторинг фізіологічного стану людини*: фізіологічні дані, зібрані сенсорними мережами можуть зберігатися протягом тривалого періоду часу і можуть використовуватися для медичного дослідження. Встановлені вузли мережі можуть також відстежувати рухи літніх людей, інвалідів та, наприклад, попереджати падіння. Ці вузли невеликі і забезпечують пацієнтові велику свободу пересування, в той же час дозволяють лікарям виявити симптоми хвороби заздалегідь. Крім того, вони сприяють забезпеченню більш комфортного життя для пацієнтів в порівнянні з лікуванням в лікарні.

2. *Моніторинг лікарів і пацієнтів в лікарні*: кожен пацієнт має невеликий і легкий вузол мережі. Кожен вузол має свою конкретну задачу. Наприклад, один може стежити за серцевим ритмом, в той час як інший знімає показання кров'яного тиску. Лікарі можуть також мати такий вузол, він дозволить іншим лікарям знайти їх в лікарні.

3. *Моніторинг медикаментів у лікарнях*: сенсорні вузли можуть бути приєднані до ліків, тоді шанси видачі неправильного ліки, можуть бути зведені до мінімуму. Так, пацієнти матимуть вузли, які визначають їх алергію і

необхідні ліки. Комп'ютеризовані системи показують, що вони можуть допомогти звести до мінімуму побічні ефекти від помилкової видачі препаратів.

Одним з етапів вдосконалення сучасної медицини є персоналізація даних і підвищення комунікації між лікарями. Легкий доступ до історії хвороби, дозволяє призначати своєчасне ефективне лікування. Ведення медичних карт поступово може перейти в мережу. «Хмарні» рішення використовуються для зберігання великих обсягів інформації в інтернеті. Завдяки інтернету лікарі різних клінік отримують доступ до даних пацієнта. Електронні медичні картки дають змогу вчасно дізнаватися про здоров'я хворого, призначати ефективне лікування. Зв'язування обладнання медичного закладу в єдину мережу дозволить отримувати необхідні дані на портативні пристрої лікарів, на які надходить інформація про пацієнта: які ліки прописані, результати аналізів і т.д.

Впровадження інтернет-технологій заощаджує час пацієнта і лікаря ,адже за допомогою комп’ютера відбувається відео-зустріч. Якщо все-таки необхідна зустріч з лікарем, то записатися на прийом можна також через інтернет.

Апарати для вимірювання тиску, ваги та інше портативний обладнання оснащується бездротовими передавачами, які дозволяють дані відразу переносити на комп'ютер і вести облік за своїм здоров'ям за допомогою чіпів, що вшиваються в одяг та передають дані на мобільний телефон. «Розумний одяг», який збирає дані про стан людини: частоту серцевого ритму, температуру тіла, частоту дихання. [10].

Висновок: IoT являється системою, що швидко розвивається, має різні будови та широкий спектр застосування, проте перш за все це набуває популярності серед звичайних людей і створюються пристрої, що зможуть створити власний розумний будинок, будову якого слід розглянути, а також, на його прикладі, загрози та атаки, що чатують з приходом IoT в нашу буденність.

РОЗДІЛ 2. АНАЛІЗ ВРАЗЛИВОСТЕЙ «РОЗУМНОГО ДОМУ»

2.1 Елементи «розумного дому»

Зростаюча різноманітність інтелектуальних датчиків, програмних рішень, підключених пристроїв, хмарних сервісів те що встановлено, щоб ми могли працювати в різних формах та форматах у наших живих та робочих середовищах. Це квартири, офісні будівлі, виробничі поверхи та інші орієнтовані на дії, жваві та чудові місця, мають бути надзвичайно потужними та розширені технологіями. Звичайні і повсякденні об'єкти цифруються, з'єднуються один з одним локальної. Це - все, що в наших місцях, систематично наділяється відповідними та правильними інтелектуальними можливостями шляхом додавання функціональних модулів всередині, а також шляхом інтеграції з віддаленим програмним забезпеченням. Навіть комунікаційні мережі наповнюються відповідними компетенціями та можливостями, щоб покращити роботу, випадкову та дешеву річ зробити розумною, будь-яку електроніку більш розумною, і в кінцевому підсумку люди - найрозумніші.

Всі види недоліків та залежностей усуваються за допомогою безлічі таких заходів, як стандартизація, адаптери, мости, проміжне програмне забезпечення, загальні інтерфейси API тощо. Можливості підключення і відтворення гарантуються. Пристрої виробляються належним чином та модернізуються, щоб об'єднувати та співпрацювати один з одним для реалізації завдань, орієнтованих на людей. Збирання інформації, агрегація, поширення, важелі впливу для полегшення розуміння інформації та концепцій візуалізації, що постійно посилюються до бачення більш інтелектуальних середовищ. Пристрої виробляються з використанням дуже сильної фабричної моделі/індустріалізації. Всі високотехнологічні IT-сервери, сховища та мережеві рішення підлягають товарообігу. Це досягається шляхом виявлення та абстрагування всіх видів загальних функціональних можливостей, особливостей та засобів. Всі реалізовані через програмне забезпечення. Важливі аспекти, такі як модифікованість, заміна, підставість, доступність,

витратні можливості тощо легко інтегруються в програмне забезпечення. Політика та бази знань у поєднанні з менеджером знань з'являються як механізм нового покоління для створення автономічної інфраструктури. Програмний маршрут рекомендується для встановлення політики та виконання.

«Розумний будинок» призначений для максимально комфортного життя людей за допомогою використання сучасних високотехнологічних засобів. Принцип роботи системи «розумний дім» полягає в автоматизації всього, з чого складається житлова споруда: освітлення, кондиціонування, система безпеки, електроенергія, опалення, водопостачання та водовідведення і так далі. До основних підсистем «розумного будинку» відносяться: клімат-контроль, освітлення, мультимедіа (аудіо і відео), охоронні системи, зв'язок і інші(рис. 2.1)

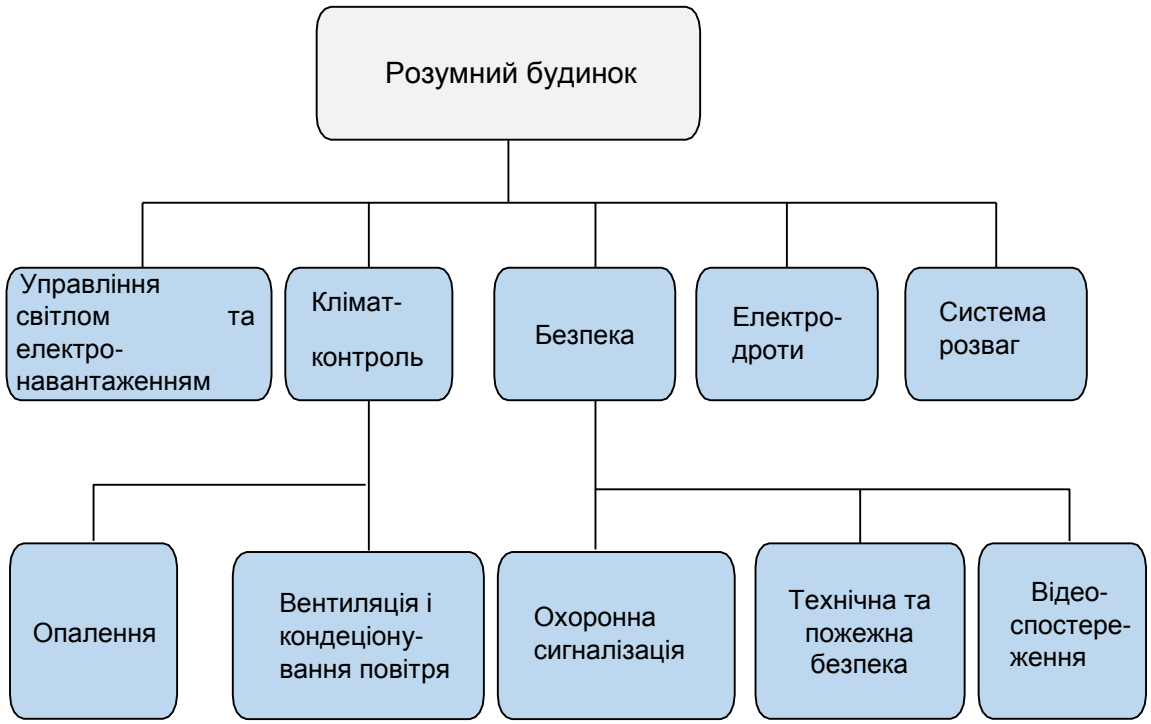

Рис. 2.1 Складові «розумного будинку»

У стандартному проекті «розумного будинку» можна виділити три основні підмережі: мережа мультимедійних пристроїв, мережа електроосвітлювального обладнання і сенсорну мережу. В останньому випадку це датчики руху, світла, температури, тиску, вологості, вібрації і т.п.

Таким чином, «розумний дім» складається з програмного і апаратного забезпечення, датчиків і провідний / бездротової мережі.

У загальному випадку, «розумний дім» надає його власнику такі переваги:

1) зниження споживання ресурсів (газ, вода, електроенергія);

2) високий рівень комфорту;

3) забезпечення необхідної взаємодії всіх систем об'єкта нерухомості, що автоматизуються, задання різних режимів роботи;

4) зниження ймовірності виникнення аварійних ситуацій;

5) підвищення оперативності, простоти і зручності управління.

Рис. 2.2 Компоненти «розумного будинку»

Для автоматизації будинку смарт-вузли можуть бути інтегровані безпосередньо в побутових пристроях, наприклад в пилососи, мікрохвильові печі, холодильники і телевізори. Вони можуть взаємодіяти один з одним і з зовнішньою мережею через Інтернет. Це дозволить кінцевим користувачам легко управляти пристроями будинку як локально, так і віддалено. Більшість побутових пристроїв з категорії «розумних» речей можна поділити на дві групи за типом використання Інтернету.

До першої групи належить техніка, яка через WWW оновлює своє програмне забезпечення, отримує нові функції, приймає сигнали, коли

знаходиться далеко господаря, і, відповідно, відправляє йому інформацію, яка підтверджує виконані дії та свій стан. Цей тип використання Інтернету побутовою технікою є найбільш розумним і здатний довести потенційному споживачеві свою корисність.

До другої групи входить техніка, в якій Інтернет є як би стороннім тілом. Суть рішення в тому, що в абсолютно звичний побутовий прилад, типу мікрохвильовки або холодильника, вбудовується спрощений комп'ютер і дисплей, після чого з їх допомогою можна отримувати мультимедійні розваги там, де їх раніше не було, наприклад, на тій же кухні.

Одним з найперших прикладів побутової техніки, що має підключення до Інтернету, є звичайний тостер, оснащений інтерфейсом для віддаленого включення і повідомлення про готовність підсмаженого тосту. Так техножарт Джона Ромки, одного з перших фахівців в області TCP / IP-протоколу, породила в далекому 1988 році технотренд Інтернету речей, який в наші дні втілюється в життя.

Зростаючий список відомих домашніх мереж та рішень для автоматизації включає в себе наступне:

▪ *Елементи безпеки та спостереження*: датчики безпеки для вікон, дверей, руху, розбиття скла та диму можуть надавати найважливішу інформацію про безпеку наших будинків, коли ви знаходитесь вдома або в офісі. IP-захищені камери безпеки та спостереження дуже важливі для забезпечення тісної, нерозбитної та непроникної безпеки. Системи виявлення та попередження вторгнення є іншими відомими модулями безпеки.

▪ *Системи опалення, кондиціонування повітря, системи вентиляції, освітлення та системи відтінків*: Комфорт стає вирішальним чинником у будинках нового покоління. Нові машини оснащуються інструментами, щоб забезпечити різні умови навколишнього середовища. Забезпечується зв'язок між різними домашніми пристроями, включаючи світлові вимикачі, настінні сенсорні панелі тощо. Роботи оснащуються різними варіаціями для здійснення

фізичних робіт для людей. Роботи, обладнані Cloud, будуть критично важливим для людей у той час, коли вони стануть розвинутими.

▪ *Обчислювальні та комунікаційні пристрої*. В даний час в домашніх умовах використовується широкий спектр обчислювальних машин, починаючи від персональних комп'ютерів (ПК), ноутбуків / ноутбуків / планшетів, маршрутизаторів Wi-Fi та шлюзів, носіїв та смартфонів..

