Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Ткача Максима Олександровича*

академічної групи *125м-22з-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Криптографічний захист даних у IoT системах*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи				
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	к.е.н., доц., Пілова Д.П.			

Рецензент				

Нормоконтролер				

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Ткача М.О.*** **академічної групи** ***125м-22з-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Криптографічний захист даних у IoT системах***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____№ _____

Розділ	Зміст	Термін виконання
Розділ 1	Розглянуто історію розвитку IoT речей, розлянуто архітектуру та екоситему IoT, шляхи передачи інформації між пристроями в мережі.	05.11.2023
Розділ 2	Виконо обгрунтування та вибір обладнення, розглятуті стандати сумістності, запропоновані більш захищені алгоритми та методи захисту інформіції в екоситемі IoT речей	20.11.2023
Розділ 3	Визначення економічної доцільності впровадження того чи іншого рішення.	01.12.2023

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 01.09.2023

Дата подання до екзаменаційної комісії: 06.12.2023

Прийнято до виконання _____ Ткач М.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 82 с., 13 рис., 2 табл., 4 додатків, 33 джерел.

Об’єкт дослідження: забезпечення інформаційної безпеки в мережах Інтернет речей IoT.

Предмет дослідження: методи забезпечення інформаційної безпеки в мережі Інтернету речей.

Мета роботи: зниження ризиків інформаційної безпеки в мережах Інтернет речей IoT за рахунок використання найбільш ефективних програмно-апаратних методів забезпечення інформаційної безпеки та як наслідок продовження терміну експлуатації пристрою на ринку.

Методи дослідження: спостереження, порівняння, аналіз, опис та розрахунки.

В першому розділі розлянуто архітектуру та екоситему интернет речей, шляхи передачи інформації.

В спеціальній частині виконо обгрунтування та вибір обладнення, запропоновані більш захищені алгоритми та методи захисту інформіції в екоситемі IoT речей.

В економічному розділі обґрунтовано економічну доцільність застосування того чи іншого рішення для збільше безпеки та терміну експлуатації IoT системі вцілому.

Наукова новизна полягає у вивчені особливостей застосування полегшеної кріптографії в IoT системі.

Практична цінність полягає у підвищені надійності та збільшеня терміну експлуатації IoT речей.

IoT, IIoT, RFID, Wi-Fi, Zigbee, Z-Wave, 3G, 4G, LTE, LoRaWAN, MQQT, LPWAN, HTTP, HTTPS, API, GPRS, GPS, M2M, VPN, QoS, MEMC, LWHF, RSA, DSA, AES, NFC, P2P.

ABSTRACT

Explanatory note: 82 p., 13 pictures, 2 tables, 4 applications, 33 sources.

Object of research: ensuring information security in Internet of Things (IoT) networks.

Subject of research: methods of ensuring information security in the IoT network.

Purpose: to reduce information security risks in IoT networks by using the most effective software and hardware methods of ensuring information security and, as a result, extending the life of the device on the market.

Research methods: observation, comparison, analysis, description and calculations.

The first chapter describes the architecture and ecosystem of the Internet of Things, as well as the ways of information transmission.

In the special part, the author justifies and selects equipment, proposes more secure algorithms and methods for protecting information in the IoT ecosystem of things.

The economic section substantiates the economic feasibility of applying a particular solution to increase the safety and lifespan of the IoT system as a whole.

The scientific novelty lies in the study of the peculiarities of using lightweight cryptography in an IoT system.

The practical value lies in the increased reliability and lifespan of IoT things.

IoT, IIoT, RFID, Wi-Fi, Zigbee, Z-Wave, 3G, 4G, LTE, LoRaWAN, MQQT, LPWAN, HTTP, HTTPS, API, GPRS, GPS, M2M, VPN, QoS, MEMC, LWHF, RSA, DSA, AES, NFC, P2P.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

IoT – Інтернет речей;

RFID – Radio Frequency IDentification;

IIoT – Industrial Internet of Things;

ARPANET – Advanced Research Projects Agency Network;

iBeacon – маячок с Bluetooth Low Energy;

МЕМС – мікро-електромеханічні системи;

IP – Internet Protocol;

LAN – Local Area Network;

FTP – file transfer protocol

Wi-Fi – Wireless Fidelity;

Zigbee – стандарт для набору високорівневих протоколів зв'язку;

Z-Wave – це протокол бездротового зв'язку;

3G – Third Generation;

4G – Fourth Generation;

LTE – Long-Term Evolution;

DSL – Digital Subscriber Line;

LoRaWAN – long range wide area network;

LPWAN Low- Power Wide-Area Network;

MQQT – message queue telemetry transport;

HTTP – hyper text transfer protocol;

HTTPS – hyper text transfer protocol secure;

HMI – Human Machine Interface;

API – Application Program Interface;

IWF – IoT World Forum;

IIC – Industrial Internet Consortium;

IWF – IoT World Forum;

ESF – Everyware Software Framework;

GPRS – General Packet Radio Service;

GPS – Global Positioning System;

ARM – Advanced RISC Machine;

DHCP – Dynamic Host Configuration Protocol;

ICMP – Internet Control Message Protocol;

M2M – Machine-to-Machine;

VPN – Virtual Private Network;

QoS – Quality of Service;

FreeRTOS – Free Real Time Operating System;

IT – інформаційними технологіями (),

ПЗ – програмне забезпечення;

OT – Operational Technology,

СУБД – Система Управління Базами Даних;

ETL – Extract Transform Load;

MIMO – Multiple Input Multiple Output;

PoE – Power over Ethernet;

SCADA – Supervisory Control And Data Acquisition;

e-MMC – Embedded Multimedia Memory Card;

CCM – Cloud Client Manager;

GPIO – General Purpose Input Output;

ЦАП – Цифро Ана́логовий Перетво́рювач;

АЦП – Ана́лого Цифрови́й Перетво́рювач;

LWHF – Lightweight Hash Functions;

ECC – Elliptic Curve Cryptography;

RSA – Rivest-Shamir-Adleman;

DSA – Digital Signature Algorithm;

ECC – Error Correcting Code;

AES – Advanced Encryption Standard;

MAC – media access control;

ПЗ – Програмне Забезпечення;

NFC – Near Field Communication;

P2P – Peer to Peer ;

ЗМІСТ

ВСТУП

Об’єкт розробки: інформаційна безпеки в мережах Інтернет речей Internet of Things IoT на протязі всього часу підтримки пристрою.

Предмет розробки: методи забезпечення інформаційної безпеки в мережі Інтернету речей IoT.

Мета кваліфікаційної роботи: зниження ризиків інформаційної безпеки в мережах Інтернет речей IoT за рахунок використання найбільш ефективних програмно-апаратних методів забезпечення інформаційної безпеки та як наслідок продовження терміну експлуатації пристрою на ринку.

Забезпечення потреб сучасної людини вимагає від технічного прогресу створення все більшої кількості електронних пристроїв. Нажаль, невеликий термін експлуатації деяких пристроїв, а що важливіше, потужний тиск маркетингових акцій на свідомість людей призводять до швидкої заміни електронних пристроїв. В Україні проблема накопичення електронних відходів стоїть дуже гостро через: зростання ринку електронної техніки та відсутність налагодженої системи її утилізації. Згідно зі статистичними даними на території України перебувають у користуванні 53,6 мільйона мобільних засобів зв’язку, щороку імпортується 300 тисяч портативних комп’ютерів.

Одним з варіантів електронного сміття є IP камери, щорічно випускають мільйони пристроїв. Період експлуатації декілька років а то і місяців, це пов’язано з припиненням підтримкою хмарою. Багато пристроїв застріли за технологіями та можливостями. Багато пристроїв мають вразливості до кібератак та інше.

Повернення цих пристроїв до екосистеми, зменшить кількість електронного сміття. Подовження терміну експлуатації зменшить кількість випускаємих камер на рік. Ці пристрої відносяться до категорії Інтернет речей IoT. Інтернет речей породжує великий потік інформації, який необхідно шифрувати на кінцевих пристроях. Причому більшу частину

девайсів займатиме індустріальний IIoT- Industrial Internet of Things. Як згадувалося вище, від подібних засобів вимагається низька ціна виробництва та обслуговування, що веде до низького обсягу батареї, обмеження оперативної пам'яті тощо.

Ось цьому для IoT потрібна легка криптографія Lightweight Cryptography - LWC, що об'єднує надійні та ефективні алгоритми з мінімальними витратами на обладнання. Також вирішенням проблеми може стати перепрограмування проблемних IP-камер на прошивку OpenIPC - це відкрита операційна система Linux для IP-камер з ARM і MIPS процесорами, покликана замінити собою закриті, непрозорі, небезпечні, часто закинуті та непідтримувані прошивки, які встановлюють під час виробництва обладнання.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Історія розвитку Інтернет речей

В даний час відбувається дуже багато розмов з приводу інтернету речей і його впливу на різні сфери життя: від того, як ми подорожуємо і робимо покупки, до того, як виробники відстежують товарні запаси. Але що таке інтернет речей? Як це працює? Зв'язок між пристроями може відбуватися між різними фізичними об'єктами. В основному пристрої, які користувачі можуть підключати до будь-якого іншого пристрою або безпосередньо до Інтернету.

Термін «інтернет речей», зобов'язаний своєю появою Кевіну Ештону, який в 1997 р, працюючи на компанію Proctor and Gamble, застосував технологію радіочастотної ідентифікації (RFID) для керування системою поставок [1]. Завдяки цій роботі в 1999 році його запросили в Масачусетський технологічний інститут, де він з групою однодумців організував дослідний консорціум Auto-ID Center

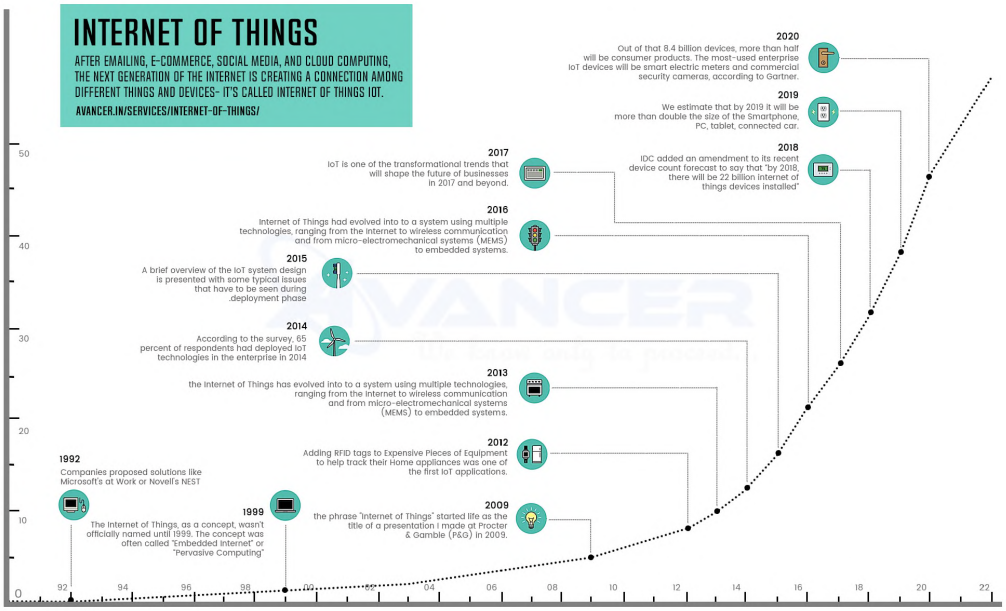

Рисунок 1.1. – Історія Інтернету речей

З тих пір Інтернет речей звершив перехід від простих радіочастотних міток до екосистеми і індустрії. Аж до 2012 р ідея підключення речей до Інтернету переважно відносилася до смартфонів, планшетів, ПК і ноутбуків, більшості технологій, на яких будується Інтернет речей, просто не існувало.

До 2000 року більшість пристроїв, які можна було підключити до Інтернету, представляло собою комп'ютери різних розмірів. Нижче показаний поступове підключення речей до Інтернету.

1973 - Маріо У. Кардулло патент на першу радіо-частотну мітку

1982 - Підключений до Інтернету автомат з газованою водою в університеті Карнегі- Меллон

1989 - Підключений до Інтернету тостер на конференції Interop '89

1991 - Компанія HP представила HP LaserJet IIISi: перший підключений до мережі Ethernet мережевий принтер

1993 - Підключена до Інтернету кавоварка в Кембриджському університеті (перша підключена до Інтернету камера)

1996 - Підрозділ General Motors OnStar (дистанційна діагностика 2001)

1998 - Поява організації Bluetooth SIG

1999 - Холодильник LG Internet Digital DIOS

2000 - Перші прояви розробленої компанією HP концепції всепроникної комп'ютеризації (Cooltown): HP Labs, система обчислювальних і комунікаційних технологій, які в поєднанні один з одним створюють підключення до Інтернету для людей, місць і об'єктів

2001 - Випуск першого пристрою, що використовує технологію Bluetooth: мобільний телефон KDDI з підтримкою Bluetooth

2005 - Міжнародний союз електрозв'язку, спеціалізована установа ООН, випустив звіт, в якому вперше були сформульовані прогнози розвитку Інтернету речей

2008 - Поява першого IoT-спільноти IPSO Alliance, метою якого було сприяння підключенню речей до Інтернету

2010 - Успішна розробка напівпровідникових світлодіодних ламп привела до розвитку концепції розумного освітлення

2014 - Компанія Apple створила протокол iBeacon для маячків.