▪ *Розваги, освіта та системи масової інформації*. Однією з найважливіших нововведень у медіа-технологіях та продуктах за останні роки. Сьогодні ми можемо похвалитися фіксованими, портативними, мобільними пристроями для повсякденного навчання. Телевізори, що підтримують IP, виробляються в масових обсягах, різко збільшуючи наш вибір, зручність та комфорт. Веб, інформаційні та побутові прилади є достатніми та новаторськими. Технології для соціальних сайтів (веб 2.0) знаходяться на підйомі, що сприяє підвищенню продуктивності праці для людей та формуванню цифрових спільнот для обміну знаннями в режимі реального часу. Для домашнього кінотеатру, музичних систем hi-fi, DVD-пристроїв, ігрових консолей тощо.

▪ *Домашня мережа*: всі пасивні, онімілі предмети перетворюються на цифрові об'єкти. Вони підключаються до бездротової та розумної мережі з усіма видами побутової електроніки, щоб обмінюватися та спілкуватися (безпосередньо [однорангові] або опосередковано, через посередницькі пристрої). Кожного для підключається все більше і більше користувачів, до національної мережі. Домашня мережа також може з'єднуватися із зовнішнім світом через всеохоплюючий Інтернет. Що дозволяє дистанційно спостерігати, управляти та обслуговувати домашні пристрої. Автомобільні мультимедіа, навігаційні та інформаційно-розважальні системи, системи керування паркуванням тощо, також підключаються до домашніх систем безпосередньо або через проміжне програмне забезпечення на базі коробки для взаємодії та взаємодії в реальному часі.

▪ *Домашній контроль доступу:* Е-замки з'являються як найважливіша заходи безпеки для домашнього контролю доступу.

▪ *Розслабляючі та об'єкти настрою:* крім об'єктів у певних місцях, таких як тренажерні зали, санаторії, санвузли, гаражі автомобілів, предмети домашнього ужитку, такі як електричні лампи, ліжечка, стільці, шафи, віконні панелі, дивани, бігові доріжки, столи, дивани, автостоянки тощо з'єднуються між собою, щоб значно покращити настрій, стан користувачів.

▪ *Системи охорони здоров'я*: медичні кабінети, пігулки та таблетки, гумоїдних роботів і так далі займають перші слоти, що гарантують здорове життя для мешканців житла.

▪ *Кухонна техніка, вироби та посуд*. Модульна кухня, що включає в себе всі види електроніки, виявляється ключовим фактором для розумніших будинків. Кавоварки, хлібні тостерів, електронні печі, холодильники, мийки для посуду, кухонні комбайни тощо покращуються, щоб бути розумнішими в домашніх умовах.

Інтернет-холодильник (Internet refrigerator або Smart refrigerator) - новий клас побутових холодильників, що з'явився на початку XXI століття. Як правило, він має вбудований комп'ютер з постійним підключенням до мережі інтернет і сенсорним екраном на фронтальній панелі (рис.2.3). Такий холодильник не тільки зберігає продукти, а й дає можливість користуватися інтернетом, через який можна отримати доступ до різних сайтів (наприклад, з кулінарними рецептами для приготування страв) і навіть замовляти продукти в інтернет-магазинах з доставкою додому. Крім того, за допомогою інтернет-холодильника можна спілкуватися, використовуючи електронну і відеопошту. Інтернет-холодильник може надавати цілий ряд сервісів: доступ в Інтернет, відеотелефон, e-mail, TV, MP3- музику, базу даних по кулінарних рецептах і правилах харчування, електронне перо, щоб залишити повідомлення, голосові послання. Ряд моделей інтернет-холодильників обладнані телевізійним і радіоприймачем. Крім того, при використанні інтернет-холодильника з'являється можливість вивести на екран картинку з веб-камери зовнішнього

відеоспостереження. Це дозволяє бачити те, що відбувається у дворі приватного будинку, навіть не покидаючи кухні, доглядати за своїм малюком, що знаходяться в дитячій кімнаті і т.д. Деякі пристрої даного типу також можуть стежити за вмістом холодильника, вибираючи оптимальні умови зберігання та заморозки продуктів. Крім цього, інтернет-холодильник відстежує продукти з терміном придатності. Інформація про все це надходить на смартфон користувача і останній, перебуваючи в магазині, може оцінити свої реальні потреби в продуктах.

Рис. 2.3 Приклад Інтернет-холодильнику

Робот-пилосос може діяти автономно, програмуватися і управлятися через Інтернет, для чого є ряд сенсорів і інфрачервона вбудована камера (рис. 2.4). Система управління роботою пилососа робить кілька знімків в секунду створюючи, таким чином, карту всього будинку або окремих його кімнат. Пристрій також має можливість запам'ятовувати оптимальний шлях збирання і визначати своє місцезнаходження в будинку. Акумулятора вистачає на певний час збирання (зазвичай до 1,5 годин), після закінчення якого робот сам відправляється на підзарядку. До пилососа є бездротовий доступ Wi-Fi за допомогою комп'ютера або смартфона. Через ці пристрої можна запустити його і в режимі реального часу спостерігати за тим, що відбувається в кімнаті. Більш того, можна поговорити з людьми, які знаходяться в будинку через

систему голосового зв'язку. Вбудований джерело світла дозволяє бачити в повній темряві і перевірити приміщення навіть вночі.

Рис. 2.4 Приклад робота-пилососа

Інтернет мікрохвильова піч має вбудований модем для виходу в інтернет, пам'ять для зберігання завантажувати інформацію і пульт управління. Вона виконує такі завдання:

- скачування рецептів з Інтернету і самопрограмування;
- зв'язок з компаніями - виробниками продуктів;
- дає доступ до системи замовлення продуктів по інтернету.

Інтернет-кондиціонер підключається до інтернету по дротову або бездротову мережу WiFi і дає користувачеві доступ до управління кондиціонером з будь-якої точки земної кулі. Власник може дистанційно вмикати і вимикати систему, програмувати настройки, вибір між режимами, температуру, швидкість вентилятора, задавати параметри, словом здійснювати будь-які маніпуляції, доступні зі звичайного пульта. Керувати таким кондиціонером можна з будь-якого пристрою (комп'ютер, ноутбук, планшет, смартфон), в якому встановлена спеціальна програма і який має вихід в інтернет.

Система по догляду за домашніми тваринами покликана забезпечити їм всі необхідні комфортні умови існування. Така система використовується в разі тривалої відсутності господарів будинку - це дозволяє не турбуватися про

добробут своїх домашніх улюбленців. Основними завданнями системи по догляду за домашніми тваринами є автоматична подача їжі і пиття, а в разі виникнення непередбачених обставин - інформування господарів про них (по телефону, за допомогою SMS або по електронній пошті). За бажанням можна скласти повний звіт про поведінку домашніх улюбленців під час відсутності господарів - скільки разів і коли їли, коли ходили в туалет, пили воду і т.д. Можна навіть супроводити цей звіт фотографіями (якщо встановлена камера спостереження) і передавати їх (по електронній пошті, за допомогою MMS) - словом, все, щоб господарі відчували себе комфортно і були впевнені в тому, що їх улюбленцям нічого не загрожує.

Отримані статистичні підрахунки та прогнози про те, що в вже з'являться сотні мікроконтролерів у будь-яких вдосконалених домашніх/офісних середовищах. Надзвичайно популярні технології, такі як картки, чіпи, наклейки, теги, інтелектуальні пил і т. д. дає початок потужному середовищу. Наші повсякденні місця будуть наповнені і насичені зростаючою кількістю об'єктів, що виробляють та споживають події, екологічний моніторинг та вимірювальні рішення, системи контролю, активації та оповіщення, інтеграційні тканини, автобуси та дисплеї візуалізації та інформаційні панелі, елементи мережевих та автоматичних пристроїв, десятки кишенькових комп'ютерів, портативних комп'ютерів, переносних приладів та ін., щоб зробити наше життя і місця приємним і придатним для життя[10].

2.2 Загрози «розумного дому»

Експерти наполегливо заявляють про те, що постачальники послуг і пристроїв ринку IoT порушують принцип наскрізної інформаційної безпеки (ІБ), який рекомендований для всіх ІКТ-продуктів і послуг. Згідно з цим принципом, ІБ повинна закладатися на початковій стадії проектування продукту або послуги і підтримуватися аж до завершення їх життєвого циклу.

Але що ж ми маємо на практиці? Ось, наприклад, деякі дані досліджень корпорації HP (літо 2014 роки), метою яких було не виявити якісь конкретні

небезпечні інтернет-пристрої і викрити їх виробників, але позначити проблему ІБ-ризиків в світі IoT в цілому.

Дослідники HPE звертають увагу на проблеми як на стороні власників пристроїв, так і на проблеми, над якими повинні подумати розробники. Так, на самому початку експлуатації користувачеві обов'язково потрібно замінити фабричний пароль, встановлений за замовчуванням, на свій особистий, оскільки фабричні паролі однакові на всіх пристроях і не відрізняються стійкістю. На жаль, роблять це далеко не всі. Оскільки не всі прилади мають вбудовані засоби ІБ-захисту, власникам також слід подбати про встановлення зовнішнього захисту, призначеної для домашнього використання, з тим щоб інтернет-пристрою не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди.

В ході проведеного HP дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротової трафік. Веб-інтрефейс 60% пристроїв експерти HP порахували небезпечним через небезпечну організацію доступу і високих ризиків міжсайтового скриптинга. У більшості пристроїв передбачені паролі недостатньою стійкості. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома.

Всього ж фахівці HP нарахували близько 25 різних вразливостей в кожному з досліджених пристроїв (телевізорів, дверних замків, побутових ваг, домашніх охоронних систем, електророзеток ...) і їх мобільних і хмарних компонентах.

Висновок експертів HP невтішний: безпечної екосистеми IoT на сьогоднішній день не існує. Особливу небезпеку речі Інтернету таять в собі в контексті поширення цільових атак (APT). Варто тільки зловмисникам проявити інтерес до будь-кого з нас, і наші вірні помічники зі світу IoT перетворюються в зрадників, нарозхрист відкривають доступ в світ своїх власників.

Рис. 2.5 Загрози «Розумного будинку»

Слабкі місця IoT:

- перехід на IPv6.
- живлення датчиків.
- стандартизація архітектури і протоколів, сертифікація пристроїв.
- інформаційна безпека.
- стандартні облікові записи від виробника, слабка аутентифікація
- відсутність підтримки з боку виробника для усунення вразливостей
- важко або неможливо оновити ПЗ і ОС

- використання текстових протоколів і непотрібних відкритих портів
- використовуючи слабкість одного гаджета, хакеру легко потрапити під всю мережу
- використання незахищених мобільних технологій
- використання незахищеною хмарної інфраструктури
- використання небезпечного ПЗ

Оскільки Інтернет речей продовжує інтегрувати, здавалося б, безглузді і незв'язані об'єкти, то повноцінна домашня операційна система виглядає цілком вірогідною. Хоча це перетворить Ваш будинок в оптимізований життєвий простір, повністю призначений для забезпечення Вашого комфорту, тим не менш, вона може також нести Вам серйозні ризики стати жертвою кібер-атаки в Вашому власному будинку.

Центральна ланка будь-якої системи безпеки розумного будинку майбутнього - це його замок. До речі, недавнє дослідження показало, що розумні замки лякаюче легко можна зламати, в результаті чого вони не можуть гарантувати виконання своєї основної функції, для якої, власне кажучи, вони й існують. Існуючі системи досить прості для кібер-хакерів і не є перешкодою для того, щоб проникнути в Ваш будинок. А що якщо далі хакери в майбутньому зможуть використовувати це технологічне досягнення проти Вас? Якщо розумний замок можна зламати, щоб його відкрити, можливо, хакери знайдуть спосіб, як повністю його закрити, щоб Ви не могли його відкрити. В цьому випадку в майбутньому можна буде досить тихо проникати в чужий будинок: хакер зможе контролювати всі події віддалено. Більш того, він зможе вимагати у своїх жертв який-небудь розумний викуп за те, щоб вони могли потрапити в свої власні будинки. До речі, це може бути ідеєю для сценарію якого-небудь страшного фільму (Зовсім один вдома), але це жахлива думка. Якщо всі Ваші пристрої безпеки взаємопов'язані, то кібер-злочинці потенційно могли б отримати доступ також до Вашої домашньої сигналізації і навіть ключів від Вашого автомобіля.

Задимлений екран - тривога про пожежу. Одна функція безпеки, яка вже вбудована в деякі доступні на ринку детектори диму, - це можливість, що дозволяє розумному будинку отримувати інформацію (і використовувати її в подальшій роботі) від інших смарт-пристроїв, що дозволяє системі реагувати відповідним чином в разі небезпеки. Ця функція впроваджена для безпеки користувача, дозволяючи домашній системі, яка виявила пожежу, наприклад, розблокувати всі двері в будинку, щоб допомогти вибратися з нього якомога швидше. Це відмінний приклад того, як виробники IoT-рішень працюють над прозорою інтеграцією і взаємодією смарт-пристроїв всередині розумного будинку. Однак є одне застереження: якщо ця технологія буде використовуватися кібер-злочинцями, то існує ймовірність створення небажаної ланцюгової реакції, яка в кінцевому підсумку може, навпаки, знизити рівень безпеки розумного будинку.

Ще один спосіб, коли хакер міг би потенційно здалеку нашкодити, - це створення хибної тривоги про пожежу, яка відправляється в пожежні служби. Хаотична сцена може виглядати у вигляді задимленого екрану, що також в результаті може зробити Вас легкою здобиччю для інших потенційно шкідливих кібер-атак.

Пилосос смерті. Згадаємо про фурор, який справив на всіх самовзривний смартфон, то не будемо дивуватися і тому, що IoT-пристрої все частіше ставлять нас в таке становище, яке надає хакерам доступ до потенційно вибухонебезпечним пристроїв!

Чи можна використовувати IoT-пристрої для кібер-атаки? Легко. Зловмисники, як правило, працюють на маси: наприклад, розподілені атаки на відмову в обслуговуванні (DDOS), коли тисячі електронних листів або запитів відправляються на якийсь сервер, щоб уповільнити його роботу або взагалі вивести його з ладу. В цьому випадку в майбутньому ми можемо зіткнутися з ситуаціями, коли хакери спробують «завалити» якомога більше машин в надії на те, що якась їх частина буде працювати неправильно, що призведе до тяжких наслідків. Взагалі-то, лякає така перспектива. Можливо, саме з цієї

причини урядові органи говорять про потенційні небезпеки Інтернету речей, пов'язаних з кібер-атаками.

Остерігайтеся холодильника. В мультсеріалі «Сімпсони» був епізод, коли Мардж нападає на домашню операційну систему з штучним інтелектом, яка готує їжу, але таємно планує «позбутися» від інших членів сім'ї. Звичайно, це кумедна пародія, але бентежить те, що нам буде потрібно всього кілька технологічних досягнень, щоб ці події вже перестали бути смішними, а опинилися жахливою дійсністю. Добре, припустимо, що Ваш холодильник поки не веде з Вами інтелектуальних бесід, і вже тим більше, не опрацьовує якісь вбивчі схеми щодо Вашої родини. Однак ще два роки тому ЦРУ відзначили загрозу з боку смарт-холодильників в розумних будинках. До чого б це? ЦРУ заметушилося від того, що холодильник використовувався як частина бот-мережі для виконання DDOS-атаки. І все це відбувалося зовсім непомітно для господаря цього холодильника, який навіть і гадки не мав про те, що його смарт-пристрій може виконувати якісь диявольські дії, крім як охолоджувати і зберігати їжу.

Що далі? Оскільки смарт-пристрої стають все розумнішими, відстежуючи Ваші купівельні переваги і здійснюючи замовлення на будинок, міг би хакер отримати доступ до Ваших банківських даних або втрутитися в Ваші покупки? Ми всі знаємо, що штучний інтелект і холодильники краще залишити як страшне бачення в мультиках, а не жах в реальному житті!

Сертифікація пристроїв IoT для захисту від хакерів. 11 жовтня 2016 року стало відомо про плани Єврокомісії - ввести обов'язкову сертифікацію або іншу аналогічну процедуру всіх приладів, що підключаються до інтернету речей. Передбачається вжити заходів на державному рівні, що повинно перешкодити хакерам використовувати інтернет речей для створення ботнетів. Як варіант, не виключається установка на пристрої мережі спеціальних уніфікованих чіпів, які убезпечать їх від атак хакерів. Ці заходи, на думку чиновників Єврокомісії, повинні підвищити рівень довіри до

інтернету речей в суспільстві і перешкодити хакерам створювати ботнети з підключається техніки.

«Заходи щодо захисту інтернету речей від хакерів слід приймати саме на державному рівні, оскільки в контролі потребують не тільки самі прилади, а й мережі, до яких вони підключені, а також хмарні сховища. Схема сертифікації інтернету речей можна порівняти з європейською системою маркування енергоспоживаючих товарів, прийнятої в 1992 році. Маркування є обов'язковою для автомобілів, побутової техніки та електричних ламп. Але виробники техніки вважають систему подібної маркування неефективною для захисту від хакерів. Замість цього вони вважали за краще б встановити в прилади стандартний чіп, який буде відповідати за безпеку підключення до інтернету.» - Тібо Клейнер (Thibault Kleiner), заступник європейського комісара з цифрової економіки та суспільству.

До групи приладів, що підключаються до інтернету, входять відеокамери, телевізори, принтери, холодильники та інша техніка. Велика частина цих пристроїв незадовільно захищена від хакерських атак. Самі по собі ці пристрої можуть не подавати інтересу для злочинців. Однак хакери зламують їх, щоб використовувати в якості роботів для створення ботнетів, за допомогою яких можна атакувати більш серйозні системи. Більшість власників зламаних пристроїв навіть не підозрюють, як використовується їхня техніка.

Як приклад наведена масштабна DDoS-атака на інтернет-ресурс Krebs On Security, в вересні 2016 року. «Інтенсивність запитів від ботнеті під час атаки досягла 700 Гб / с. У складі ботнету більш 1 млн камер, відорегістраторов та інших підключених до інтернету речей пристроїв. Це не перший резонансний випадок, коли подібні пристрої стають частиною ботнету, проте вперше мережа складалася майже повністю з таких приладів.» - Брайан Кребс (Brian Krebs), власник ресурсу.

За даними Gartner, до інтернету речей підключено близько 6 млрд приладів, а до 2020 року їх число досягне 20 млрд, що створить хакерам ширші можливості для проведення масштабних атак за допомогою ботнетів.

У споживачів немає впевненості в безпеці пристроїв IoT. Компанія Gemalto оприлюднила в жовтні 2017 року статистику: виявляється, 90% споживачів не довіряють безпеці пристроїв Інтернету речей. Ось чому понад дві третини споживачів і майже 80% організацій підтримали уряди, що беруть заходи щодо забезпечення безпеки IoT.

Основні побоювання споживачів (згідно двом третинам респондентів) стосуються хакерів, які можуть встановити контроль над їх пристроєм. Фактично, це викликає більше занепокоєння, ніж витік даних (60%) і доступ хакерів до особистої інформації (54%). Незважаючи на те, що пристроями IoT володіє більше половини (54%) споживачів (в середньому, по два пристрої на людину), тільки 14% вважають себе обізнаними про безпеку цих пристроїв. Така статистика показує, що як споживачам, так і підприємствам, необхідно додаткову освіту в даній сфері.

Що стосується рівня інвестицій в безпеку, то опитування показало, що виробники пристроїв IoT і постачальники послуг витрачають всього 11% свого загального IoT-бюджету на забезпечення безпеки пристроїв Інтернету речей. Дослідження показало, що ці компанії дійсно визнають важливість захисту пристроїв і даних, які вони генерують або передають, а 50% компаній забезпечують безпеку на основі проектного підходу. Дві третини (67%) організацій повідомляють про застосування шифрування в якості основного методу захисту активів IoT з 62%-вим шифруванням даних відразу після досягнення IoT-пристрої, а 59% - при виході з пристрою. Дев'яносто два відсотки компаній спостерігали збільшення продажів або використання продукту після впровадження заходів по забезпеченню безпеки IoT. Згідно з опитуванням, компанії підтримують положення, що дають зрозуміти, хто несе відповідальність за забезпечення безпеки пристроїв і даних IoT на кожному етапі їх застосування (61%) і які наслідки недотримання безпеки (55%). Фактично, майже кожна організація (96%) і кожен споживач (90%) відчувають необхідність в правилах щодо забезпечення безпеки Інтернету речей, прийнятих на рівні уряду.

Контроль над смарт-пристроями. Уразливість в мобільному і хмарному додатках LG SmartThinkQ дозволили дослідникам Check Point віддалено увійти в хмарний додаток SmartThinQ, і, заволодівши обліковим записом LG, отримати контроль над пилососом і вбудованої в нього відеокамерою. Отримавши контроль над обліковим записом конкретного користувача LG, зловмисник може контролювати будь-який пристрій LG або пристрій, пов'язаний з цим обліковим записом, включаючи пилососи, холодильники, плити, посудомийні і пральні машини, фени та кондиціонери, розповіли в компанії. Уразливість HomeHack дає хакерам можливість стежити за сімейним життям користувачів за допомогою відеокамери робота-пилососа Hom-Bot, яка в режимі реального часу надсилає відео в додаток LG SmartThinQ в рамках функції HomeGuard Security. Залежно від моделей пристроїв LG зловмисники можуть також включати і відключати посудомийні або пральні машини. Наразі таку уразливість усунено[15].

2.3 Атаки

Очевидно, що «розумний дім» знаходиться в небезпеці, оскільки, крім дротових загроз існують атаки по бездротових мережах і тому є більш уразливими, в наслідок використання відкритого середовища в якості носія даних і широкомовної природи бездротових з'єднань. Рис.2.5 ілюструє класифікацію атак, що можуть вразити, навіть, ваш пилосос.

Рис. 2.6 Класифікація атак

2.2.1 Пасивні атаки

Аналіз трафіку і прослуховування комунікаційного каналу неавторизованими особами класифікується як пасивна атака. Атаки, націлені виключно на отримання передаються даних є пасивними по своїй натурі. Найбільш частими є наступні види атак спрямовані на порушення конфіденційності даних:

Моніторинг і прослуховування. Даний вид атаки зустрічається найбільш часто. За допомогою підслуховування зловмисник може з легкістю отримати доступ до передається даними. При передачі контрольної інформації про конфігурацію мережі, дана техніка може становити найбільшу небезпеку для конфіденційності даних.

Аналіз трафіку. Навіть коли інформація передається в зашифрованому вигляді, залишається ймовірність використання зловмисником техніки аналізу комунікаційних патернів. Активність сенсорів потенційно може розкрити досить інформації для нанесення зловмисником шкоди сенсорної мережі.

2.2.2 Активні атаки

Різні модифікації даних під час комунікації, здійснювані неавторизованими особами, класифікуються як активні атаки. Нижче надаються описи активних атак.

Атаки маршрутизації

Атаки, які здійснюються на мережевому рівні (network layer) моделі OSI називаються атаками маршрутизації. Наступні атаки маршрутизації зустрічаються найбільш часто:

Змінена маршрутна інформація. Найбільш схильні до даної атаки децентралізовані мережі, де кожен вузол є маршрутизатором і відповідно може змінювати маршрутну інформацію. Внаслідок даної атаки можуть відбуватися закільцьовування маршруту, збільшуватися час пакета даних в шляху до точки призначення і т. д.

Вибіркова розсилка. Скомпрометований вузол сенсорної мережі може вибірково видаляти певні пакети. Особливо ефективною дана атака може бути

в комбінації з атаками, які збирають велику кількість трафіку на одному вузлі мережі. В результаті даної атаки серйозно страждає цілісність і доступність даних, що може істотно знизити рівень сервісу, що надається сенсорної мережею.

Атака «бездонна воронка» (Sinkhole Attack). Дана атака характерна тим, що скомпрометований вузол мережі починає діяти подібно воронці, використовуючи весь трафік сенсорної мережі. Особливо в мережах з протоколом маршрутизації, заснованому на широкомовній розсилці, зловмисник «слухає» запити на маршрути і відповідає сенсорним вузлам, що «знає» найкоротший маршрут до базової станції. Як тільки скомпрометованому вузлу вдалося встати між сенсорним вузлом, що транслює і базовою станцією, він може виробляти будь-які дії з пакетами даних, що надходять.