Інтернет речей захопив практично кожен сегмент в сфері промисловості, бізнесу, охорони здоров'я і споживчих товарів [2].

1.2 Інтернет речей в промисловості IIoT

Ключовою технологією програми Industry 4.0 вважається Інтернет Речей. Складовою частиною Інтернету Речей і його головною на даному етапі розвитку технологій рушійною силою є Промисловий (або Індустріальний) Інтернет Речей (Industrial Internet of Things, IIoT). Промисловий Інтернет Речей — це система об'єднаних комп'ютерних мереж і підключених до них промислових (виробничих) об'єктів з вбудованими датчиками і програмним забезпеченням для збору та обміну даними, з можливістю віддаленого контролю і управління в автоматизованому режимі, без участі людини.

На першому етапі впровадження IIoT на промислове обладнання встановлюють датчики, виконавчі механізми, контролери та людино-машинні інтерфейси. В результаті стає можливим збір інформації, яка дозволяє керівництву отримувати об'єктивні і точні дані про стан виробництва. Оброблені дані надаються всім підрозділам підприємства. Це допомагає налагодити взаємодію між співробітниками різних підрозділів і приймати обґрунтовані рішення.

Отримана інформація може бути використана для запобігання позаплановим простоям, поламкам устаткування, скороченню позапланового техобслуговування та збоям в управлінні ланцюжками постачання, тим самим дозволяючи підприємству функціонувати більш ефективно. При обробці величезного масиву неструктурованих даних, що надходять з датчиків, їх фільтрація і адекватна інтерпретація стає пріоритетним завданням. Тому особливого значення набуває представлення інформації в зрозумілому користувачеві вигляді. Для цього використовуються передові аналітичні платформи, призначені для збору, зберігання і аналізу даних про технологічні процеси і події, що відбуваються в реальному масштабі часу.

Промисловий IoT дозволяє створювати виробництва, які виявляються більш ощадливими, гнучкими і ефективними, ніж чинні. Бездротові пристрої з підтримкою протоколу IP, включаючи смартфони, планшети і датчики, вже

активно використовуються на виробництві. Наявні дротові мережі датчиків в найближчі роки будуть розширені і доповнені бездротовими мережами, завдяки чому на підприємствах суттєво розширяться зони застосування систем моніторингу та управління. Наступний етап оптимізації виробничих процесів буде характеризуватися все більш щільною конвергенцією кращих інформаційних і операційних технологій.

В міру становлення цифрових екосистем виробничі підприємства з ізольованих систем, які самостійно виконують всі необхідні для виробництва продукції виробничі та бізнес-процеси, будуть перетворюватися у відкриті системи, що поєднують різних учасників ринку; управляти засобами виробництва в цих системах буде не персонал, а хмарні сервіси, кінцева мета всіх цих трансформацій — не випуск продукції, а надання послуг споживачеві.

1.3 Екосистема Інтернету речей

До екосистеми Інтернету речей відносяться усі засоби, сервіси і технології, які використовуються в Інтернеті речей.

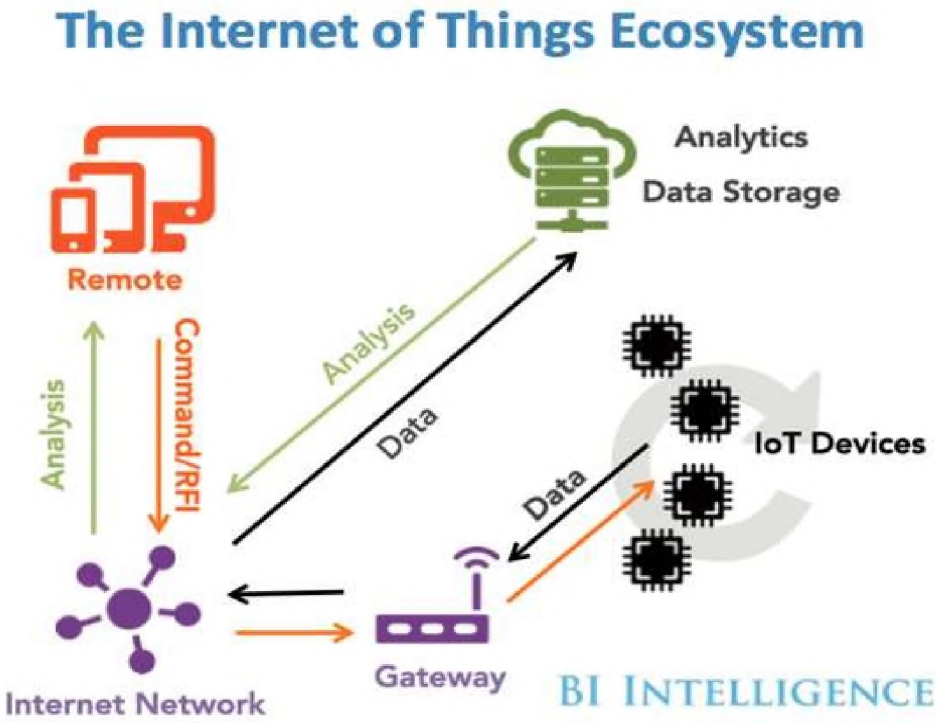

Рисунок 1.2. – Екосистема Інтернету речей

До них можна віднести:

1. sensors: вбудовані системи, операційні системи реального часу, джерела безперебійного живлення, мікро-електромеханічні системи МЕМС;

2. системи зв'язку з датчиками: зона охоплення бездротових персональних мереж становить від 0 см до 100 м. Для обміну даними між датчиками застосовуються низькошвидкісні малопотужні інформаційні канали, які часто побудовані не на протоколі IP;

3. локальні обчислювальні мережі LAN: зазвичай це системи обміну даними на основі протоколу IP, наприклад, 802.11 Wi-Fi-мережу для швидкої радіозв'язку, часто це пірингові або зіркоподібні мережі;

4. агрегатори, маршрутизатори, шлюзи, пограничні пристрої Edge Device: постачальники вбудованих систем, самі бюджетні складові (процесори, динамічна оперативна пам'ять і система зберігання даних), виробники модулів, виробники пасивних компонентів, виробники тонких клієнтів, виробники стільникових і бездротових радіосистем, постачальники міжплатформового програмного забезпечення, розробники інфраструктури туманних обчислень, інструментарій для граничної аналітики, безпеку граничних пристроїв, системи управління сертифікатами;

5. глобальна обчислювальна мережа: оператори стільникового зв'язку, оператори супутникового зв'язку, оператори малопотужних глобальних мереж LPWAN. Зазвичай застосовуються транспортні протоколи Інтернету для IoT і мережевих пристроїв MQTT, CoAP і навіть HTTP ;

6. хмара: інфраструктура в якості постачальника послуг, платформа в якості постачальника послуг, розробники баз даних, постачальники послуг потокової і пакетної обробки даних, інструменти для аналізу даних, програмне забезпечення в якості постачальника послуг, постачальники озер даних, оператори програмно-визначених мереж/програмно-визначених периметрів, сервіси машинного навчання;

7. сервіси аналізу даних: величезні масиви інформації передаються в хмару. Робота з великими обсягами даних і отримання з них користі - це

завдання, що вимагає комплексної обробки подій, аналітики і прийомів машинного навчання;

8. безпека: при зведенні всіх елементів архітектури воєдино постають питання кібербезпеки. Безпека стосується кожного компонента: від датчиків фізичних величин до ЦПУ і цифрового апаратного забезпечення, систем радіозв'язку і самих протоколів передачі даних. На кожному рівні необхідно забезпечити безпеку, достовірність і цілісність. У цьому ланцюзі не повинно бути слабких ланок, оскільки Інтернет речей стане головною мішенню для атак хакерів в світі [3].

1.4 Архітектура Інтернету Речей

Архітектура Інтернету речей відрізняється в залежності від реалізації. Тим не менше вона дещо схожа на архітектуру класичних систем АСУТП. Один із прикладів архітектури показаний на рисунку 1.3.

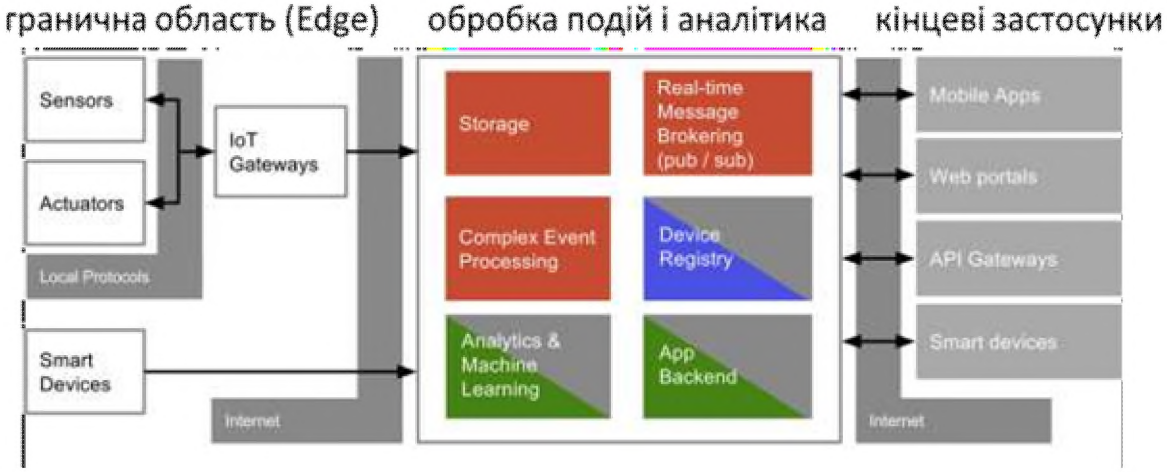

Рисунок 1.3 – Архітектура Інтернету Речей

Взаємодія з «речами» відбувається через датчики та виконавчі механізми, аналогічно як це робиться в АСУТП для будь якого об’єкту керування. Ці датчики разом з усією інфраструктурою для інтеграції з рівнем обробки подій через мережу Internet формують так звану граничну область.

Дані що поступають з граничної області зберігаються і обробляються відповідно до задачі (рівень обробки подій і аналітики, event processing. На цьому рівні події зберігаються, обробляються, перенаправляються потрібним

додаткам (Real-Time Message Brokering, Stream Processing). Додатково на цьому рівні відбувається адміністрування та керування пристроями з граничної області. Дані обробляються з використанням аналітичних сервісів на основі них проводиться машинне навчання, що дозволяє зробити певні висновки про об'єкт. Цей рівень як правило реалізований з використанням хмарних Cloud або туманних Fog обчислень. Якщо провести аналогію с АСУТП, то це рівень контролерів та SCADA (за виключенням функцій HMI). Отримання результатів, контроль, віддалене керування та адміністрування системи проводиться через кінцеві застосунки з використанням Internet. Цей рівень можна умовно порівняти з HMI в АСУТП.

На рисунку 1.4. показана подібна наведеній вище архітектура, однак у вигляді сервісів. На ньому область Edge представлений у вигляді датчиків, Device Hub/Gateway - збір та маршрутизація даних Device Management - керування пристроями. Останні частково виконуються як хмарні обчислення так і на граничних пристроях. Усі функції збереження та первинної обробки подій (даних) зведені до Data Management. Усі інші функції обробки, в тому числі аналітичні показані як додатки PaaS, що взаємодіють з сервісами керування даних через API.