«Шаманська атака» (Sybil attack). Під час даної атаки один скомпрометований вузол може використовувати кілька псевдо ідентифікаторів, видаючи себе відразу за кілька вузлів. Подібні атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі і т. д. По суті будь-яка мережа з рівноправними вузлами (особливо бездротові і децентралізовані мережі) є схильною до даної атаки.

Атака (Wormhole attack). Дана атака передбачає створення спеціального шляху між двома і більше скомпрометованими вузлами сенсорної мережі для передачі по ним перехоплених пакетів, доступних тільки для атакуючої системи. Подібні атаки представляють серйозну загрозу безпеці сенсорної мережі тому, що не вимагають компрометації вузла сенсорної мережі. Тоді коли вузол B (базова станція або звичайний вузол) використовує широкомовну розсилку для запиту маршруту, зловмисник отримує даний запит і перенаправляє його до найближчого сусіда. Будь-який вузол, який отримав подібний перенаправлений запит розглядає себе як вузол, що знаходиться в зоні досяжності вузла B і запам'ятовує вузол B як свого «батька». Навіть якщо

цей вузол знаходиться на великій відстані від вузла В і його відокремлюють від вузла В безліч сенсорних вузлів, він буде розглядати вузол В як наступний від себе.

Флуд атака (HELLO flood attack). Дана атака є широкомовною атакою, покликаною направити в сенсорну мережу масу необов'язкових повідомлень, які повинні позбавити мережу різноманітних ресурсів - канальної ємності, обчислювальної потужності, енергетичних ресурсів і т.д. Під час подібної атаки зловмисник за допомогою високочастотного радіопередавача з достатньою обчислювальною потужністю розсилає Hello пакети до безлічі вузлів сенсорної мережі. Вузли, які отримали Hello пакети, розглядають скомпрометований вузол як свого сусіда. Під час наступної передачі даних, вони будуть використовувати отриманий адресу з Hello пакетів для відправки. Таким чином, зловмисник отримає доступ до даних.

Відмова в обслуговуванні

Даний вид атаки може бути результатом ненавмисного виходу з ладу вузлів сенсорної мережі або ж результатом дій зловмисників. Найпростіша атака такого роду спрямована на витрату всіх ресурсів, доступних скомпрометованому вузлу за допомогою відправки непотрібних пакетів даних, таким чином перешкоджаючи легітимним користувачам мережі отримувати призначені їм сервіси і ресурси. Дана атака має на увазі не тільки спроби зловмисника зруйнувати мережу або розірвати з'єднання, але і будь-яка подія, що знижує здатність мережі надавати певні послуги і ресурси. Безліч типів подібних атак може бути здійснено на різних рівнях моделі OSI.

Захоплення вузла (node subversion)

Захоплення вузла зловмисником може спричинити розкриття важливої інформації, наприклад, криптографічних ключів, що в свою чергу може спричинити компрометацію всієї сенсорної мережі.

Несправність вузла (malfunction)

Несправний в результаті атаки вузол генерує невірні дані, що може порушити цілісність сенсорної мережі, особливо, якщо несправний вузол є вузлом, що агрегує дані, наприклад, головним вузлом кластера.

Простій вузла / вихід з ладу

Простій вузла або його вихід з ладу трапляється тоді коли вузол перестає функціонувати. У разі виходу з ладу головного вузла кластера, протокол сенсорної мережі повинен бути здатний надати альтернативний маршрут для пакетів даних.

Фізичні атаки

Вузли мережі часто встановлюються в середовищах із зовнішніми впливами. В таких середовищах маленький впливаючий фактор вузлів сенсорної мережі в поєднанні з відсутністю постійного нагляду за ними робить їх схильними до різних фізичних атак. На відміну від інших видів атак, фізичні атаки руйнують сенсори незворотньо.

Спотворення повідомлення

Будь-яка зміна контенту повідомлення зловмисником неминуче компрометує цілісність передаються даних.

Хибний вузол

Даний вид атак передбачає впровадження в мережу вузла, який посилає вузлів сенсорної мережі некоректні дані. Дана атака є однією з найбільш небезпечних атак, оскільки запроваджений вузол, який поширює зловмисний код, може привести до загибелі всю сенсорну мережу.

Копіювання вузла мережі

Концептуально дана атака полягає в наступному: зловмисник намагається впровадити заздалегідь підготовлені вузли в існуючу сенсорну мережу, використовуючи ідентифікатори вже існуючих вузлів в даній мережі. Для цього зловмисник фізично захоплює один вузол мережі з метою отримання його унікальних даних. Отримані дані згодом використовуються для конфігурації заздалегідь підготовлених вузлів, які згодом стають клонами

захопленого вузла. За допомогою впровадження реплікованих вузлів в певні точки мережевий топології зловмисник може з легкістю управляти сегментом мережі[16].

Висновок: Оскільки, загроза очікує Вас, навіть, в буденних речах, а хакери можуть проникнути у ваш холодильник, тож кожна ланка Вашої системи потребує захисту. Маючи дані про можливі загрози та атаки, необхідно створити методику, певний алгоритм згідно з яким можна захистити не тільки домашню мережу, а і мережу на підприємстві.

РОЗДІЛ 3. МЕТОДИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІОТ

Більшість пристроїв IoT виглядаються, як «закриті системи». Покупці не зможуть додавати/змінювати програмне забезпечення безпеки після того, як пристрої покинуть завод. Таке втручання анулює гарантію, а часто просто неможливо. З цієї причини, захисні функції повинні бути спочатку вбудовані в пристрої IoT, щоб вони були безпечними за своєю архітектурою. Для більшої частини індустрії ІБ така «безпека всередині», тобто вбудована при виготовленні пристрою на заводі - це новий спосіб забезпечення захисту, це стосується і класичних технологій безпеки, таких як шифрування, перевірка справжності, перевірка цілісності, запобігання вторгнень і можливості безпечного оновлення. З огляду на тісний зв'язок апаратного і програмного забезпечення в моделі IoT, іноді простіше, щоб програми для захисту використовували розширення функцій апаратної частини і створювали «зовнішні» рівні безпеки. Добре, що багато виробників чіпів вже вбудували функції безпеки в обладнання. Але апаратний рівень - це всього лише перший шар, необхідний для комплексного захисту зв'язку і пристроїв. Комплексний захист вимагає інтеграції функцій управління ключами, захисту на основі хоста, інфраструктури і аналітики безпеки. Відсутність навіть одного з наріжних каменів у фундаменті безпеки залишить широкий простір діям зловмисників. Оскільки промисловий інтернет і IoT привносять мережевий інтелект в фізичні речі навколо нас, ми повинні уважно ставитися до питань їх безпеки. Наше життя залежить від літаків, поїздів і автомобілів, які перевозять нас, від інфраструктури охорони здоров'я та цивільної інфраструктури, яка дозволяє нам жити і працювати. Неважко уявити, як незаконне маніпулювання світлофорами, медичним обладнанням або незліченними іншими пристроями може привести до плачевних наслідків. Також ясно, що прості громадяни і покупці IoT не хочуть, щоб незнайомі люди зламували їх будинку або машини, щоб хтось робив їм шкоду, влаштовуючи збої на автоматизованих промислових об'єктах. У цій ситуації необхідно скласти методику, алгоритм

дій, які сформують цілісну безпеку для IoT, одночасно зробивши її ефективної і простий в реалізації.

3.1 Безпека зв'язку. Посилена модель довіри для IoT.

Шифрування, перевірка справжності і керованість незмінно є основою стійкої безпеки. Є відмінні бібліотеки з відкритим вихідним кодом, які виконують шифрування навіть в пристроях IoT з обмеженими обчислювальними ресурсами. Але, на жаль, більшість компаній як і раніше піддаються небезпечним ризикам, допускаючи помилки при управлінні ключами для IoT. Транзакції на 4 млрд доларів в день електронної торгівлі захищені простою і надійною моделлю довіри, яка обслуговує мільярди користувачів і понад мільйон компаній по всьому світу. Ця модель довіри допомагає системам безпечно проводити перевірку достовірності систем інших компаній і взаємодіяти з ними по зашифрованих каналах зв'язку. Модель довіри сьогодні є критичним фактором безпечного взаємодії в комп'ютерних середовищах і ґрунтується на дуже короткому списку довірених центрів сертифікації (CA). Ці ж CA встановлюють сертифікати в мільярди пристроїв щороку. Сертифікати пристроїв дозволяють, наприклад, перевіряти справжність мобільних телефонів для безпечного підключення до базових станцій, перевіряти справжність інтелектуальних лічильників для електроенергетики, а також приставок в індустрії кабельного телебачення. Надійні CA дозволяють легко і безпечно генерувати, видавати, реєструвати, контролювати і відкликати сертифікати, ключі та облікові дані, які мають вирішальне значення для надійної перевірки справжності даних. З огляду на реалізовані обсяги сертифікатів безпеки для IoT, більшість сертифікатів пристроїв продаються великими партіями за вельми скромну суму грошей за одиницю (в доларовому вираженні йдеться про десятки центів за сертифікат).

Безпека не може розглядатися як додаток до пристрою, а скоріше як невід'ємна частина надійного функціонування пристрою. Контроль безпеки програмного забезпечення необхідно ввести на рівні операційної системи, скористатися перевагами апаратних засобів безпеки, які зараз надходять на

ринок, і розширювати їх через стек пристрою, щоб постійно підтримувати надійну обчислювальну базу. Забезпечення безпеки на рівні ОС примушує розробників та розробників пристроїв встановлювати системи для пом'якшення загроз та забезпечення безпечності своїх платформ.

Коли пристрій підключено до мережі, він повинен аутентифікувати себе перед отриманням або передачею даних. Глибоко вбудовані пристрої часто не мають користувачів, що сидять за клавіатурами, очікуючи на введення облікових даних, необхідних для доступу до мережі. Як же ці пристрої правильно ідентифікувати до авторизації? Так само, як аутентифікація користувача дозволяє користувачеві отримати доступ до корпоративної мережі на основі імені користувача та пароля, аутентифікація пристрою дозволяє пристрою отримувати доступ до мережі на основі аналогічного набору облікових даних, що зберігаються в безпечній зоні зберігання[20].

Чому перевірка справжності має значення? Небезпечно приймати дані від неперевірених пристроїв або неперевірених сервісів. Такі дані можуть пошкодити або скомпрометувати систему, передати контроль над обладнанням зловмисникам. Використання надійної перевірки справжності для обмеження небажаних підключень допомагає вберегти системи IoT від подібних небезпек і зберегти контроль над вашими пристроями і сервісами. Незалежно від того, чи з'єднується пристрій з якимось іншим пристроєм або відбувається обмін даними з віддаленим сервісом, наприклад, хмарним, зв'язок завжди повинна бути захищений. Всі взаємодії вимагають надійної перевірки справжності і взаємної довіри. Виходячи з цих міркувань, економія на сертифікатах пристроїв видається спірною. На щастя, безліч стандартів було розроблено для спрощення споживачам розгортання надійної перевірки справжності всіх ланок ланцюга обміну даними. Стандарти існують для форматів сертифікатів, і надійні центри сертифікації підтримують як стандартні, так і кастомні формати. У більшості випадків сертифікатами можна легко керувати віддалено за допомогою стандартних протоколів, таких як Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure

Transport (EST) і Online Certificate Status Protocol (OCSP). Завдяки надійному центру сертифікації, який надає можливість обробляти сертифікати, ключі та облікові дані, фактичну перевірку справжності можна робити за допомогою потужних стандартів Transport Layer Security (TLS) і Datagram TLS (DTLS) - родинних SSL.

Взаємна перевірка справжності, коли обидві кінцеві точки перевіряють один одного, має вирішальне значення для якісного захисту систем IoT. В якості додаткового бонусу, одного разу виконавши перевірку достовірності за TLS або DTLS, дві кінцеві точки можуть обмінюватися ключами шифрування або отримувати їх для обміну даними, які неможливо розшифрувати підслуховуючим пристроям. Для багатьох додатків IoT потрібно абсолютна конфіденційність даних, це вимога легко виконується використанням сертифікатів і протоколів TLS / DTLS. Однак коли конфіденційність не є обов'язковою вимогою, справжність переданих даних може перевірятися будь-якою стороною, якщо вони були підписані під час їх появи на датчику - такий підхід не обтяжує канал шифруванням, що переважно в архітектурі multi-hop.