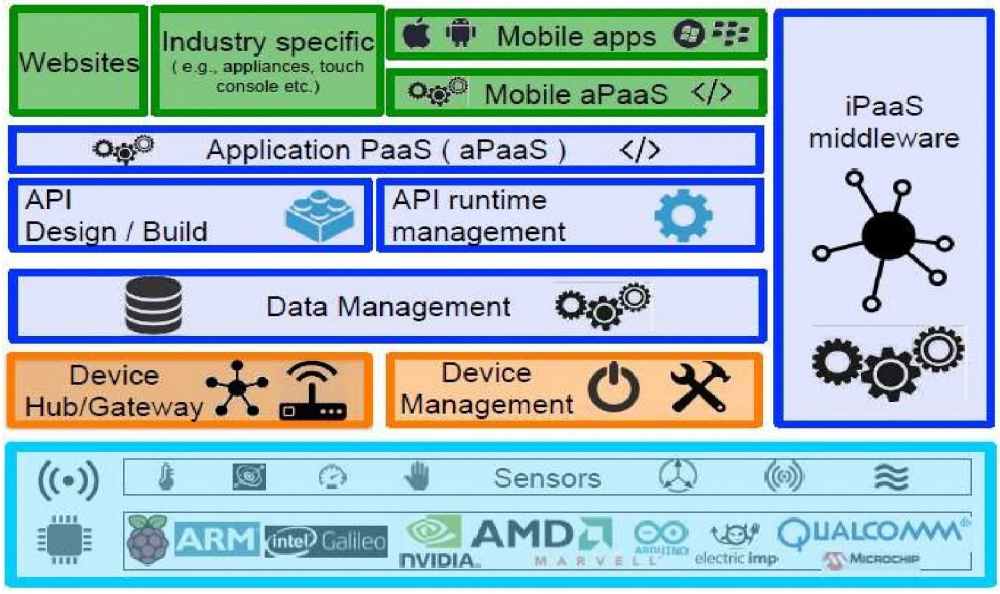

Рисунок 1.4 – Архітектура у вигляді сервісів

Ще один приклад архітектури Інтернету Речей показаний на рисунку 1.5. Як видно, усі наведені архітектури мають спільні риси: наявність трьох рівнів, подібні функції, наявність хмарних обчислень, використання Інтернету як інтеграційного рівня.

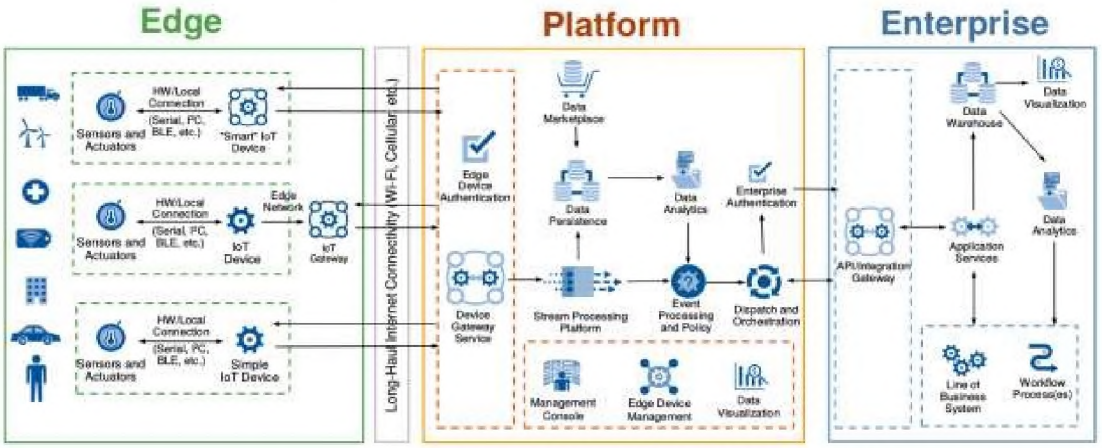

Рисунок 1.5 – Архітектура Інтернету речей

Інтернет починається або закінчується однією подією: простий рух, зміна температури або, може бути, важіль замикає замок. На відміну від багатьох існуючих IT-пристроїв, Інтернет речей здебільшого пов'язаний з фізичною дією або подією. Він формує реакцію на якийсь фактор реального світу. Іноді при цьому один-єдиний датчик може згенерувати величезний обсяг даних, наприклад, акустичний датчик для профілактичного огляду обладнання. В інших випадках всього одного біта даних достатньо, щоб передати життєво важливі відомості про стан здоров'я пацієнта. Якою б не була ситуація, системи датчиків еволюціонували і, відповідно до закону Мура, зменшилися до субнанометрових розмірів і стали істотно дешевше. Саме до цього апелюють ті, хто прогнозує, що до Інтернету речей будуть підключені мільярди пристроїв, і саме тому ці прогнози виправдаються.

Тому, розглядаючи Інтернет Речей, необхідно розглядати мікроелектромеханічні системи, датчики і інші типи недорогих граничних пристроїв і їх електрофізичних властивостей. Також це стосується силових і енергетичних систем, необхідних для живлення цих граничних пристроїв. Не можна вважати, що граничні пристрої забезпечуються енергією за замовчуванням. Мільярди маленьких датчиків все одно потребують великої

кількості енергії. З питанням живлення також пов’язані питання організації хмарних сервісів IoT.

1.5 Передача даних в IoT системах

Велика увага при розроті IoT приділяється встановленню з'єднання і роботі мереж. Інтернету речей не існувало б без надійних технологій передачі даних з найвіддаленіших і несприятливих областей в найбільші центри збору даних компаній Google, Amazon, Microsoft і IBM. Словосполучення «Інтернет речей» містить слово «Інтернет», тому необхідно вивчати питання, що стосуються мережних технологій, обміну даними та навіть теорії сигналів. Базова властивість Інтернету речей - це не датчики і не програми, а можливість встановити з'єднання.

Передача даних і встановлення мережевого з'єднання базуються на базі систем зв'язку ближньої дії - персональних мереж, зазвичай побудованих без дотримання правил IP- протоколу. Це може бути як проводові так і бездротові мережі. До бездротових IoT- мереж/протоколів як правило відносяться протоколи Bluetooth, mesh-мережі, Zigbee, Z- Wave. Для IIoT це також Wireless Hart та ISA100. Це яскравий приклад різноманіття бездротових систем зв'язку IoT. Перелік дротових мереж ще більший, так як сюди входять усі можливі промислові мережі та протоколи.

IP-протоколу, включаючи широкий діапазон Wi-Fi-мереж на основі стандартів IEEE 802.11, 6LoWPAN і технології Thread. Інколи використовуються телекомунікації на основі стільникових стандартів (3G, 4G LTE) і нові стандарти, що забезпечують роботу Інтернету речей і міжмашинної взаємодії, такими як Cat-1 і Cat-NB, а також пропрієтарні протоколи LoRaWAN і Sigfox, що використовуються саме для IoT.

Для передачі даних від датчиків в Інтернет-простір необхідні дві технології: маршрутизатор-шлюз і опорні інтернет-протоколи, що забезпечують ефективність обміну даними. Маршрутизатор особливо важливий в таких аспектах, як безпека, управління і напрям даних. Граничні

маршрутизатори керують і стежать за станом відповідних mesh-мереж, а також вирівнюють і підтримують якість даних. Також велике значення належить конфіденційності та безпеки даних. Маршрутизатор відіграє важливу роль в створенні віртуальних приватних мереж, віртуальних локальних мереж і програмно- визначених глобальних мереж. Вони в буквальному сенсі можуть містити тисячі вузлів, що обслуговуються єдиним граничним маршрутизатором, і в якійсь мірі маршрутизатор служить розширенням для хмари.

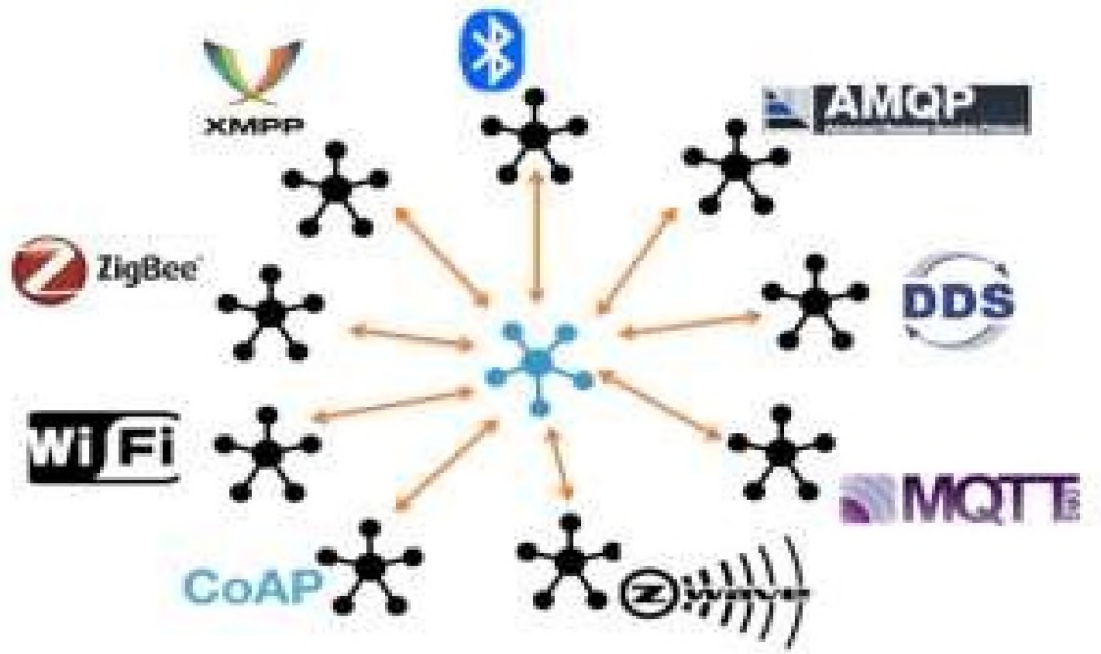

Рисунок 1.8 – Мережі та протоколи IoT

На цьому рівні використовується ряд протоколів, необхідних для обміну даними між вузлами, маршрутизаторами і хмарними сервісами в межах IoT-системи. Інтернет речей відкрив дорогу новим IoT-протоколам, які виходять на один рівень з традиційними протоколами HTTP і SNMP, які застосовуються вже кілька десятків років. Для передачі IoT- даних потрібні ефективні, енергозберігаючі протоколи з малою затримкою, здатні легко і безпечно відправляти дані в хмару і з нього. Зокрема тут використовуються такі протоколи, як всюдисущий MQTT, AMPQ і CoAP.

Туманні і граничні обчислення, аналітика і машинне навчання

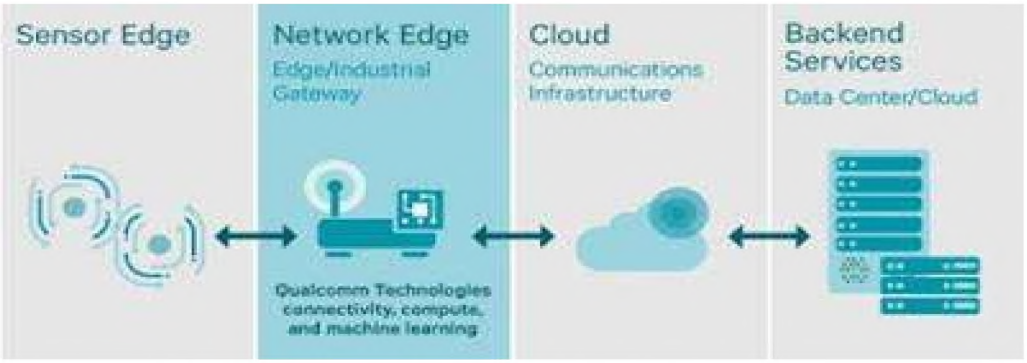

Рисунок 1.9 – Туманні та граничні обчислення

На цьому етапі необхідно вирішити, що робити з потоком даних, що надходять в хмарний сервіс з граничного вузла. Щоб навчитися правильно оцінювати, як система буде розвиватися і рости, необхідно розібратися у всіх тонкощах і складнощах архітектури хмарних систем, який вплив на IoT-систему робить запізнювання. Крім того, не все треба відправляти в хмару. Пересилання всіх IoT-даних обходиться значно дорожче, ніж їх обробка на кордоні мережі (граничні обчислення, Edge Computing) або включення граничного маршрутизатора в зону, яку обслуговує хмарний сервіс (туманні обчислення, Fog computing). Туманні обчислення також стандартизуються, зокрема є стандарт туманних обчислень, наприклад архітектура OpenFog.

Дані, які були отримані шляхом перетворення аналогового фізичного впливу в цифровий сигнал, можуть мати велику вагу. Саме тут в гру вступають засоби аналітики і процесори правил IoT-системи. Ступінь складності введення в дію IoT-системи залежить від того, яке рішення проектується. У деяких ситуаціях все досить просто: наприклад, коли на граничний маршрутизатор, який контролює кілька датчиків, потрібно встановити простий процесор правил, що відслідковує аномальні скачки температури. Інша ситуація - величезна кількість структурованих і неструктурованих даних в режимі реального часу передається в хмарне озеро даних, що вимагає високої швидкості обробки (для прогнозної аналітики) і довгострокового прогнозування на базі високотехнологічних моделей машинного навчання, таких як рекурентна нейронна мережа в пакеті аналізу сигналів з кореляцією по часу. Тут є певні проблеми і складнощі аналітики,

які вирішуються різними підходами та методами, наприклад складними обробниками подій, байесовськими мережами і формування нейронних мереж.

1.6 Безпека Інтернет речей

Багато IoT-систем не будуть обмежені безпечним простором будинку або офісу. Вони будуть розташовуватися в громадських місцях, в дуже віддалених областях, в рухомих транспортних засобах або навіть всередині людини. Інтернет речей - це величезна єдина мішень для будь-яких видів хакерських атак. Вже було виявлено нескінченна кількість направлених на IoT-пристрої навчальних атак, добре організованих зломів і навіть уразливостей в системі безпеки національного масштабу. Розробник IoT рішень повинен знати особливості таких вразливостей і способи їх усунення, стандартні заходи, спрямовані на захист Інтернету речей або будь-якого компонента мережі.

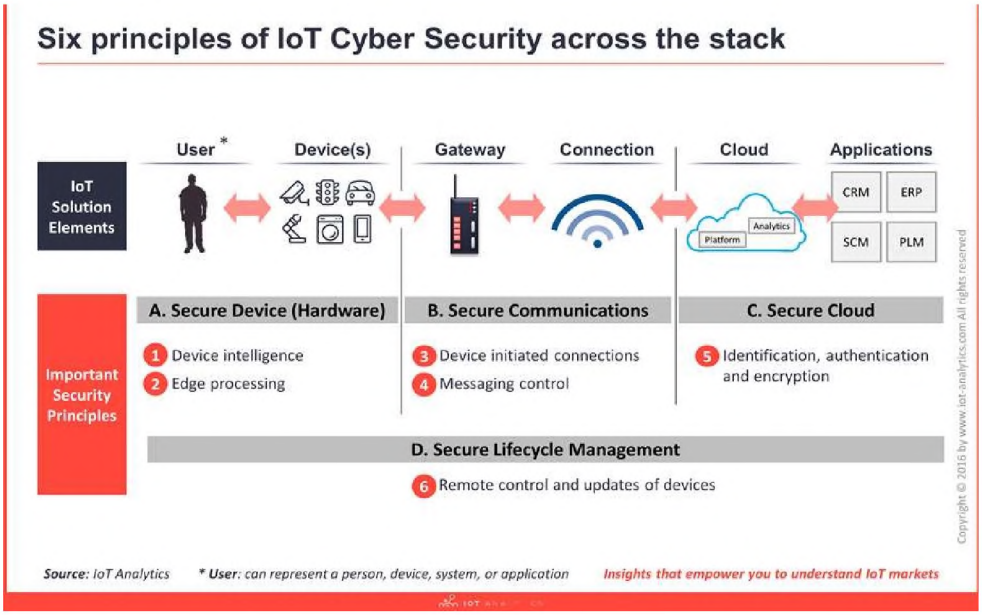

Рисунок 1.20 – Безпека в мережі IoT.

Найближчим часом різнорідні «острівці» рішень, швидше за все, будуть випереджати в своєму розвитку розгортання IoT-рішень, заснованих на функціонально-сумісних стандартах. Так йдуть справи з будь-якою новою технологією на етапі її зародження [3].

1.7 Постановка задачі

IoT речей та IIoT речей в промисловості - це величезна мішень для будь-яких видів хакерських атак. Вже було виявлено делика кількість направлених на IoT-пристрої навчальних атак, добре організованих зломів і навіть уразливостей в системі безпеки національного масштабу. Розробники IoT рішень повинені вивчати особливості таких вразливостей і способи їх усунення, стандартні заходи, спрямовані на захист Інтернету речей або будь-якого компонента мережі. Отже, передусім потрібно буде зробити наступне:

– розглянути стандарти сумістності IoT;

– дослідити малоресурсної криптографії для IoT пристроїв;

– розробити рекомендації з використання того чи іншого обладнення;

– розрахувати економічну еіективність від впровадженят того чи іншого рішення.

1.8 Висновки

Отже в наступному розділі необхідно освітити наступні питання:

- стандарти сумісності IoT;

- розглянути Еталонна модель IoT;

- розглянути IoT-шлюзи від компанії Eurotech, Intel, Huawei, Dell, Cisco та NEXCOM. Зробити акцент на особливостях використання того чи іншого рішеня;

- дослідити питаня використання малоресурсної криптографії для IoT пристроїв, переваги та недоліки цього рішення;

- провести розрахунок економічної доцільність використання;

- зробити висновки по отриманим результатам.

2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Стандарти сумісності IoT

Наприклад, Sutaria and Govindachari [4] відзначають, що дві характеристики мережевих IoT-пристроїв, що викликають найбільші проблеми, - це наявність пристроїв з низьким енергоспоживанням (розрахованих на роботу місяцями і роками без підзарядки) і частий обмін даними по мережах з втратою пакетів.

Нинішні стандартні протоколи Інтернету в цих умовах неоптимальні.

У більш широкому сенсі має місце дисбаланс між величезною кількістю пристроїв, що генерують дані з шаленою швидкістю в різних місцях, і використанням мережевих технологій і хмарних систем, які зберігають величезні обсяги даних в невеликій кількості локацій при відносно низькій швидкості оновлення даних.

Інтеграція цих двох класів систем для задоволення потреб користувачів вимагає певних можливостей від мережевих протоколів у всій архітектурі мережі і протоколів, від фізичного рівня до прикладного.

Над вирішенням цих питань працює кілька організацій і стандартизаційних форумів, прагнучі розширити або адаптувати протоколи Інтернету для пристроїв IoT. Основники організаціями є:

- Міжнародний союз електрозв'язку (International Telecommunication Union, ITU): 193 країни [5] і понад 700 членів по секторам і асоціаціям (науково-промислових підприємств, державних і приватних операторів зв'язку, радіомовних компаній, регіональних і міжнародних організацій).

- Всесвітній форум IoT (IoT World Forum, IWF): IBM, Intel, Cisco, Samsung.

- Національний інститут стандартів і технології Міністерства торгівлі США.

- Консорціум індустріального Інтернету (Industrial Internet Consortium,IIC): SAP, IBM, Intel, Fujitsu, General Electric, Oracle.

Для створення єдиної структури і класифікації необхідних функцій за їх місцем в стеку протоколів ряд цих груп також займається питанням формальної архітектури для IoT. У той час як існуючі стандарти та Інтернет зробили IoT можливим, в найближчому майбутньому навряд чи можлива поява стека нових стандартів, які доповнять або модифікують існуючі для сфери IoT.

Як і багато інших досягнень, що стали можливими завдяки Інтернету, IoT буде якийсь час стихійно розвиватися і проходити через процеси природного відбору, поки поступово не виявили життєздатні технології та механізми протоколів.

Але з урахуванням складності IoT має сенс створення архітектури, яка б специфікувала основні компоненти і їх взаємозв'язок. Архітектура IoT може надати такі переваги:

- дати адміністраторам мережі або IT-менеджеру корисний контрольний список для оцінки функціональності і повноти пропозицій від різних постачальників;

- служити орієнтиром для розробників в плані того, які функції потрібні в IoT і як вони взаємодіють;

- служити основою для стандартизації, стимулюючи сумісність і скорочення витрат.

Еталонна модель IoT від Міжнародного союзу електрозв'язку (МСЕ-Т) описана в Рекомендації Y.2060 [6]. На відміну від більшості інших еталонних моделей і архітектурних моделей, описаних в літературі, модель МСЕ-Т деталізує фактичні фізичні компоненти екосистеми IoT. Це корисно, тому що це зосереджує увагу на елементах екосистеми IoT, які повинні бути з'єднані, інтегровані, керовані і надані додаткам. Детальна специфікація екосистеми описує вимоги до можливостей IoT.

Один з важливих аспектів, який загострює модель, є той факт, що IoT на ділі не є мережею фізичних речей. Це скоріше мережа пристроїв, які з'єднано фізичними речами, разом з прикладними платформами - такими як

комп'ютери, планшети і смартфони, які взаємодіють з цими пристроями. Тому огляд моделі MCE-T необхідно почати з визначення пристроїв:

- Мережа зв'язку (Communication Network) - інфраструктурна мережа, що з'єднує пристрої та додатки, така як мережа на основі стека протоколів IP або Інтернет.

- Річ (Thing) - предмет фізичного світу (фізичні речі) або інформаційного світу (віртуальні речі), який може бути ідентифікований та інтегрований в мережі зв'язку.

- Пристрій (Device) - елемент обладнання, який володіє обов'язковими можливостями зв'язку та додатковими можливостями вимірювання, спрацьовування, а також введення, зберігання і обробки даних.

- Пристрій переносу даних (Data-carrying Device) - пристрій переносу даних підключається до фізичної речі і непрямим чином з'єднує цю фізичну річ з мережами зв'язку. Прикладами можуть служити активні мітки RFID.

- Пристрій збору даних (Data-capturing Device) - під пристроєм збору даних розуміється пристрій, що зчитує / записуючий пристрій, що має можливість взаємодії з фізичними речами. Взаємодія може здійснюватися непрямим чином за допомогою пристроїв перенесення даних або безпосередньо за допомогою носіїв даних, підключених до фізичних речей.

- Носій даних (Data Carrier) - безбатарейний об'єкт перенесення даних, підключений до фізичної речі і має можливість надавати інформацію придатному для цього пристрою збору даних. Ця категорія включає штрих-коди і QR-коди, наклеєні на фізичні речі.

- Сенсорний пристрій (Sensing Device) - пристрій, який може виявляти або вимірювати інформацію, що відноситься до навколишнього середовища, і перетворювати її в цифрові електричні сигнали.

- Виконавчий пристрій (Actuating Device) - пристрій, який може перетворювати цифрові електричні сигнали, що надходять від інформаційних мереж, в дії.

- Пристрій загального призначення (General Device) – пристрій загального призначення володіє вбудованими можливостями обробки і зв'язку і може обмінюватися даними з мережами зв'язку з використанням дротових або бездротових технологій. Пристрої загального призначення включають обладнання та прилади, які стосуються різних галузей застосування IoT, наприклад, верстати, побутові електроприлади і смартфони.

- Шлюз (Gateway) - елемент IoT, що з'єднує пристрої з мережами зв'язку.

Він виконує необхідну трансляцію між протоколами, що використовуються в мережах зв'язку і в пристроях.

Унікальним аспектом IoT, в порівнянні з іншими мережевими системами, очевидно є наявність безлічі фізичних речей і пристроїв, відмінних від обчислювальних пристроїв і пристроїв обробки даних.

На рисунку 2.1, адаптованому з Рекомендації Y.2060, зображені типи пристроїв в моделі MCE-T. Модель розглядає IoT як мережу пристроїв, тісно пов'язаних з речами. Сенсорні і виконавчі пристрої взаємодіють з фізичними речами в навколишньому середовищі. Пристрої збору даних зчитують дані з фізичних речей або записують дані на фізичні речі шляхом взаємодії з пристроями перенесення даних або носіями даних, підключеними або пов'язаними з фізичним об'єктом тим чи іншим чином.

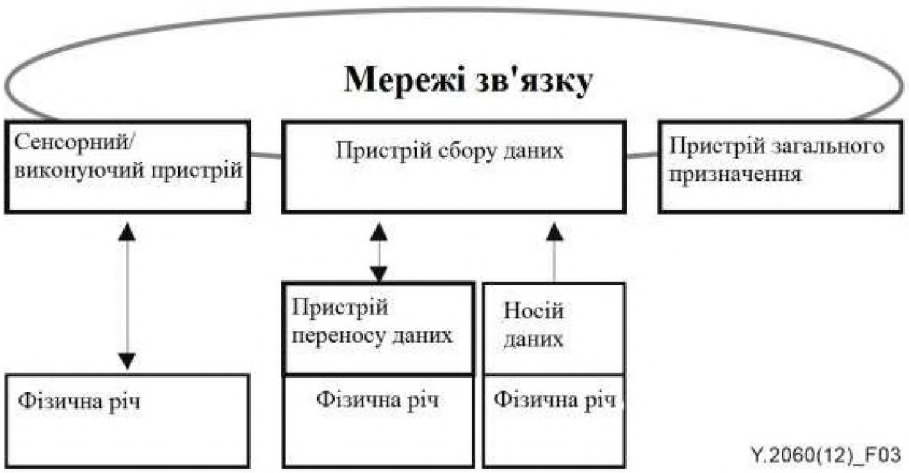

Рисунок 2.1. Типи пристроїв та їх взаємозв’язок із фізичними речами

Ця модель показує відмінність між пристроями перенесення даних і носіями даних. Пристрій переносу даних є пристроєм в сенсі Рекомендації Y.2060. Як мінімум, пристрій завжди має можливості зв'язку і може мати інші електронні можливості. Прикладом пристрою перенесення даних є RFID-мітка. У той же час носій даних - це елемент, приєднаний до фізичної речі з метою ідентифікації або інформування.

В рекомендації Y.2060 відзначається, що технології, які використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження. Приклади кожної з них:

- Радіочастотні: радіочастотні ідентифікаційні (RFID) - бірки, або радіопозначки.