Часто виникають питання щодо вартості та продуктивності чіпів IoT для криптографічних операцій. Тут потрібно взяти до уваги, що Elliptic Curve Cryptography (ECC) в 10 разів швидше і ефективніше, ніж традиційне шифрування навіть в обмежених обчислювальними ресурсами пристроях. Така швидкість і ефективність досягається без зниження рівня безпеки. ECC навіть продемонстрував рівень захисту industry best practice, еквівалентний RSA 2048, в тому числі на надзвичайно обмежених в ресурсах чіпах - на 8-bit 1-MHz процесорах і 32-bit 1-KHz процесорах, при споживанні лише мікроват енергії. DTLS, варіант TLS був розроблений спеціально для малопотужних пристроїв, які періодично працюють між циклами сну. І нарешті, ціна таких 32-розрядних чіпів становить всього кілька десятків центів (при розрахунку в доларах), тому ціну або потужність чіпів не вийде використовувати в якості аргументу для зниження вимог щодо захисту нижче розумних порогових значень, коли безпека має значення.

Сьогодні ми не можемо уявити собі таку незручність, як ручну установку сертифікатів в наші браузери для кожного веб-сервера, в той же час, ми не можемо уявити собі, який це буде шкодити, якщо сліпо вірити будь-якому сертифікату. Ось чому кожен браузер має кілька коренів довіри, за якими верифікуються всі сертифікати. Вбудовування цих коренів в браузери дало можливість масштабувати захист на мільйони серверів в Інтернеті. Оскільки мільярди пристроїв стають онлайн щорічно, в рівній мірі важливо, щоб в пристрої вбудовувалися і коріння довіри, і сертифікат пристрою. Дані, пов'язані з IoT, повинні зберігатися в безпеці весь час. Наше життя часто залежить від правильності, цілісності і належного функціонування цих систем більше, ніж від конфіденційності даних. Перевірка справжності інформації, пристроїв і походження інформації можуть мати вирішальне значення. Дані часто зберігаються, кешуються і обробляються декількома вузлами, а не просто передаються з точки А в точку Б. З цих причин дані завжди повинні бути підписані в той момент, коли вони були вперше зафіксовані і збережені. Це допомагає знизити ризики будь-якого втручання в інформацію. Підписання об'єктів даних, як тільки вони були зафіксовані, і ретрансляція підписи з даними навіть після їх дешифрування є все більш поширеною і успішною практикою.

Отже, спочатку введено в дію пристрій, справжність та цілісність програмного забезпечення котрих перевіряється на пристрої за допомогою криптографічних цифрових підписів. У значній мірі так само, як людина підписує чек або правовий документ, цифровий підпис, прикріплений до зображення програмного забезпечення та перевіряється пристроєм, гарантує, що тільки програмне забезпечення, яке було дозволено запускати на цьому пристрої, і підписане суб'єктом, який авторизований, буде завантажений. Створено фундамент довіри, але пристрій все ще потребує захисту від різноманітних загроз і зловмисних намірів.

3.2 Захист пристроїв. Захист програмного коду IoT.

При включенні кожен пристрій завантажується і запускає певний виконуваний код. Нам вкрай важливо бути впевненими в тому, що пристрої будуть робити тільки те, на що ми їх запрограмували, а сторонні не зможуть перепрограмувати на зловмисну поведінку. Тобто першим кроком у захисті пристроїв є захист коду, щоб гарантовано завантажувався і запускався тільки потрібний нам код. На щастя, багато виробників вже вбудували можливості безпечного завантаження в свої чіпи. Схожим чином справи йдуть і з високорівневим кодом - різні перевірені часом клієнтські бібліотеки з відкритим вихідним кодом, на кшталт OpenSSL, можуть використовуватися для перевірки підпису і дозволу коду тільки з авторизованого джерела. Внаслідок цього все більшого поширення набувають підписані прошивки, образи завантаження і більш високорівневий вбудований код, в тому числі підписані базові програмні компоненти, куди входять будь-які операційні системи. Все частіше зустрічаються не просто підписані прикладні програми, а взагалі весь код на пристрої. Такий підхід гарантує, що всі критичні компоненти систем IoT: датчики, механізми, контролери та реле сконфігуровані правильно - на запуск тільки підписаного коду і ніколи не запустять непідписаний код.

Доброю манерою було б дотримуватися принципу «ніколи не довіряти не підписаним коду». Логічним продовженням було б «ніколи не довіряти не підписаним даними і, тим більше, не підписаним конфігураційним даними». Використання сучасних засобів перевірки підпису і поширення апаратної реалізації безпечного завантаження, ставлять серйозне завдання перед багатьма компаніями - управління ключами і контроль доступу до ключів для підпису коду і захисту програмно-апаратних засобів. На щастя, деякі центри сертифікації пропонують хмарні сервіси, які роблять простіше, безпечніше і надійніше адміністрування програм для підписування коду і гарантують суворий контроль, хто може підписувати код, відкликати підписи, і як ключі для підписання і відкликання захищені. Виникають ситуації, коли програмне

забезпечення потрібно оновити, наприклад, в цілях безпеки, але при цьому необхідно врахувати вплив оновлень на заряд батареї. Операції перезапису даних збільшують споживання енергії і скорочують період автономної роботи пристрою.

З'являється необхідність підписати і оновити окремі блоки або фрагменти таких оновлень, а не монолітні образи цілком або бінарні файли. Тоді програмне забезпечення, підписана на рівні блоків або фрагментів, можна оновлювати з набагато більш тонкої деталізацією, не жертвуючи безпекою або зарядом батареї. Для цього не потрібна обов'язково апаратна підтримка, таку гнучкість можна досягти від передзавантажувального середовища, яке може працювати на безлічі вбудованих пристроїв.

Якщо час автономної роботи настільки важливий, чому б просто не конфігурувати пристрій з незмінної прошивкою, яку ніхто не може змінити або оновити? На жаль, необхідно припустити, що пристрої в польових умовах схильні до зворотної розробки для шкідливих цілей. Після цього виявляються і експлуатуються уразливості, які необхідно виявляти і позбуватися якомога швидше. «Заплутування» і шифрування коду можуть істотно уповільнити процес зворотної розробки та відбити охоту продовжувати атакувати у більшості зловмисників. Але ворожі спецслужби або міжнаціональні деструктивні організації все-таки здатні це зробити навіть для програм, захищених за допомогою «заплутування» і шифрування, перш за все тому, код повинен бути дешифрований для запуску. Такі організації знайдуть і скористаються уразливими місцями, які не були вчасно поміченими. У зв'язку з цим можливості віддаленого оновлення мають вирішальне значення і повинні бути вбудовані в пристрої до того, як вони покинуть завод[17].

3.3 Захист пристроїв. Ефективний хостовий захист для IoT

Для пристрою також потрібен брандмауер або функція глибокої перевірки пакетів для керування трафіком, призначеним для припинення роботи пристрою. Чому потрібен брандмауер на основі хоста або IPS, якщо на мережних пристроях є місце? Глибоко вбудовані пристрої мають унікальні

протоколи, відмінні від корпоративних IT-протоколів. Наприклад, сітка інтелектуальної енергії має свій набір протоколів, що визначають, як пристрої спілкуються один з одним. Саме тому для виявлення шкідливих платіжних навантажень, що ховаються в протоколах, не пов'язаних із IT, необхідні фільтри для протоколів та глибокі можливості перевірки пакетів. Пристрій не має займатися фільтрацією загальнодоступного Інтернет-трафіку на вищому рівні - мережеві пристрої повинні про це піклуватися, але для цього необхідно фільтрувати конкретні дані, призначені для завершення роботи на цьому пристрої, таким чином, щоб оптимально використовувати обмежені обчислювальні ресурси[20].

IoT-пристрої стикаються з багатьма загрозами, в тому числі шкідливим кодом, який може поширюватися через перевірені з'єднання, скориставшись уразливими або помилками в конфігурації. В таких атаках часто експлуатуються кілька слабких місць, включаючи, але не обмежуючись: невикористання перевірки підпису коду і безпечного завантаження; погано реалізовані моделі перевірки, які можна обійти. Атакуючі часто використовують ці недоліки для установки програмного забезпечення для збору даних, можливості передачі файлів для витягання конфіденційної інформації з системи, а іноді навіть для інфраструктури command & control (C & C) для маніпулювання поведінкою системи. Особливо тривожить здатність деяких зловмисників експлуатувати вразливості для установки шкідливих програм прямо в пам'ять вже працюють систем IoT. Причому іноді вибирається такий спосіб зараження, при якому шкідлива програма зникає після перезавантаження пристрою, але встигає наносити величезної шкоди. Це працює, тому що деякі системи IoT і багато промислових системи майже ніколи не перезавантажуються. Для відділу безпеки в цьому випадку ускладнюється можливість виявлення використаної уразливості в системі і розслідування походження атаки. Іноді такі атаки відбуваються через IT-мережу, підключену до промислової мережі або до мережі IoT, в інших випадках атака відбувається через інтернет або через прямий фізичний доступ

до пристрою. Як ви розумієте, не важливо, який був вихідний вектор інфекції, але якщо він не виявлений, то перше скомпрометований пристрій як і раніше залишається довіреною і стає провідником для зараження іншої мережі, будь то автомобільна мережа транспортного засобу або ціла виробнича мережа заводу. Таким чином, безпека IoT повинна бути комплексною. Закриваючи вікна, залишати двері відчиненими - неприйнятно. Всі вектори загроз повинні придушуватися.

На щастя, в поєднанні з надійним підписом коду і моделлю перевірки, хостовий захист може допомогти захистити пристрій від безлічі небезпек. У хостового захисту використовується ряд технологій захисту, в тому числі розмежування доступу до системних ресурсів, пісочниця, захист на основі репутації і поведінки, захист від шкідливих програм і, нарешті, шифрування. Залежно від потреб конкретної системи IoT комбінація цих технологій може забезпечити найвищий рівень захисту для кожного пристрою. Розмежування доступу до ресурсів і пісочниця захистять всі «двері» в систему. Вони обмежують мережеві підключення до додатків і регламентують вхідний і вихідний потік трафіку, захищають від різних експлойтів, переповнення буфера, цілеспрямованих атак, регулюють поведінку додатків, при цьому дозволяють зберегти контроль над пристроєм. Такі рішення ще можуть використовуватися для запобігання несанкціонованого використання знімних носіїв, блокування конфігурації та налаштувань пристрою і навіть для зменшення користувальницьких привілеїв, якщо потрібно. Хостовий захист має можливості аудиту і оповіщення, допомагаючи відстежувати журнали і події безпеки. Технології на основі політик можуть працювати навіть в середовищах без підключення до інформаційної мережі або при обмеженій обчислювальної потужності, необхідної для використання традиційних технологій. Технологія захисту на основі репутації може використовуватися для визначення сутності файлів по їхньому віку, поширеності, розташування і до решти для виявлення небезпек, що не виявляються іншими засобами, а також давати уявлення про те, чи слід довіряти новому пристрою навіть при

успішній перевірці справжності. Таким способом можна ідентифікувати загрози, які використовують мутуючий код або адаптують свою схему шифрування, просто відокремлюючи файли з високим ризиком від безпечних, швидко і точно виявляючи шкідливі програми, незважаючи на всі їхні хитрощі. Зрозуміло, поєднання застосовуваних технологій буде залежати від конкретної ситуації, але наведені вище засоби можуть об'єднуватися для захисту пристроїв, навіть в середовищах з обмеженими обчислювальними ресурсами.