- Оптичні: штрих-коди і QR-коди можуть служити прикладами ідентифікаційних носіїв даних, які зчитуються оптично.

- Інфрачервоні: інфрачервоні мітки, що можна використовувати в Збройних Силах, лікарнях та інших середовищах, де потрібно відстежувати розташування і переміщення персоналу. Це можуть нашивки на військовій формі, що відбивають світло, і такі, що працюють від батарейок та випромінюють ідентифікуючу інформацію.

Останні можуть мати кнопку, при натисканні якої бейдж може використовуватись для проходу через автоматичні контрольні пункти, або ж бейджи, що автоматично повторюють сигнал для контролю за переміщеннями персоналу.

Пульти дистанційного керування, що використовуються в побуті або в інших середовищах для управління електронними пристроями, теж можна легко інтегрувати в IoT.

- Гальванічне збудження: прикладом можуть служити медичні імпланти, які використовують електропровідні властивості людського тіла [7]. В ході комунікації між імплантом і поверхнею гальванічна пара передає сигнали з імпланта на електроди, виведені на шкіру. Ця схема використовує

дуже мало енергії, що дозволяє знизити розмір і складність імплантованого пристрою.

Останнім типом пристроїв з рисунку є пристрої загального призначення.

Вони володіють можливостями обробки даних і зв'язку, які можуть бути інтегровані в IoT. Хорошим прикладом є технологія «розумного будинку», яка може інтегрувати практично будь-який пристрій в будинку в мережу для централізованого або дистанційного керування.

В Рекомендації Y.2060 наведено огляд елементів, задіяних в IoT. Розглядаються різні способи зв'язку з фізичними пристроями. Передбачається, що одна або кілька мереж підтримують зв'язок між пристроями.

В рекомендації особливу увагу приділено такому простою, пов'язаному з IoT: шлюзу. Як мінімум шлюз працює транслятором між протоколами. Шлюзи вирішують одну з головних проблем при проектуванні IoT, а саме проблему сумісності, як між різними пристроями, так і між пристроями та Інтернетом або корпоративною мережею.

«Розумні» пристрої підтримують широкий спектр бездротових і дротових технологій передачі даних і мережевих протоколів. Крім того, можливості обробки даних у таких пристроїв, як правило, обмежені.

Рекомендація Y.2067 [5] закріплює вимоги до шлюзів IoT, які зазвичай розпадаються на три категорії:

- Шлюз підтримує різні технології доступу до пристроїв, дозволяючи пристроїв обмінюватися даними один з одним і з мережею Інтернет або корпоративною мережею, що містить додатки IoT. Такі схеми доступу можуть, наприклад, включати ZigBee, Bluetooth і Wi-Fi.

- Шлюз підтримує необхідні мережеві технології як для локальних, так і для глобальних мереж. Ці технології можуть включати в себе Ethernet і Wi-Fi на території організації, а також стільниковий зв'язок, Ethernet, DSL і кабельний доступ до Інтернету і глобальним корпоративним мережам.

- Шлюз підтримує взаємодію з додатками, управління мережею і функції безпеки.

Дві перших вимоги включають в себе трансляцію протоколів між різними мережевими технологіями і стеками протоколів.

Третя вимога зазвичай називається функцією IoT-агента. По суті, IoT-агент надає функціональність високого рівня від імені IoT-пристроїв, таку як організація або резюмування даних з декількох пристроїв для передачі в IoT-додатки, забезпечення протоколів і функцій безпеки і взаємодія з системами управління мережею.

Термін «мережа зв'язку» прямо не визначається в серії IoT-стандартів Y.206x. Мережа (або мережі) зв'язку підтримує зв'язок між пристроями і може безпосередньо підтримувати прикладні платформи. Вона може мати розміри невеликого IoT, такого як домашня мережа

«розумних» пристроїв. У більш загальному сенсі мережу (або мережі) пристроїв з'єднується з корпоративними мережами або Інтернетом для зв'язку з системами додатків і серверами, на яких розташовані бази даних, пов'язані з IoT.

В рекомендації розглядаються також можливості зв'язку пристроїв між собою.

- Перша можливість - зв'язок між пристроями через шлюз. Наприклад, за допомогою шлюзу сенсорне або виконавчий пристрій з підтримкою Bluetooth може здійснювати зв'язок з пристроєм збору даних або пристроєм загального призначення, що використовують Wi-Fi.

- Друга можливість - зв'язок по мережі зв'язку без шлюзу. Наприклад, якщо всі пристрої в мережі «розумного будинку» підтримують Bluetooth, вони можуть управлятися з комп'ютера, планшета або смартфона з підтримкою Bluetooth.

- Третя можливість - прямий зв'язок пристроїв між собою за окремою локальної мережі, в той час як зв'язок із зовнішньою мережею (на малюнку не показана) здійснюється через шлюз LAN.

Кожна фізична річ в Інтернеті речей може бути представлена в інформаційному світі однією або декількома віртуальними речами, але при цьому віртуальна річ може існувати без відповідної фізичної речі. Фізичні речі зіставлені віртуальним речам, що зберігаються в БД і інших структурах даних. Додатки обробляють віртуальні речі і працюють з ними.

Рисунок. 2.2. Еталона модель IoT за рекомендацією Y.2060

Еталонна модель IoT від МСЕ-Т складається з чотирьох рівнів плюс можливості управління і безпеки, що діють між рівнями. До сих пір ми говорили про рівень пристрою. У термінах функціональності зв'язку рівень пристрою включає в себе, грубо кажучи, фізичний і канальний рівні OSI.

Рівень мережі виконує дві базові функції. Можливості мережі відносяться до взаємодії пристроїв і шлюзів. Транспортні можливості відносяться до транспорту інформації служб і додатків IoT, а також інформацією управління і контролю IoT.

Грубо кажучи, ці можливості відповідають мережевому і транспортному рівням OSI.

Рівень підтримки послуг і підтримки додатків надає можливості, які використовуються додатками. Багато різноманітних додатків можуть використовувати загальні можливості підтримки. До прикладів належать спільне опрацювання даних і управління БД. Спеціалізовані можливості

підтримки – це конкретні можливості, які призначені для задоволення потреб конкретного підмножини додатків IoT.

Рівень додатку складається з усіх додатків, взаємодіючих з IoT-пристроями.

Рівень можливостей управління охоплює традиційні функції управління мережею, тобто управління несправностями, управління конфігурацією, управління обліком, управління показниками роботи і управління безпекою.

В Рекомендації Y.2060 як приклади загальних можливостей управління перераховані:

- управління пристроями: приклади включають виявлення пристроїв, автентифікацію, дистанційну активацію і дезактивацію пристроїв, конфігурацію, діагностику, оновлення прошивки або ПЗ, управління робочим статусом пристрою;

- управління топологією локальної мережі: прикладом є управління конфігурацією мережі;

- управління трафіком і перевантаженнями: наприклад, виявлення умов перевантаженості мережі і реалізація резервування ресурсів для термінових або життєво важливих потоків трафіку.

Спеціалізовані можливості управління тісно пов'язані з вимогами додатків, наприклад, вимогами з контролю лінії передачі електроенергії в «розумній» електромережі.

Рівень можливостей забезпечення безпеки включає загальні можливості забезпечення безпеки, які не залежать від додатків. В Рекомендації Y.2060 приклади загальних можливостей забезпечення безпеки включають:

- На рівні програми: авторизацію, автентифікацію, захист конфіденційності і цілісності даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист;

- на рівні мережі: авторизацію, автентифікацію, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;

- на рівні пристрою: автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами додатків, наприклад, вимогами безпеки мобільних платежів.

Еталонна модель від Всесвітнього форуму IoT

Всесвітній форум IoT World Forum - щорічна подія, що спонсорується галуззю та об'єднує представників бізнесу, державних структур та вузівської науки з метою просування IoT на ринок.

Комітет з архітектури Всесвітнього форуму IoT, складений з лідерів індустрії, включаючи IBM, Intel та Cisco, в жовтні 2014 опублікував еталонну модель IoT. Ця модель є загальною структурою, покликаною допомогти галузі прискорити розгортання IoT.

Модель призначена для того, щоб стимулювати співпрацю та сприяти створенню повторюваних моделей впровадження.

Ця еталонна модель є корисним доповненням до моделі MCE-T. Документи MCE-T роблять упор на рівнях пристрою та шлюзу, описуючи верхні рівні лише в загальних рисах. І дійсно, в Рекомендації Y.2060 увесь опис рівня додатку вмістився в одну фразу. Найбільше уваги рекомендації серії Y.206x приділяють визначенню концепції для підтримки розробки стандартів взаємодії з пристроями IoT.

IWF стурбований більш масштабним питанням розробки додатків, проміжного програмного забезпечення і функцій підтримки для корпоративного Інтернету речей. Запропонована семирівнева модель зображена на рисунку 2.3.

Рисунок. 2.3. Еталонна модель від Всесвітнього форуму IoT

Документальний опис моделі IWF, опублікований Cisco [7], вказує, що розроблена модель відрізняється наступними характеристиками:

- спрощує: допомагає розбити складні системи на частини так, щоб кожна з цих частин стала більш зрозумілою;

- прояснює: надає додаткові відомості для точної ідентифікації рівнів IoT і вироблення загальної термінології;

- ідентифікує: ідентифікує аспекти, в яких ті чи інші типи обробки оптимізовані в різних частинах системи;

- стандартизує: є першим кроком до того, щоб постачальники могли створювати продукти IoT, здатні взаємодіяти один з одним;

- організовує: робить IoT реальним і доступним, а не просто абстрактною концепцією.

Рівень 1 утворюють фізичні пристрої та контролери, які можуть керувати кількома пристроями. Рівень 1 моделі IWF приблизно відповідає рівню пристрою в моделі MCE-T . Як і в моделі MCE-T, елементи на цьому рівні – не фізичні речі як такі, а пристрої, які взаємодіють з фізичними речами, такі як сенсорні і виконавчі пристрої. Серед інших можливостей ці пристрої можуть вміти здійснювати аналого-цифрове і цифро-аналогове перетворення, генерацію даних, а також підтримувати дистанційний опитування або дистанційне керування.

Рівень 2 моделі IWF приблизно відповідає рівню мережі в моделі MCE-T. Основна відмінність в тому, що модель IWF відносить шлюзи до рівня 2, в

той час як в моделі MCE-T вони відносяться до рівня 1. Оскільки шлюз є мережевим пристроєм і пристроєм зв'язку, віднесення його до рівня 2 має більше сенсу.

З логічної точки зору цей рівень реалізує зв'язок пристроїв між собою і між пристроями і низькорівневою обробкою на рівні 3. З фізичної точки зору цей рівень складається з мережевих пристроїв, таких як маршрутизатори, комутатори, шлюзи і брандмауери, що використовуються для створення локальних і глобальних мереж і підключення до Інтернету.

Цей рівень дозволяє пристроям здійснювати зв'язок один з одним і за допомогою більш високих логічних рівнів обмінюватися даними з прикладними платформами, такими як комп'ютери, пристрої дистанційного управління і смартфони.

У багатьох впроваджуваних системах IoT розподілена мережа датчиків може генерувати великі обсяги даних. Наприклад, офшорні нафтові родовища і нафтопереробні заводи можуть генерувати до терабайта даних щодня. Літак може генерувати кілька терабайт даних на годину. Замість того, щоб зберігати всі ці дані постійно (або хоча б довгий час) в централізованому сховищі, доступному для додатків IoT, часто більш доцільно виконувати якомога більшу частину обробки даних якомога ближче до датчиків. Тому завданням рівня периферійних обчислень (edge computing level) (рівень 3) є перетворення мережевих потоків даних в інформацію, придатну для зберігання і більш високорівневої обробки. Елементи обробки на цьому рівні можуть мати справу з великими обсягами даних і виконувати операції перетворення даних, в результаті яких зберігати доводиться вже набагато менший обсяг.

Опублікований Cisco документ по моделі IWF [7] містить такі приклади операцій на рівні периферійних обчислень:

- аналіз: аналіз даних по критеріях того, чи підлягають вони обробці на більш високому рівні;

- форматування: переформатування даних для однакової високорівневої обробки;

- розархівування / декодування: обробка криптографічних даних з додатковим контекстом (таким як походження);

- дистиляція / скорочення: скорочення або резюмування даних для того, щоб мінімізувати обсяг даних, трафік в мережі і в високорівневих системах обробки;

- оцінка: визначення того, чи становлять дані порогове значення або аварійний сигнал; цей процес повинен включати перенаправлення даних додатковим одержувачам.

Елементи обробки на цьому рівні відповідають пристроїв загального призначення в моделі MCE-T. Як правило, вони розгортаються фізично на краю мережі IoT, тобто поруч з сенсорами і іншими пристроями генерації даних. Таким чином, частина базової обробки великих обсягів генеруються даних знімається з прикладних програм IoT, розташованих центрально.

Обробка на рівні периферійних обчислень іноді називається туманними обчисленнями. Туманні обчислення і туманні служби, як очікується, стануть відмінною характеристикою IoT. Цей принцип проілюстрований на рисунку. 2.4.

Туманні обчислення представляють в сучасних мережевих технологіях тренд, протилежний хмарних обчислень. У хмарні обчислення великий обсяг централізованих ресурсів зберігання і обробки даних доступний розподіленим споживачам за допомогою хмарних мережевих структур для відносно невеликого числа користувачів.

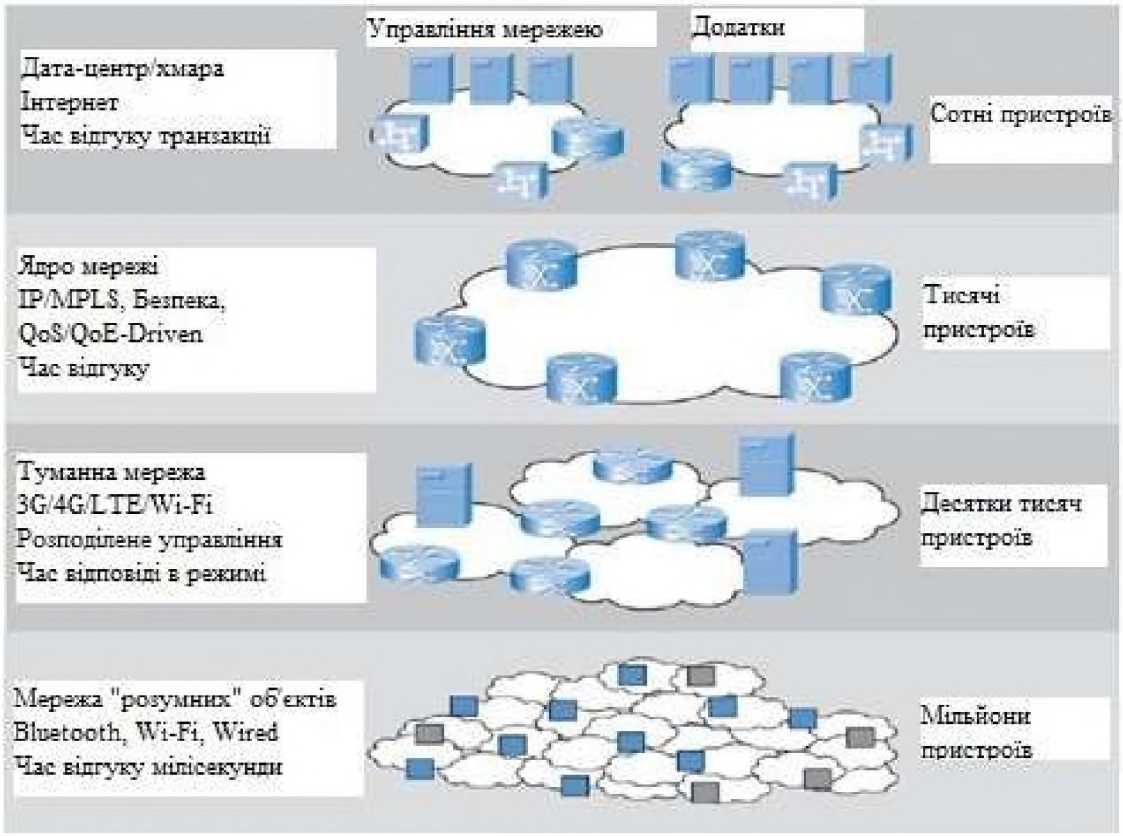

Рисунок. 2.4. Туманні обчислення

В туманних обчисленнях велике число окремих інтелектуальних об'єктів здійснюють зв'язок з туманними мережевими структурами, які здійснюють обчислення і зберігають ресурси поруч з периферійними пристроями в IoT.

Туманні обчислення вирішують проблеми, що виникли внаслідок діяльності тисяч або мільйонів «розумних» пристроїв, включаючи проблеми безпеки, конфіденційності, обмежених можливостей мережі і затримки. Термін «туманні обчислення» обраний тому, що туман стелиться по землі, в той час як хмари знаходяться високо в небі.

На рівні 4, рівні накопичення даних, дані, що надійшли з різних пристроїв, профільтровані і оброблені рівнем периферійних обчислень, поміщаються в сховище, де будуть доступні для більш високих рівнів. Цей рівень разюче відрізняється і від низькорівневих (туманних), і від високорівневих (хмарних) обчислень за особливостями конструкції, вимогам і методам обробки.

Дані, що проходять крізь мережу, називаються «даними в русі» [8]. Швидкість і організація даних в русі визначається пристроями, що генерують дані. Генерація даних відбувається по подіям, або періодично, або по виникненні якої-небудь події в середовищі. Для збору даних та їх обробки необхідно реагувати на їх появу в реальному часі. Навпаки, багатьом додаткам не потрібно обробляти дані зі швидкістю мережевої передачі. На практиці ні хмарна мережу, ні прикладні платформи не змогли б встигати за обсягами даних, що генеруються величезною кількістю IoT-пристроїв. Замість цього додатки мають справу з «даними в спокої», тобто даними в тому чи іншому легкодоступному сховище. Додатки можуть звертатися до даних у міру необхідності або поза режимом реального часу. Таким чином, високі рівні функціонують за принципом транзакцій, в той час як три нижніх рівні працюють по подіях.

Нижче перераховані названі в [8] операції, що виконуються на рівні накопичення даних:

- перетворення «даних в русі» в «дані в спокої»;
- перетворення формату з мережевих пакетів в реляційні таблиці БД;
- перехід від обчислень щодо подій до обчислень за запитом;
- значне зниження обсягу даних за рахунок фільтрації і вибіркового зберігання.

Ще один погляд на рівень накопичення даних полягає в тому, що він являє собою кордон між інформаційними технологіями IT, під якими розуміється цілий спектр технологій обробки інформації, включаючи ПЗ, обладнання, технології зв'язку і супутні служби, і операційними технологіями OT, що представляють собою обладнання і ПЗ, які виявляють або викликають зміни шляхом прямого моніторингу або контролю фізичних пристроїв, процесів і подій на підприємстві.

Рівень накопичення даних вбирає велику кількість даних і поміщає їх в сховище, практично не пристосовуючи до потреб конкретних програм або груп додатків. З рівня периферійних обчислень в сховище може надходити

безліч різних видів даних в різних форматах і від різнорідних оброблювачів. Рівень абстракції (рівень 5) даних може агрегувати і форматувати такі дані способами, які роблять доступ додатків більш керованим і ефективним. У числі пов'язаних завдань можуть бути наступні:

-Комбінування даних з різних джерел, включаючи вивірку кількох форматів даних.

-Виконання необхідних перетворень для забезпечення однакової семантики даних з різних джерел.

-Приміщення відформатованих даних у відповідну базу даних, наприклад, великі обсяги повторюваних даних поміщаються в систему великих даних, таку як Hadoop. Дані подій направляються в реляційну СУБД, що відрізняється більш швидким часом реакції і адекватним інтерфейсом для таких типів даних.

- Оповіщення додатків більш високого рівня про те, що дані заповнені або досягнутий певний рівень даних.

- Консолідація даних в одному місці ETL, ELT або надання доступу до декількох джерел даних шляхом віртуалізації даних.

- Захист даних шляхом відповідної автентифікації і авторизації.

- Нормалізація / денормалізація і індексація даних для швидкого доступу додатків.

Рівень 6 (рівень додатку) містить додатки будь-якого типу, що використовують дані IoT на вході або керуючі IoT-пристроями. Як правило, додатки взаємодіють з рівнем 5 і з даними в спокої, тому їм не обов'язково функціонувати на швидкостях мережі.

Слід передбачити спрощений режим роботи, який дозволить додаткам минути проміжні рівні і безпосередньо взаємодіяти з рівнем 3 або навіть рівнем 2. Модель IWF не визначає додатки по всій строгості, вважаючи цей аспект виходять за рамки дискусії про модель IWF.

Рівень взаємодії і процесу (рівень 7) з'явився в результаті визнання того, що IoT буде корисний лише тоді, коли з ним зможуть взаємодіяти

люди. Цей рівень може включати кілька додатків і обмін даними і / або керуючої інформацією по Інтернету або корпоративної мережі.

IWF вважає еталонну модель IoT прийнятої в галузі базовою структурою, спрямованої на стандартизацію концепцій і термінології, пов'язаних з IoT.

Що ще більш важливо, модель IWF визначає необхідний функціонал і проблеми, які потрібно вирішити до того, як галузь зможе реалізувати цінність IoT.

2.2 Шлюзи IoT від компанії Eurotech

Компанія Eurotech в першу чергу відома своєю хмарної IoT платформою Everyware, яка покликана спростити адміністрування пристроїв і керування даними, забезпечуючи підключення розподілених пристроїв через захищені хмарні сервіси. Використовуючи цю платформу, замовники можуть відслідковувати, конфігурувати свої пристрої і керувати ними протягом всього життєвого циклу.

Широка лінійка шлюзів містить як компактні пристрої з низьким енергоспоживанням, так і високопродуктивні вбудовані ПК з широким функціональним набором.

Пристрої серій ReliaGATE 10-20, ReliaGATE 10-11 і ReliaGATE 10-05 можуть служити малопотужним шлюзом для легких промислових застосувань. Їх основні функції - агрегування даних, одержуваних з польових пристроїв, перетворення повідомлень і протоколів, маршрутизація пакетів, організація двобічного зв'язку з хмарним сервером, де дані збираються, зберігаються і обробляються за допомогою бізнес-додатків.

Шлюзи серій ReliaGATE 20-25, ReliaGATE 20-26, DynaGATE 15-10 пропонують додаткові можливості по обробці і зберіганню даних для надання послуг в автономному режимі, а при підключенні до хмарних додатків забезпечують контроль і управління в реальному часі. Вони часто

застосовуються для виконання аналітичних функцій або завдань попередньої обробки, зокрема для передачі даних, що відповідають заданим параметрам.

Практично всі шлюзи, крім ReliaGATE 20-26, який використовує Red Hat Linux, поставляються з попередньо встановленою операційною системою Yocto Linux. Велика частина шлюзів забезпечується програмним забезпеченням Everyware Software Framework (ESF) на базі Eclipse Kura і Java/OSGi. Крім того, в якості шлюзів можуть виступати і процесорні плати в різних форм-факторах, на які також встановлюється спеціалізоване програмне рішення. ESF - це промислова версія Eclipse Kura (версія з відкритим вихідним кодом) з додатковими можливостями з безпеки, діагностики, конфігурації і віддаленого доступу, повністю інтегрована в платформу Everyware Cloud. ESF/Kura дозволяє розробникам зосередити свою увагу на аналітиці та специфіці додатків і полегшити контроль і управління роботою шлюзу (змінювати параметри в реальному часі, оновлювати ПЗ, робити моніторинг пристрою, діагностику, забезпечувати безпеку і т. д.) [9].

2.3 Шлюзи IoT компанії Intel

Шлюзи Intel для IoT дуже різноманітні і здатні задовольнити розробників проектів будь-якої складності. Їх оснащують процесорами Quark, Atom, Core, Xeon.

Шлюзи на базі Intel Quark, засновані на платі Intel Galileo, є гнучким, малопотужним і недорогим рішенням для організації нескладних обчислень іінтеграції пристроїв IoT. Процесори Intel Atom і Intel Core останніх поколінь забезпечують більш високу продуктивність, хорошу графіку і багату інтеграцію введення-виведення.

Сімейство Intel Xeon допомагає створювати шлюзи для інфраструктури з обчисленнями в пам'яті, аналізу в режимі реального часу, підвищеною оперативністю і безпекою. Шлюзи оснащують сховищами даних і

оперативною пам'яттю, які відповідають вимогам процесора і призначень пристроїв.

Шлюзи технології Intel IoT Gateway випускаються більш ніж десятком фірм. Вони забезпечуються засобами для створення власних додатків первинної обробки даних, збору даних з безлічі пристроїв, функціями перетворення протоколів і керування різними пристроями. Шлюзи Intel для IoT можуть підтримувати різні операційні системи, включаючи Windows 10 IoT і кілька мов програмування.

Більшість моделей поставляється з встановленою ОС Wind River Linux, в якій передбачений захист пристроїв від внутрішнього або зовнішнього несанкціонованого доступу. При цьому, в області захисту даних, тут є шифрування і безпечний обмін інформацією з зовнішніми системами.

У Wind River Linux в систему вбудовано керуюче ПО, яке дозволяє управляти не тільки локальними, але і віддаленими пристроями. Контролювати їх можна або вручну, або в автоматичному режимі, ґрунтуючись на критеріях, заданих адміністраторами і програмістами. Крім того, підтримка платформ Wind River Helix Device Cloud і Wind River Helix App Cloud, дають великі можливості по управлінню пристроями, додатками і хмарними сервісами.