3.4 Контроль пристроїв. Безпечне та ефективне управління IoT

Зворотну розробку пристроїв рано чи пізно буде проведено, уразливості будуть виявлені, а для пристроїв необхідно буде надавати оновлення(віддалено). Звичайно, механізми оновлення додають складність архітектурі пристроїв IoT, тому багато інженерів намагаються уникати їх на свій страх і ризик. На щастя, хороший механізм OTA(оновлення по повітрю) може використовуватися для багатьох цілей, не тільки для виправлень програмного забезпечення і функціональних оновлень, але також:

- Оновлення конфігурації
- Управління телеметрією безпеки для аналітики захищеності
- Управління телеметрією для контролю правильності функціонування пристрою
- Діагностики та відновлення
- Управління обліковими даними доступу до мережі (NAC)
- Управління правами / привілеями і безлічі інших завдань

Звичайно, все перераховане вище має виконуватися безпечно і надійно, тут необхідний більш ретельний підхід до підписання коду і організації передачі файлів. Деякі з рішень масштабуються для управління мільярдами пристроїв. Управління безпекою кожного пристрою може припускати управління конфігурацією за допомогою хостовой захисту. Також існують технології безпеки, засновані на політиках, яким оновлення потрібні тільки при перевстановленні на пристрої програмного забезпечення для якихось

цілей, наприклад, для додавання функціональних можливостей. Проте обидва типи технологій можуть генерувати телеметрію безпеки, яка має велике значення при зіткненні з цілеспрямованими атаками. Тому телеметричні дані безпеки завжди повинні збиратися від цих host-based (device-based) технологій для централізованого аналізу. Зрозуміло, компоненти безпеки не єдині в пристрої IoT, якими необхідно управляти безпечно і надійно.

Більшість пристроїв генерують телеметрію або дані з датчиків, які потрібно також безпечно і надійно збирати і передавати в місця зберігання та аналізу. Багато пристроїв вже містять в собі функції контролю, якими потрібно акуратно управляти через конфігураційні параметри, а ті в свою чергу безпечно і надійно зберігати і оновлювати. На щастя, інфраструктури управління пристроями, які використовують загальноприйняті безпечні протоколи, можуть застосовуватися і для захищеного управління основними функціями пристрою, контентом безпеки і телеметрії пристрою. Фактично подібні моделі адаптуються для OTA-керування автомобілями і використовуються для управління торговими автоматами. Деякі з інфраструктур управління комбінують агентські та без агентські протоколи управління IoT, тоді як пристрої випускаються з підтримкою стандартизованого управління для спрощення функцій контролю. А окремі інфраструктури управління можуть додатково поєднувати всі ці методи управління з розумінням інформації, отриманої від мережевих аналізаторів трафіку. У ситуації, що склалася системи IoT повинні спочатку мати вбудовані можливості оновлення OTA.

Відсутність цих можливостей залишить пристрої схильними до впливу загроз і вразливостей протягом всього терміну їх служби. Зрозуміло, оновлення OTA може застосовуватися ще для управління конфігураціями пристроїв, контентом безпеки, обліковими даними, а також для розширення функціональних можливостей пристроїв, збору телеметрії і даних програмного оточення, для доставки латки безпеки і багато чого іншого. Однак з додатковою функціональністю або без неї базові можливості

оновлення і управління захищеністю повинні бути передбачені ще на етапі проектування пристроїв IoT.

Застосовуються різні форми керування ресурсами та доступом. Обов'язкові або рольові елементи керування доступом, вбудовані в операційну систему, обмежують привілеї компонентів пристрою та програм, а отже, вони отримують доступ лише до ресурсів, які їм потрібні для виконання своїх завдань. Якщо який-небудь компонент скомпрометовано, контроль доступу гарантує, що вторгнення має як мінімальний доступ до інших частин системи, наскільки це можливо. Механізми контролю доступу на базі пристроїв аналогічні мережевим системам контролю доступу, таких як Microsoft® Active Directory®: навіть якщо хтось зможе вкрасти корпоративні облікові дані для отримання доступу до мережі, скомпрометована інформація буде обмежуватися лише такими областями мережі, що авторизована цими особливими повноваженнями. Принцип мінімальних привілеїв передбачає, що мінімальний доступ, необхідний для виконання функції, повинен бути дозволений, щоб мінімізувати ефективність будь-якого порушення безпеки[20].

3.5 Аналітика безпеки як реакція на погрози за рамками контрзаходів

Незалежно від того, наскільки добре ви захистили пристрій, код, зв'язок, і не має значення, наскільки добре ви керуєте безпекою, навіть застосовуючи кращу з можливих інфраструктур управління OTA, в розпорядженні деяких зловмисників цілком достатньо ресурсів і можливостей для подолання захисту. Таким чином, стратегічні загрози вимагають стратегічних технологій для мінімізації негативних наслідків. Аналітика безпеки може використовувати телеметрію безпеки з пристроїв і мережевого обладнання, щоб давати чітке уявлення про те, що відбувається в обчислювальному середовищі, включаючи виявлення прихованих загроз. Ці ж дані використовуються в аналітичних системах в рамках вирішення завдань оптимізації роботи систем IoT.

Не менш важливо, що моніторинг і аналітика часто можуть бути розгорнуті в якості тимчасового рішення в середовищах, де розгортання інших засобів захисту займе кілька років. Давайте розглянемо приклади. Legacy-прилади(устарілі) в промислових системах управління (виробництво, нафта і газ, комунальні послуги) не можна модифікувати до заміни системи цілком. Автоматизовані автомобілі, чиї мікроконтролери глибоко вбудовані, вже знаходяться на дорозі, і очевидно, їх не можна просто демонтувати і замінити на нові. У середовищі охорони здоров'я виробники зовсім забороняють лікарням модифікувати обладнання для додавання захисних функцій. У таких випадках рішення для виявлення аномалій можуть бути надзвичайно корисними. Багато мереж IoT характеризуються чітко визначеними шаблонами поведінки, а відхилення в таких системах легко ідентифікуються. Широка різноманітність промислових протоколів IoT ускладнює ситуацію, але нові технічні рішення, які використовують просунуте машинне навчання, успішно вирішують аналітичні завдання. З огляду на те, що багато систем IoT висувають високі вимоги до доступності, засоби захисту в пасивному режимі «виявлення» будуть вести себе менш агресивно, ніж в активному режимі «запобігання», так як помилкові спрацьовування не впливатимуть на роботу системи IoT.

Іншим варіантом захисту є шлюзи, наприклад, між застарілими і більш сучасними захищеними середовищами, оскільки атака в одній частині оточення може передаватися по всій мережі, якщо її не зупинити раніше. Однонаправлені шлюзи / діоди даних використовуються для гарантовано односпрямованої передачі між відкритими мережами і мережами з обмеженим доступом. Настільки ж високопріоритетними об'єктами розподіленого моніторингу та централізованої аналітики є шлюзи між промисловими і загальними IT-мережами, між головним блоком транспортного засобу та сотовою мережею, між автомобільною системою приводу і інформаційно-розважальними системами.

У більшості випадків замовники можуть співпрацювати з компаніями, які спеціалізуються на захисті інформації, для використання їх існуючої інфраструктури big data аналітики безпеки і великомасштабних систем збору подій безпеки по всьому світу для того, щоб отримувати, аналізувати і обмінюватися інформацією про всілякі мережі і екосистеми. Досить активно така діяльність ведеться в різних галузях, в першу чергу в сфері роздрібної торгівлі і критичної інфраструктури, так як це дає гарантії швидкого оновлення системи цілком для захисту від будь-яких виникаючих загроз[18].

Коли пристрій увімкнеться, він почне отримувати гарячі виправлення та оновлення програмного забезпечення. Операторам потрібно згорнути патчі, а пристрої повинні аутентифікувати їх таким чином, щоб вони не споживали пропускну здатність або погіршували функціональну безпеку пристрою. Це одна річ, коли корпорація Майкрософт надсилає оновлення користувачам Windows® і встановлює зв'язки між ними на 15 хвилин. Це зовсім інше, коли тисячі пристроїв у цій галузі виконують критичні функції або служби та залежать від патчів безпеки, які захищають від неминучої вразливості. Оновлення програмного забезпечення та патчі безпеки повинні доставлятися таким чином, щоб зберігати обмежену смугу пропускання та переривчасте підключення вбудованого пристрою, і абсолютно усуває можливість погіршення функціональної безпеки[20].

Найчастіше експертні знання в області безпеки, необхідні в аналітиці для виявлення складних загроз, можуть виходити за рамки можливостей компаній, які не спеціалізуються в області IT та ІБ. З цих причин багато організацій звертаються до аутсорсингу, щоб можна було покластися на експертів, що виконують моніторинг і аналітику. У деяких випадках компанії будують свої власні сховища телеметрії безпеки IoT і надають доступ до цього сховища декільком партнерам по аналітиці для спільного пошуку цілеспрямованих атак. Деякі аналітичні продукти і платформи надають API і SDK для забезпечення спільного доступу, безпечної взаємодії та обміну даними,

наприклад, можна надавати права заданому списку партнерів до певних даних і обмежувати доступ для інших.

У прикладі з об'єднаними промисловими і IT-мережами рекомендується створити єдину площину даних, що охоплює обидві середовища, для отримання в пріоритетному порядку подання про різні погрози та мінімізації ризиків проникнення загроз з одного середовища в іншу. Такі рішення повинні працювати з різними виробниками, всілякими пристроями та протоколами, щоб клієнти отримували цілісне уявлення, без сліпих зон про свою мережі. Принцип «виявлення і реагування» може доповнювати технології посиленого захисту для відображення переважної більшості атак, а також для мінімізації ризиків збитку від найбільш грізних супротивників.

3.6 Контроль взаємодій в мережі

Сьогодні незліченні технології та системи IoT вдають із себе не більше ніж «інтернет речей». Однак оскільки все більше систем повинні будуть зв'язуватися один з одним, все важливішим стає знати, «чому довіряти». Сертифікати пристроїв можуть містити інформацію про походження і тип пристрою. Проте на питання про те, чи потрібно довіряти цьому пристрою, в кінцевому підсумку повинні будуть відповідати інші служби, наприклад, засновані на репутації, або «Довідник речей» (Directory of Things). Такий каталог здатний не тільки відслідковувати інформацію про безпеку для кожного пристрою і систем IoT, але ще відстежувати і керувати привілеями, і повноваженнями, якими пристрої та системи наділяють один одного. Фактично кожен з нас виявляється оточеним все великою кількістю пристроїв IoT, а такі довідники можуть допомогти розібратися з пристроями з важливими функціями в областях, що цікавлять. Модель довідника робить можливим швидкий пошук віддаленого пристрою через каталог і, можливо, буде сприяти прискоренню прийняття рішення про використання даних з чужого пристрою. Навіть, якщо ви ніколи не бачили пристрій раніше, інформація про пристрій, включаючи його можливості і репутацію, можуть бути вказані в такому каталозі. Якщо припустити, що пристрій захоче

дізнатися, чи може він довіряти користувачеві, то «Довідника речей», можливо, буде недостатньо, і в цьому випадку скоріше буде потрібно «Довідник всього» (Directory of Everything), який буде включати пристрої, системи та користувачів.

Звичайно, у багатьох людей немає розумних чайників або розумних холодильників, проте це поки що. Але у багатьох з нас вже є автомобіль, який отримує інформацію для навігатора через інтернет, Smart TV або програвачі Blu-ray, які транслюють відео через інтернет, фітнес браслети, а ще ми використовуємо банкомати та вендингові апарати. Наша взаємодія з IoT насправді частіше, ніж здається. У цій ситуації користувач, ймовірно, захоче мати власний «Довідник речей». Захищаючи пристрій і зв'язок, керуючи програмними оновленнями і виконуючи аналітику безпеки для стратегічної захисту від загроз, зрозуміло, що всі ці заходи абсолютно необхідні для захисту IoT. Концепція каталогів «чому довіряти» вельми перспективна, але не є сьогодні ні основоположною технологією, ні ключовим інгредієнтом в «контролі взаємодій в мережі» для більшості учасників. Ця перспективна концепція каталогів стоїть вже перед багатьма компаніями, як виклик, і складне масштабне завдання. Це є актуальна проблема для деяких компаній, оскільки вони несуть відповідальність за захист більш ніж мільярда пристроїв. Для них це «майбутнє» вже настало, і вони не самотні.