Шлюзи Intel володіють великими мережевими можливостями. Вони можуть підключатися відразу до двох локальних дротових мереж, одночасно працювати в декількох Wi-Fi-мережах, і, не перериваючи зв'язок, взаємодіяти зі спеціалізованими пристроями, використовуючи інші типи мереж.

Різноманітність підтримуваних мережевих інтерфейсів дозволяє рішенням для IoT створювати мережі на базі технологій Bluetooth, ZigBee, 6LoWPAN і ін., підключатися до хмарних сервісів, організовувати різні схеми управління. У список підтримуваних мережевих інтерфейсів входять і мобільні мережі: GPRS, 2G, 3G. LTE [10].

2.4 Шлюзи IoT компанії Huawei

У компанії Huawei є цілий спектр продуктів, який формує середовище передачі, зберігання і обробки даних IoT за допомогою різних аналітичних систем. Шлюзи серії AR від Huawei працюють як високопродуктивні маршрутизатори IoT, і особливо підходять для відеоспостереження, виробництва, транспортування, електропостачання та інших зовнішніх операцій. Лінійка дуже різноманітна и може задовольнити будь-які потреби як у плані обчислювальної здатності, так і у вимогах до різноманітних інтерфейсів підключення. Легкість зв'язку із речами та шлюзами забезпечується платформою IoT Connection Management Platform.

У лінійки в наявності є безліч типів інтерфейсів, які підходять до різноманітних терміналів. Шлюзи підтримують різні протоколи бездротового зв'язку: Wi-Fi, ZigBee, Bluetooth та RF. Також наявна підтримка сотового зв'язку у мережах GSM, 3G та 4G/LTE, що разом із підтримкою GPS робить шлюз працездатним при перегонах транспорту. Маршрутизація трафіку може бути гнучко налаштована політикою маршрутизацій, статичними маршрутами та підтримкою динамічних протоколів RIP, OSPF, IS-IS, BGP. Підтримується перетворення різних галузевих протоколів та побудова єдиної мережевої платформи.

У лінійці використанні високопродуктивні ARM процесори, що доповнюються великими об'ємами постійної пам'яті, в якості операційної системи використовується Wind River LINUX. Підтримка віртуалізації і можливість гнучкої масштабованої інтеграції додатків прискорюють розгортання послуг. Платформа надає управління повним життєвим циклом ІКТ-ресурсів: розгортання, моніторинг видалення додатків через Agile Controller.

Платформа від Huawei надає зручне та об'єднане управління терміналами, шлюзами, програмами та даними. Запуск розгортання можна запустити всього лиш відсканувавши серійний номер пристрою (ESN). Це дозволяє дуже швидко вводити пристрої у експлуатацію. Завдяки

уніфікованій системі керування мережею (NMS), пристрої можна об'єднувати в певні групи та масово ними керувати. Є можливість встановлення ПЗ із USB-накопичувача та майже моментальний початок користування завдяки функції «plug-and-play».

Безпека підтримується міжмережевим екраном із поділом на зони та відстеженням стану, автентифікацією на основі 802.1X та автентифікацією по MAC-адресі та веб- автентифікація. Наявний захист ARP і захист від атак ICMP. Додаткова безпека досягається завдяки відстеженню пакетів DHCP і відстеженню пакетів DHCPv6 CPCAR, чорному списку і відстеженню джерела атаки PKI і KPM [11].

2.5 Шлюзи IoT компанії Cisco та NEXCOM

Зокрема, компанія пропонує шлюзи, комутатори промислового класу і вбудовуються маршрутизатори для IoT з підтримкою платформи туманних обчислень IOx. IOx - це середа для додатків, яка допомагає мережевим пристроям, які її підтримують, контролювати і управляти пристроями IoT. Ця середа поєднує в собі найпопулярнішу відкриту ОС Linux, мережеву ОС Cisco IOS та потужні сервіси для швидкої та надійної інтеграції із сенсорами IoT, що дозволяє клієнтам створювати і запускати програми безпосередньо на промислових мережевих пристроях Cisco. Компанія Cisco створює та підтримує відкрите середовище для заохочення розробників переносити існуючі програми та створювати нові в різних галузях промисловості.

Компанія Cisco створює шлюзи для різноманітних вертикалей ринку: промисловість, енергозабезпечення, транспорт та логістика, розумні міста, навчання, охорона здоров'я та ін.

Також існує лінійка безпровідних шлюзів для мереж пристроїв LoRaWAN, що складається зі шлюзів IXM-LPWA-800-16-K9 (підтримує частоти 863–870 МГц) та IXM- LPWA-900-16-K9 (підтримує частоти 902–928 МГц). Цей тип зв'язку забезпечує M2M взаємодію на відстанях до 15 км при мінімальному енергоспоживанні, що забезпечує декілька років автономної

роботи на одному акумуляторі AA. Вони підтримують до 16 каналів LoRa та захищені по стандарту IP67. Ці шлюзи вкрай зручні при використанні на рухомих об’єктах в автономному режимі роботи, а за рахунок волого- та пилозахищеності не потребують додаткових захисних коробів.

Широкий вибір маршрутизаторів у промисловому виконанні забезпечує функціональні можливості корпоративного класу, включаючи високоякісну передачу даних, можливості голосового та відео зв'язку зі стаціонарними і мобільними вузлами мережі через дротові та бездротові канали зв'язку. Маршрутизатори Cisco надають доступну функціональність, що необхідна при створенні корпоративних рішень:

- динамічний багатоточковий VPN (DMVPN);
- аналіз якості обслуговування (QoS) для стільникового зв'язку;
- мульти-віртуальна переадресація маршрутів (VRF) для стільникового зв'язку;

Cisco IOx для маршрутизаторів 809 і 829, що забезпечує виконання граничного додатків в мережах IoT Основною лінійкою IoT шлюзів від Cisco є Cisco 800, які позиціонуються як маршрутизатори промислової інтегральної мережі. На шлюзах Cisco встановлена операційна система Cisco IOS, що забезпечує просте управління, дає змогу створювати еластичні комунікації та підтримувати високий рівень безпеки. Всі маршрутизатори серії 800 мають інтегроване 4G/LTE бездротове з'єднання WAN та підтримують більш старі версії стільникового зв’язку. Дві зовнішні антени забезпечать максимально якісний зв’язок, а дві різні, одночасно активні, SIM карти допоможуть підтримувати зв’язок різних операторів в залежності від якості сигналу.

Багатогалузева сертифікація шлюзів Cisco надає їм перевагу у корпоративних рішеннях, де велика увага приділяється надійності постачальника [12].

Стратегія Cisco в області IoT будується на шести стовпах технології: рішення з передачі даних в IoT-мережі, прикладна середу IOx і fog-додатки, а також IT- безпека, аналітика даних, засоби автоматизації та підтримка

додатків. Саме Cisco ввів поняття туманних обчислень та Інтернету всього (IoE, Internet of Everything).

Серія NEXCOM CPS складається зі шлюзів IoT, готових до застосування, які легко встановлювати та налаштовувати. Заздалегідь встановлена за допомогою NEXCOM Industrial IoT Studio допоможе полегшити розробку додаткового ПЗ. У лінійки наявна широка підтримка різноманітних операційних систем. Відтак на шлюзи можуть бути встановленні Windows 10 IoT, Ubuntu 14.04, FreeRTOS та інші Linux системи.

Встановлені процесори Intel Atom надають достатню потужність для обробки даних на краю при цьому мають гарну енергоефективність. Для більш потужних обчислень можна обрати моделі із використанням повноцінних та більш енергоємних процесорів Intel Celeron. Вид жорсткого диску та його об'єм варіюється від 16 ГБ e-MMC до 128 ГБ SSD із підтримкою порту розширення SD карткою.

Серія CPS може витягувати та аналізувати дані PROFIBUS, PROFINET та Ethernet, надсилати попереджувальні повідомлення, зберігати дані в локальні та віддалені бази даних та виконувати інші функції обробки даних після декількох кліків мишею. Серія CPS також підтримує API хмарних інтерфейсів для підключення до хмарних серверів через бездротові 3G/Wi-Fi (додатковий модуль) та/або дротові локальні мережі. За допомогою серії CPS виробники можуть изначати потоки даних, завантажувати дані з кінцевих пристроїв у платформи хмарної служби, включаючи Microsoft Azure та IBM Bluemix.

Завдяки надійному дизайну, серія CPS може бути встановлена поряд з PLC, датчиками та пристроями вводу-виводу в жорстких середовищах. На зосередженість у сфері промисловості та транспорту вказує захист від вібрацій та ударів, а також можливість роботи в температурному діапазоні від -20°C до +65°C при високій вологості [13].

2.6 Шлюзи IoT компанії Dell

Компанія Dell просуває свої шлюзи серії Edge Gateway як економічне за витратами рішення підвищеної надійності, призначене для агрегації, передачі даних і організації їх аналізу безпосередньо на периметрі мережі. Компанія пропонує два модельних ряди - Edge Gateway серія 5000 і Edge Gateway серії 3000.

Шлюзи серії 5000 передбачають модульне розширення, орієнтовані на стаціонарні системи, великі сенсорні мережі і більш серйозну аналітику в прикордонних сегментах IoT мережі. Серія 3000 ідеально підходить як для фіксованих, так і мобільних варіантів використання, які потребують менших сенсорних мереж, менше місця, а також більш просту аналітику.

Віддалене управління може здійснюватися для платформи WindRiver за допомогою Helix Device Cloud або Windows IoT Industry, а для Snappy Ubuntu - Dell Cloud Client Manager (CCM) або Dell Client Command Suite, Шлюзи серії 5000 є ідеальною платформою для засобів інтеграції внутрішніх даних і аналітики від компанії Dell, також вони сумісні зі сторонніми рішеннями, в тому числі від сертифікованих незалежних постачальників ПЗ з числа партнерів компанії Dell. Захист мережевої периферії і датчиків забезпечується завдяки вбудованим засобам IT-безпеки Dell.

Універсальна підсистема вводу-виводу, яку легко розширити, дозволяє підключати, об'єднувати, передавати і відслідковувати дані з використанням практично будь-яких датчиків і мережевих протоколів від успадкованих протоколів (BACNet, Modbus і CANbus) до сучасних мереж (Zigbee, 6LoWPAN і Z- Wave). Мережеві можливості шлюзів підтримуються двома портами Gigabit Ethernet і модулями 802.11n Wi-Fi, Bluetooth Low Energy, модулем зв'язку 3G або LTE.

Серія 3000 включає три моделі, які призначені для використання в якості вбудованих рішень в сфері промислової автоматизації, енергетики, транспорту і в системах цифрових табло. Вони дозволяють безпечно

передавати важливі дані про функціонування фізичного обладнання на периферії мережі в реальному часі.

Опціональне ПЗ Dell Edge Device Manager (EDM) допомагає з легкістю управляти віддаленими пристроями і гарантувати безпеку кожного з них.

Крім того, кожна модель шлюзів лінійки орієнтована на певну область застосування за рахунок додаткових можливостей. Модель 3001 орієнтована на застосування в сучасних виробничих середовищах, тр анспортних системах і периферійних мережах. Багатофункціональний порт GPIO (8-канальний) і програмовані послідовні порти (2 x RS- 232, RS-422 або RS-485) дозволяють працювати з успадкованими системами, а також розширюють можливості підключення. Є можливість вибору ОС - Ubuntu Core 16.0 і Microsoft Windows 10 IoT. Модель 3002 орієнтована на застосування на транспорті і в логістиці.

Стійкість до перебоїв живлення, підтримка інтерфейсу CANbus, наявність вбудованих адаптерів ZigBee дозволяє організувати стабільний зв'язок з самими різними системами і датчиками на різних видах транспорту. Модель 3003 розроблена для установки в цифрових табло і терміналах роздрібної торгівлі. Вона має вихід DisplayPort 1.1 для відеодисплеїв (2560 x 1600) і роз'єм лінійного входу/виходу 3,5 мм для високоякісної потокової передачі аудіо.

Всі моделі обслуговуються службою підтримки Dell. Наприклад, пакет послуг Dell ProSupport передбачає автоматизоване визначення проблем, цілодобовий доступ до інженерів служби підтримки і швидкої заміни компонентів для мінімізації простоїв; послуги розгортання Dell Deployment; програма Dell IoT Solutions Partner Program для управління рішеннями IoT [14].

2.7 Шлюзи IoT компанії Hewlett Packard

В області IoT компанія HP активно просуває рішення, що дозволяють перенести обробку даних з хмарних центрів обробки даних на периферію

мережі (на кордон між OT і IT). Спеціалізовані IoT системи представлені в лінійці HPE Edgeline. Лінійка HPE Edgeline Intelligent Gateway призначена для збору, передачі даних і обробки подій, а лінійка HPE Edgeline Converged IoT System - для рівня первинного аналізу даних і потокової аналітики.