3.7 Необхідність комплексної безпеки IoT

Розглянемо приклад, котрий доведе, що ніяким з позначених раніше наріжних каменів можна нехтувати - розглянемо поїзд. У поїздах контролери електродвигунів часто контролюють не тільки прискорення, але ще і рекуперативного гальмування. Якщо в якості страховки від неконтрольованого прискорення можна підключити механічні гальма, то від екстреного гальмування такого механічного захисту немає. Можуть постраждати люди, не кажучи вже про потяг та транспортну інфраструктуру, якщо зловмисники зможуть перепрограмувати контролер двигуна на раптове гальмування. Тому дуже важливо, щоб весь код, що виконується в

контролерах, гальмах, перемикачах та інших елементах, був належним чином підписаний. Необхідно, щоб всі компоненти були правильно налаштовані і ніколи не запускали непідписаний код. Аналогічно, якщо немає перевірки справжності при взаємодії компонентів поїзда, а також при взаємодії поїзда з іншою інфраструктурою, наслідки можуть бути серйозними. Не важко уявити собі, що станеться, якщо керуючі сигнали в поїзді для прискорення і гальмування будуть сфальсифіковані, і що буде, якщо підроблять дозволяють сигнали, коли попереду небезпека.

Крім того, без хостового захисту самі контролери легше зламати, зловмисники можуть досягти своєї мети без зайвих зусиль і без подолання механізмів перевірки справжності та підписів коду. Разом з тим, необхідність комплексної безпеки не обмежується потягами. В автомобілі встановлюють системи охорони, що дозволяють віддалено вимкнути двигун, підключають системи віддаленого пуску двигуна для прогріву і навігаційні системи.

Оскільки підключених в стільникову мережу і інтернет автомобілів стає все більше і більше, для них теж потрібний аналогічний хостовий захист. Такий захист може бути розгорнутий в головному блоці автомобіля, навіть якщо на машині працює операційна система реального часу. Звичайно ж, у міру віддаленого оновлення коду політики безпеки теж можуть оновлюватися віддалено з використанням тієї ж самої системи OTA. Без можливості «підстроювання» безпеки віддалено зловмисники швидко виявлять слабкі місця і вдарять по них. Проте, навіть якщо все зроблено правильно, найсильніші супротивники все-таки зможуть подолати контрзаходи. Тому аналітика безпеки бекенд повинна мінімізувати негативні впливи стратегічних загроз. Ці системи можуть в безперервному режимі збирати дані і формувати «базові поведінкові показники» для поїздів, літаків, автомобілів, виробництв, систем продажу товарів і, напевно, взагалі всього чого завгодно. Завдяки таким «базовим поведінковим показниками», аналітика безпеки IoT може швидко виявляти аномалії, допомагати виявляти приховані загрози і

покращувати кореляцію загроз, виступаючи частиною ширшої аналітики в боротьбі зі стратегічними загрозами.

Звісно, важливо відзначити, що безпека IoT не існує у вакуумі. Багато з цих пристроїв потребують «фізичний захист», і її тип буде сильно залежати від варіанту використання. Для домашнього IoT-пристрою може бути досить огорожі, щоб, наприклад, покоївка не шпигувала за роботодавцями, а IoT на заводі, як правило, треба захищати за кількома рівнями фізичного захисту - від ключів до приміщень, до вимог до відстані від забору, яке визначається електромагнітними ризиками.

Необхідність захисту персоналу також буде помітно відрізнятися. Однак фізична безпека і захист персоналу не є чимось унікальним для IoT. Більшість компаній сьогодні добре справляються з цим завданням, в тому числі щодо своїх традиційних IT-систем. Звичайно, багато хто з цих пристроїв часто взаємодіють з традиційними бекенд-системами, які працюють в приватному центрі обробки даних або в хмарі. Потрібно пам'ятати, що якщо традиційні IT-системи пускають у хід IoT-пристрої або обробляють дані від них, то небезпечна взаємодія IoT з традиційними IT-системами може повністю підірвати всю безпеку, яку користувач вбудував в свою систему IoT[17][18].

3.8 Алгоритм забезпечення безпеки IoT

Забезпечення безпеки Інтернету речей - складний бізнес. Зокрема той факт, що IoT пристрої мають різну форму, розмір та функцію. Це робить традиційні моделі захисту кінцевої точки непрактичними. Крім того, за своєю природою пристрої IoT обмежені ресурсами з точки зору потужності, продуктивності та функціональності. Багато хто використовує дуже індивідуальні та нестандартні операційні системи (наприклад, NANIX, версію Linux для переносних пристроїв).

З багатьох причин доступ до пристроїв може бути обмеженим, тож мережеві адміністратори майже не можуть дізнатись, що відбувається з усіма складовими системи. Подальше ускладнення цієї проблеми полягає в тому, що пристрої IoT мають дуже тривалий життєвий цикл і практично не мають

захисту, наприклад, датчик температури в комерційному або промисловому середовищі. Крім того, вони не можуть бути легко замінені або оновлені новим програмним забезпеченням через їх оригінальний дизайн або обмежені ресурси, такі як пам'ять та процесор.

І звісно, багато підключених пристроїв використовують нестандартні та застарілі протоколи зв'язку (наприклад, M2M), які не розпізнаються більшістю продуктами безпеки.

Після аналізу вразливостей та існуючих способів захисту Інтернет речей, наведемо базовий алгоритм надання захисту такій системі:

1. Стандартизація: мережа IoT в даний час є переважно бездротовою, це робить безпеку набагато складнішою, ніж традиційні дротові мережі через різноманіття нових протоколів і стандартів щодо радіочастот та радіозв'язку. Пристрої та система в цілому має відповідати стандартам, щоб забезпечити безпеку вашої системи та не зробити її уразливою для злочинців.
2. Сертифікація пристроїв/перевірка справжності: окрім відповідності стандартам, необхідно забезпечувати складові мережі сертифікатами, що видаються центрами сертифікації, для можливості перевірки пристроїв, що бажають проникнути в Вашу мережу та можуть їй зашкодити. Така перевірка допомагає проаналізувати певний пристрій на реєстрацію в своєрідній базі та надасть інформацію стосовно якості і можливості нанести збитки.
3. Аутентифікація: пристрої IoT повинні бути законними користувачами. Методи досягнення такого роду аутентифікації від статичних паролів до двофакторної аутентифікації, біометрії та цифрових сертифікатів. Унікальним для IoT є те, що пристрої(наприклад, вбудовані датчики) повинні розпізнати інші пристрої. Саме це зменшує ймовірність проникнення чужорідного тіла в системі.
4. Шифрування: необхідне для запобігання несанкціонованого доступу до даних. Це важко забезпечити через розмаїття пристроїв IoT та

апаратних профілів. Проте шифрування має бути частиною повного процесу управління безпекою. На сьогоднішній день вчені сперечаються з приводу надійності того чи іншого варіанту та використання його в IoT, проте вже розроблений чіп для шифрування на еліптичних кривих, що може застосовуватися в пристроях Інтернету речей.

5. Захист інтерфейсу: більшість виробників обладнання та програмного забезпечення надають доступ до пристроїв через програмний інтерфейс(API). Їх забезпечення вимагає наявності аутентифікації та авторизації пристроїв, які потребують обміну даними. Тільки авторизовані пристрої, розробники та програми здатні здійснювати зв'язок між захищеними пристроями.
6. Механізми доставки: потрібні постійні оновлення та патчі, необхідні для подолання мінливої тактики кібератакерів. Це вимагатиме знань у патчах, що виправлятиме прогалини в критичному програмному забезпеченні на льоту.
7. Аналітика безпеки та прогнозування загроз: необхідно не лише стежити та контролювати дані пов'язані з безпекою, а також використовувати їх для прогнозування майбутніх загроз. Вони повинні доповнювати традиційні підходи, які шукають дії, що виходять за рамки встановленої політики. Прогноз вимагає нових алгоритмів та застосування штучного інтелекту для обмеження доступу до нетрадиційних стратегій нападу на Вашу систему.
8. Контроль доступу: якщо який-небудь компонент скомпрометовано, контроль гарантує, що вторгнення матиме мінімальний доступ до інших частин системи, наскільки це можливо[19]. Механізми контролю доступу на базі пристроїв аналогічні мережевим системам, навіть якщо хтось зможе вкрасти корпоративні облікові дані для входу в систему, скомпрометована інформація буде обмежуватися лише тими областями мережі, де вона авторизована.

9. Фізична безпека: окрім безпеки внутрішньої, мережі необхідний захист ззовні, тобто, наприклад, якщо це датчик, то він має бути розміщений таким чином, щоб зловмисник не мав до нього прямого фізичного доступу і був непомітний для нього.

Як відомо, машини швидко розвиваються і вже можуть самостійно навчатися. Такий стрімкиий розвиток відіграє велику роль у забезпеченні безпеки, змінюється з точки зору архітектури та дизайну, а також може з'ясувати аномальну поведінку в короткі проміжки часу.

Тобто можна ввести таке поняття як «індекс довіри» для пристроїв IoT. Застосовувати його задля забезпечення інформаійної безпеки на почтакових етапах «спілкування» з чужорідним пристроєм. Індекс довіри прямо пропорційний достовірності джерела з точки зору схожості. Вищий показник довіри більше шансів, що система вважатиме, що дані надійдуть від авторизованого пристрою IoT або джерела. На малюнку представлений алгоритм перевірки для підключення в систему(рис. 3.1).

Якщо індекс довіри нижче порогового, то відповідно пристрій не зможе знаходитися в мережі. Система переспрямовує трафік з пристрою на сервіс, який аналізує відповідь і намагається зібрати більше даних про напад. Ці дані надходять до підсистеми безпеки, і він оновлює параметри характеристик рівня для вивчення та аналізу атаки або зупиняє її на першому ж етапі.

Такий алгоритм вводиться в піраміду для зменшення ймовірності спуфінга(рис. 3.2). Коли ми рухаємося по мережевому стеку, для зловмисників буде не легко копіювати дані. Це відбувається з тієї причини, що складність рівня збільшується, і стає важче влізти в систему або створити хибні характеристики. Наприклад, характеристики фізичного рівня, такі як направлення на абонента(angle of arrival) в бездротовому зв'язку. Приймач отримає дані, програмно визначити їх неможливо. Будь-який зловмисник не зможе придумати такі характеристики, доки він не використовуватиме таке ж обладнання (антену та суміжні схеми) і навіть таке ж місцеположення.

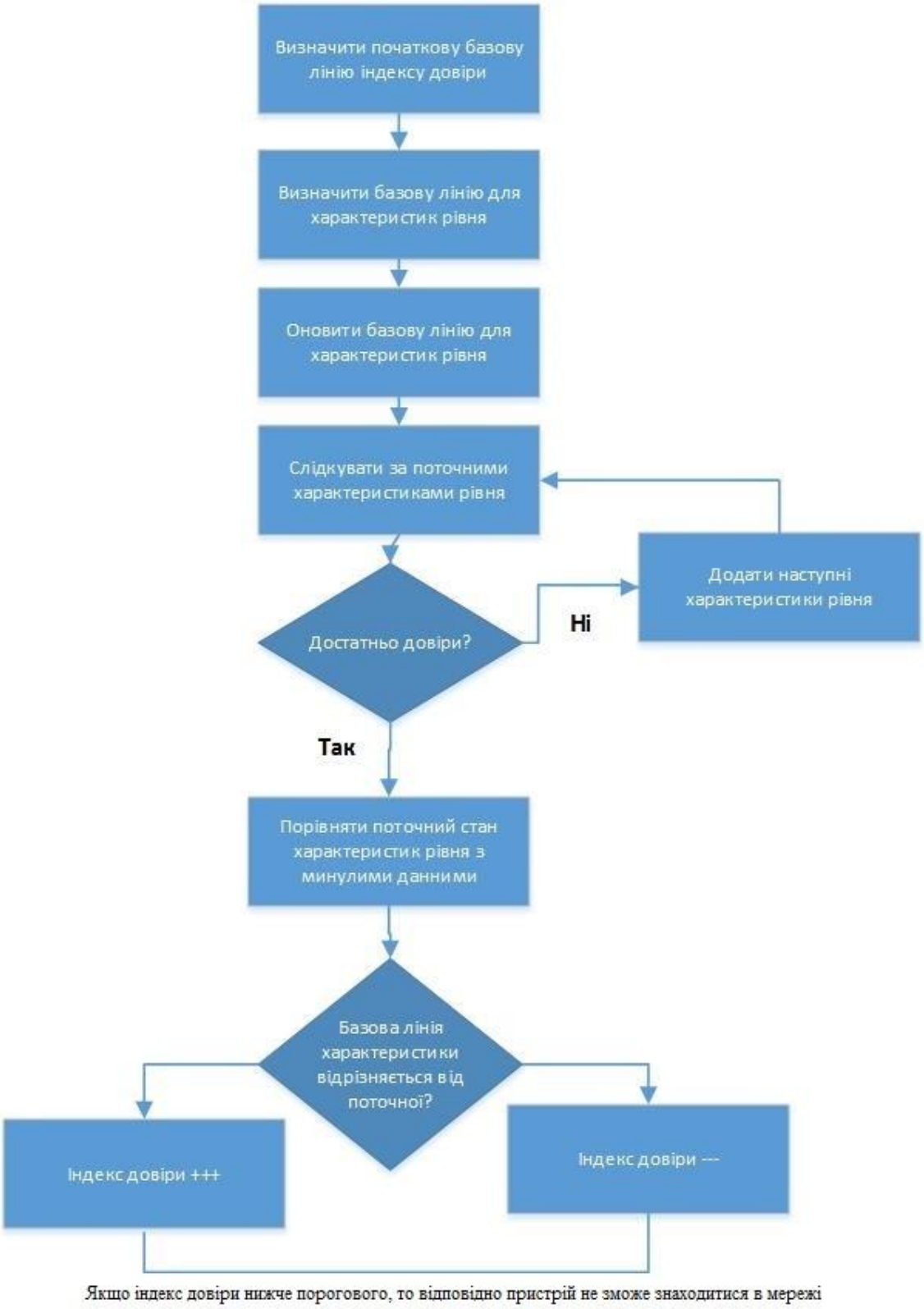

Рис. 3.1 Алгоритм перевірки безпеки

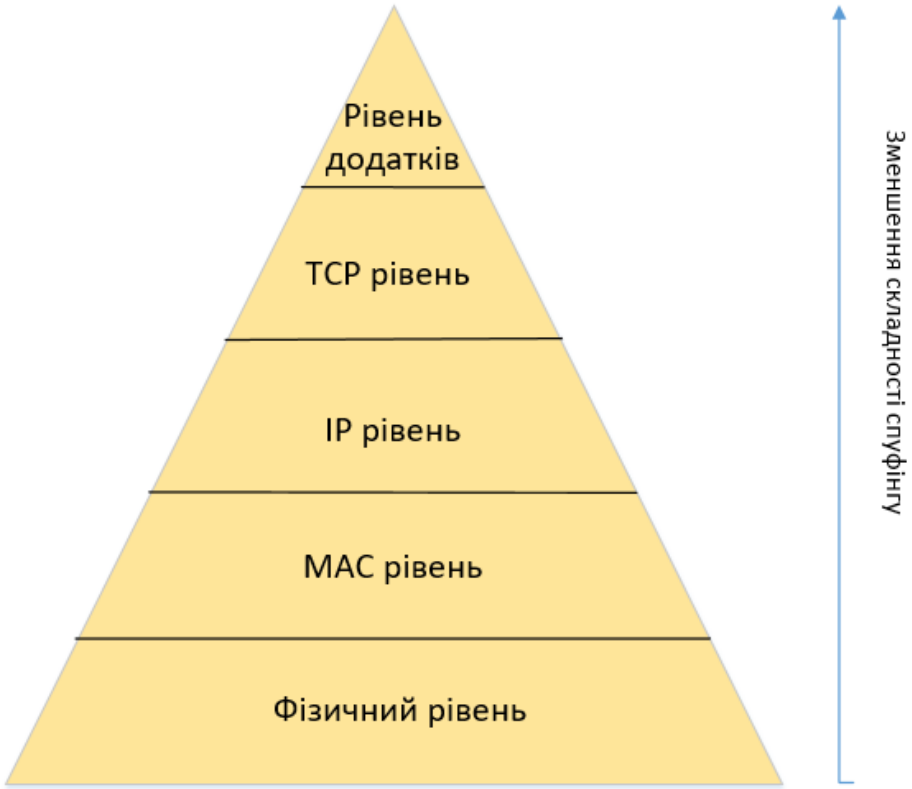

Рис. 3.2 Піраміда зменшення складності спуфінгу

Рис. 3.3 Архітектура системи

ВИСНОВКИ

Інтернет речей - це всесвітня павутина пов'язаних між собою машин та інших фізичних предметів, за допомогою якої може здійснюватися обмін інформацією без людського втручання. Гаджети підключаються до Інтернету, транслюють основні дані в "хмару", звідки інші предмети, оснащені датчиками, що приймають сигнал, можуть збирати ці відомості і використовувати для спрощення багатоступеневих завдань.

Інтернет речей – система, що розвивається дуже стрімко та набуває популярності у всіх галузях нашого життя, зокрема, вже існує поняття «розумне життя». Тобто, вже через певний час нас будуть оточувати речі, що зможуть зчитувати навіть, наші емоції та перефарбовувати стіни під настрій. І це не кажучи вже про виробництво та транспортні мережі. Де IoT повністю зможе замінити людські ресурси. Та на дорогах неможливо буде обманути систему та уникнути штрафів за порушення.

Проте IoT має свої мінуси, це велика кількість стандартів, використання застарілих стандартів, проблема енергоспоживання, самоврядування, конструкції, децентралізації, живлення. Проте однією з найважливіших проблем в реалізації IoT – інформаційна безпека.

Швидке зростання пристроїв IoT та проблеми, пов'язані з бездротовим зв'язком між цими пристроями, потребують розширеного фокусу на кібербезпеці. Як можна захистити IoT? Системи IoT бувають дуже складними, їм потрібні комплексні заходи захисту, що покривають рівні хмар і підключень, також необхідна підтримка пристроїв IoT з обмеженими обчислювальними ресурсами, яких недостатньо для підтримки традиційних рішень безпеки. Простого універсального рішення не існує, і для забезпечення безпеки недостатньо замкнути двері, залишивши вікна відкритими. Безпека повинна бути всебічною, інакше атакуючі просто скористаються найслабшою ланкою. Звичайно, традиційні IT-системи як правило передають і обробляють дані з систем IoT, але самі системи IoT володіють своїми унікальними потребами в захисті.

IoT стає все більш поширеним явищем і все частіше з'являється в системах, від яких залежить життя людей, наприклад, автомобілях, літаках і промисловому обладнанні, тому безпека повинна правильним чином вбудовуватися в ці системи, щоб вони були «безпечні по архітектурі» з захистом, вбудованою від самого початку. У більшості випадків ставки занадто високі для помилок. Дана робота спрямована на підвищення безпеки в системах і спрямована на досягнення успіхів навіть при мінімальному наборі наріжних каменів, які забезпечують фундамент адекватного захисту від сучасних загроз. Запропонована проста і ефективна еталонна архітектура захисту IoT, яку легко розгорнути і масштабувати. Архітектура зниження впливу шкідливого коду гарантує, що весь код криптографічно підписаний і авторизований для пристрою, непідписаний код не дозволений для запуску. Захищений зв'язок за допомогою взаємної перевірки справжності та шифрування. Застосовуються перевірені часом центри сертифікації, які вже захищають понад мільярд IoT-пристроїв. Використовуються нові алгоритми для забезпечення високого рівня безпеки в пристроях IoT з обмеженими обчислювальними ресурсами. Ця архітектура додатково послаблює шкідливу дію за допомогою хостового захисту і підсилює ефективність мінімізації ризиків від всіх інших загроз за допомогою аналітики безпеки. При виявленні вразливостей і загроз ризик їх реалізації можна знизити за допомогою ефективного, надійного і захищеного динамічного управління системою. Успішне забезпечення безпеки систем починається з моделювання ризиків. Без розуміння, як зловмисники можуть скомпрометувати систему, малоймовірно надійно захистити будь-яку IT-систему. Тож було запропоновано алгоритм захисту пристроїв за допомогою поняття «індекс довіри», що зможе допомогти системі проаналізувати мережу на наявність «чужих» пристроїв та вберегти її від взлому та не дозволить зловмиснику проникнути в мережі та забезпечить інформаційну безпеку Вашої «розумної» системи.

СПИСОК ЛІТЕРАТУРИ

1. Что такое Интернет вещей(IoT)? // електрон. текст. дані URL: https://r-iot.org/2016/04/04/что-такое-интернет-вещей-iot/ (дата звернення: 04.12.2018)
2. Найдич А. «Интернет вещей» — реальность или перспектива? // електрон. текст. дані URL: https://compress.ru/article.aspx?id=24290 (дата звернення: 04.12.2018)
3. Интернет вещей – а что это? // електрон. текст. дані URL: https://habr.com/post/149593/ (дата звернення: 04.12.2018)
4. Интернет вещей – технология будущего, которая меняет реальность сегодня // електрон. текст. дані URL:https://robo-sapiens.ru/stati/internet-veshhey/ (дата звернення: 04.12.2018)
5. Восков Л.С. Беспроводные сенсорные сети // електрон. текст. дані URL: http://nit.miem.edu.ru/sbornik/2009/plen/006.html (дата звернення: 04.12.2018)
6. Pethuru Raj Anupama C. Raman The Internet of Things Enabling Technologies, Platforms, and Use Cases // електрон. книга URL: *https://www.kahkeshan.com/Source/.../948edc08-24ea-4b8d-a398-a761dd825bc3* (дата звернення: 04.12.2018)
7. Лекція 1. Загальні поняття Інтернету речей // електрон. текст. дані URL: http://academicfox.com/lektsiya-1-zahalni-ponyattya-internetu-rechej/ (дата звернення: 04.12.2018)
8. Борейко О.Ю. Проектування IoT // електрон. текст. дані URL: https://www.slideshare.net/ssuserf405bc/iot-79608563 (дата звернення: 04.12.2018)
9. Vladimir_Sklyar Стандарті архитектурі для IoT // електрон. текст. дані URL: https://habr.com/post/307668/ (дата звернення: 04.12.2018)
10. Росляков А.В. Интернет вещей // електрон. текст. дані URL: http://elib.psuti.ru/Roslyakov_Vanyashin_Grebeshkov_Internet_veschej.pdf (дата звернення: 04.12.2018)

11. Дейв Эванс Интернет вещей Как изменится вся наша жизнь на очередном витке развития Всемирной сети // електрон. текст. дані URL: https://www.cisco.com/c/dam/global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf (дата звернення: 04.12.2018)
12. Сафронов П.С. Анализ характеристик протокола функционирования беспроводных сенсорных сетей LEACH // електрон. текст. дані URL: http://dspace.susu.ru/xmlui/bitstream/handle/0001.74/16406/2017_272_safronovps.pdf?sequence=1 (дата звернення: 04.12.2018)
13. The Smart Grid: How Energy Technology Is Evolving // електрон. текст. дані URL: https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/02/the-smart-grid-how-energy-technology-is-evolving (дата звернення: 04.12.2018)
14. Розроблення проекту супроводу системи управління дорожнім трафіком на базі інтелектуальної системи відеоспостереження // електрон. текст. дані URL: http://5fan.ru/wievjob.php?id=38630 (дата звернення: 04.12.2018)
15. Информационная безопасность интернета вещей (Internet of Things) // електрон. текст. дані URL: http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернет_вещей_(Internet_of_Things) (дата звернення: 04.12.2018)
16. Богуслав А.М. Методи та моделі забезпечення захисту безпроводних сенсорних мереж// електрон. текст. дані URL: http://er.nau.edu.ua/bitstream/NAU/22464/2/diser_ua_2.0.pdf (дата звернення: 04.12.2018)
17. Орешкина Д. Эталонная архитектура безопасности интернета вещей // Часть 1. електрон. текст. дані URL: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 (дата звернення: 04.12.2018)
18. Орешкина Д. Эталонная архитектура безопасности интернета вещей // Часть 2. електрон. текст. дані URL: https://www.anti-

malware.ru/practice/solutions/iot-reference-architecture-protection-part-2 (дата звернення: 04.12.2018)

19. John Blyler 8 Critical IoT Security Technologies // електрон. текст. дані URL: https://www.electronicdesign.com/industrial-automation/8-critical-iot-security-technologies (дата звернення: 04.12.2018)
20. Security in the internet of things // електрон. текст. дані URL: Sehttps://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf (дата звернення: 04.12.2018)