Конфігурація HPE GL10 IoT включає процесор lntel Atom, 4 Гбайт ОЗУ, твердотільний накопичувач 32 Гбайт, а HPE GL20 IoT - процесор lntel i5, 8 Гбайт ОЗУ, твердотільний накопичувач 64 Гбайт. Операційні системи – Microsoft Windows IoT Core, Microsoft Windows Server, Canonical Ubuntu Snappy Core, CentOS.

Шлюзи GL10/GL20 мають можливість комунікацій по Wi-Fi, через мобільні стільникові мережі, мають по 2 порти Gigabit Ethernet.

Пристрої HPE Edgeline Converged IoT System представляються компанією HPE як перші в галузі конвергентні системи для промислового Інтернету речей. Системи Edgeline EL1000 і EL4000 можна представити як шлюзи 2-го рівня, які об'єднують дані з HPE Edgeline Intelligent Gateway.

Системи HPE Edgeline оптимізовані для високопродуктивного аналізу, інтерпретації, візуалізації даних і надання інформації в режимі реального часу на периферійних ділянках мережі. Вони об'єднують обчислювальні ресурси, сховища, засоби захоплення і контролю даних, операційне середовище рівня підприємства і надають розробникам платформу для доступу до структурованої і неструктурованої інформації, а також забезпечують автоматизацію роботи з цими даними.

Іншою важливою особливістю HPE Edgeline є унікальна інтеграція збору точних даних з вимірювальних систем і їх управління, заснована на базі відкритих PXI стандартів. Коли вони доповнюються автоматичним машинним навчанням, це відкриває нові можливості в моніторингу і управлінні, прогностичній аналітиці для виявлення можливих поломок, а також доповнену реальність для мінімального ручного обслуговування. HPE Edgeline приносить всі можливості управління віддаленими системами, які надає Integrated Lights Out.

HPE Edgeline повністю сумісні з такими популярними IoT системами безпеки як Aruba ClearPass для автоматизації автентифікації, запобігання загрозам злому і функцій відновлення систем в умовах підвищеного ризику поза ЦОДами. Aruba Virtual Intranet Access (VIA) дозволяє організувати безшовні Virtual Private Network (VPN) тунелі для безпечних з'єднань між вузлами на кордоні IT-мереж і корпоративною мережею.

Важливою особливістю HPE Edgeline є безпрецедентні обчислювальні можливості. У EL1000 можна встановити один обчислювальний модуль (до 16 ядер Xeon D або Xeon E3) з двома відсіками для дисків SATA SFF, двома портами Gigabit Ethernet або 10 Gigabit Ethernet. Широкі можливості підключення периферійних пристроїв забезпечуються за допомогою двох слотів PCIe або PXI/PXIe разом з бездротовими модулями Wi-Fi або 3G. У EL4000 можна розмістити 4 обчислювальних модуля, кожен з яких може отримати свій модуль розширення PCIe або PXIe і два 10G Ethernet порти для прямого підключення до мережі.

Модель Edgeline 4000 також надає можливість організувати відмовостійку розподілену систему зберігання даних, а також працювати з аналітичною платформою на базі SQL HPE Vertica для отримання, обробки і завантаження готових даних від мільйонів «розумних лічильників» в секунду, з затримками в наносекунди [15].

2.8 Дослідження малоресурсної криптографії для IoT пристроїв

З появою 5G технології, IoT стали центром розвитку майже для всіх сучасних галузей. Пристрої в цій архітектурі значно менші та мають низьке енергоспоживання. Звичайні алгоритми шифрування, як правило, дорогі в обчислювальному плані через їхню складність і вимагають багато раундів, однак це може поставити під загрозу бажану цілісність. Криптографія з низьким ресурсом — це компроміс між вартістю впровадження, швидкістю, безпекою, продуктивністю та енергоспоживанням на пристроях IoT. Мотивація полегшеної криптографії полягає в тому, щоб використовувати

менше пам’яті, менше обчислювальних ресурсів і менше енергоспоживання, щоб забезпечити рішення безпеки, яке може працювати на пристроях з обмеженими ресурсами.

Блокові шифри мають фіксовану довжину бітів і різні кроки перетворення, які визначаються симетричним ключем. Блокові шифри дуже універсальні, що дуже корисно з точки зору IoT. Ще одна перевага полягає в тому, що цей процес має майже ідентичні методи шифрування та дешифрування. Тому його можна реалізувати з меншими ресурсами.

Однак, навколо Інтернету речей існує багато складнощів [16]. Перш за все це зв’язано зі складністю, як елементної бази, так і спеціальних алгоритмів обробки даних, що реалізуються в IoT пристроях. Процес обміну такою великою кількістю даних починається з самих пристроїв, які повинні безпечно взаємодіяти з платформою [16]. Пристрої, з яких складається система Інтернет

Існуючі в даний час платформи IoT використовують переважно централізовану модель, згідно з якою вони виступають в якості «брокерів» або концентраторів для управління обміном даними між пристроями IoT [16]. Однак, багато досліджень свідчать, що IoT повинен використовувати насамперед децентралізовану модель для забезпечення безпечного обміну даними. При цьому ключовими проблемами реалізації традиційної криптографії в пристроях IoT вважаються наступні [17]:

- низький рівень наявної обчислювальної потужності (або відсутність батареї у випадку пасивних RFID-міток);
- обмеженість ресурсів наявної пам'яті IoT пристроїв ;
- невелика фізична площа для реалізації збірки;
- низький заряд батареї (або навпаки її відсутність);
- реакція в реальному часі.

Малоресурсна або ж легка криптографія є компромісом між такими категоріями, як вартість реалізації, швидкість, безпека, продуктивність та енергоспоживання на пристроях з обмеженими ресурсами. При цьому,

мотивація для використання малоресурсної криптографії полягає у використанні меншого обсягу пам'яті, менших обчислювальних ресурсів та меншого енергоспоживання заради забезпечення безпеки [18].

Класифікація та застосування малоресурсних криптографічних примітивів За останнє десятиліття було запропоновано низку малоресурсних криптопримітивів, які мають переваги у продуктивності порівняно з стандартними криптографічними стандартами. Ці примітиви відрізняються від звичайних алгоритмів припущеннями, що малоресурсні примітиви не призначені для широкого кола застосувань і можуть накладати обмеження на потужність зловмисника. Малоресурсна криптографія - це розділ криптографії, метою якого є розробка алгоритмів для використання в пристроях, які не здатні забезпечити більшість існуючих кодів і мають достатні ресурси (пам'ять, потужність, розмір) для роботи [18]. Добре відомі чотири типи малоресурсних криптографічних примітивів, які доступні для використання:

- Малоресурсні блокові шифри (LWBC);
- Малоресурсні потокові шифри (LWSC);
- Малоресурсні хеш-функції (LWHF);
- Криптографію еліптичних кривих (ECC).

Основними факторами, за якими можна проаналізувати малоресурсні криптографічні примітиви є: розмір блоку, розмір ключа, структура та кількість раундів. ECC є ще одним із варіантів малоресурсної криптографії, причому, будучи асиметричним шифром, він має можливість забезпечувати автентифікацію та неспростування. Властивості малоресурсної криптографії обговорювалися в ISO/IEC 29192 в ISO/IEC JTC 1/SC 27.

ISO/IEC 29192 є новим проектом зі стандартизації малоресурсної криптографії, і проект знаходиться в процесі стандартизації. У стандарті ISO/IEC 29192 властивості малоресурсності описуються на основі цільових платформ. Дотричаючись завдань проектування, малоресурсні алгоритми використовують зазвичай менші розміри блоків - 32, 48 або 64 біт, ніж

звичайний шифр, який має більший розмір блоків - 64 або 128 біт [19]. Малоресурсні алгоритми застосовують менші розміри ключів, (менше 96 біт). Найменший розмір ключа, за даними NIST, становить 112 біт [19].

У стандарті ISO/IEC 29192 [19] детально описані властивості малоресурсності, що встановлюються на цільових платформах. По-перше, легкість апаратних засобів оцінюється за розміром мікросхеми та їх енергоспоживання і, по-друге, за обсягом потрібної пам'яті. Поряд з продуктивністю та вартістю, безпека є невід'ємним показником для будь-якого алгоритму малоресурсної криптографії. Властивість стійкості до атак будь-якого алгоритму малоресурсної криптографії може бути виміряна за допомогою криптоаналізу. Сенс криптоаналізу заключається в пошуці слабких місць алгоритму та розробку методів дешифрування [20].

Існує чотири основних типи атак на блоковий шифр [21]:

- диференціальний криптоаналіз;
- лінійний криптоаналіз;
- інтегральний криптоаналіз;
- алгебраїчні атаки.

Ці атаки базуються на використанні «відомого відкритого тексту», «тільки шифрованого тексту», «обраного шифрованого тексту», «обраного відкритого тексту», а також атаки «людина посередині», атаки «грубою силою» та атак «побічного каналу» [21].

Крім того криптографію розділяють на дві основні напряму: симетричні та асиметричні шифри. Відповідно, у таблиці 2.1 наведено порівняння, яке дозволяє продемонструвати різницю між асиметричною та симетричною криптографією [22].

Розглянемо криптографію з симетричним ключем, має можливість широко застосовуватися на пристроях, що піддаються жорстким ресурсним обмеженням [18]. В свою чергу, асиметричні шифри набагато вимогливі до обчислювальних ресурсів, ніж їх симетричні альтернативи.

Таблиця 2.1 – Порівняння методів криптографії

	Особливості різновидів реалізації	
Параметр	Криптографія з симетричним ключем	Криптографія з асиметричним ключем
Ключ	Один загальний приватний ключ	Унікальна пара приватного та публіч- ного ключів. Генерація відкритих ключів залежить від криптографічних алгоритмів, заснованих на односто-ронніх математичних функціях.
Кількість ключів	Експоненційно пропорційні кількості користувачів	Лінійно пропорційні кількості користувачів
Швидкість та складність	Це прості алгоритми, завдяки цьому процес шифрування може бути здійс- нений швидко.	Це набагато складніший процес, ніж шифрування з симетричним ключем, і він відбувається повільніше через те, що для використання різних ключів потрібно більше часу.
Апаратна складність	Використовує алгоритми що потребують відносно недорогого апаратного забезпечення.	Більш складна реалізація апаратного забезпечення, яка обчислює важкі алгоритми які потребують більш потужне апаратне забезпечення.
Використання	Здебільшого використовується, для передачі великих обсягів даних.	Використовується в невеликих транзак-ціях, в першу чергу для автентифікації та встановлення безпечного каналу зв'язку перед фактичною передачею даних.
Алгоритми	RSA, DSA, ECC	Stream cipher: Trivium, Chacha, WG-8, Espresso, Grain 128. Block Ciphers: AES, DES, 3DES, Blowfish, Twofish, Curupira, PRESENT, KATAN. TEA, Humming Bird, RECTANGLE, SIMON

Криптографія з симетричним ключем складається з основних функцій, таких як блокові або потокові шифри, а також методів застосування основної функції до пакету, яку носять назву режимом роботи блокового шифру для автентифікації чи шифрування [22]. Зусилля щодо криптографічній стандартизації малоресурсних примітівів розглядають як програмний, так і апаратний аспекти безпеки, котрі, зазвичай, мають, різні метрики.

Програмні метрики включають цикли, пам'ять і цикл на байт, тоді як апаратні метрики враховують пропускну здатність, площу, співвідношення по всій площі. Тому важко отримати пряме порівняння між цими двома показниками [19]. Симетричне шифрування використовує один і той же ключ, як для шифрування, так і для розшифрування даних. Цей метод шифрування є безпечним і відносно швидким. Його основним недоліком є спільне використання ключа двома сторонами, що спілкуються. Зловмисник може розшифрувати дані, якщо має доступ до ключа.

Алгоритми з симетричним ключем забезпечують конфіденційність і цілісність даних, але не гарантують автентифікацію [22]. Цей тип шифрування використовує три типи алгоритмів, заснованих на хешуванні, потоковому та блоковому шифрах.

Малоресурсні блокові шифри.

Симетрична шифрування допомагає при проектуванні однієї і тієї ж схеми для шифрування і дешифрування з мінімальними витратами. Блокові шифри - різновид симетричних шифрів, в яких обробляється відразу весь блок. Блокові шифри використовуються для побудови хеш-функцій та кодів автентифікації повідомлень (MAC) [23]. Полегшені блокові шифри базуються на двох типах структур: Мережа підстановки-перестановки (SPN) та Фейстеля. Мережа Фейстеля (FN) - це багатораундовий шифр, який ділить вхідний блок на дві частини і працює тільки над половиною (дифузія) в кожному раунді шифруванні або дешифруванні. Між раундами ліворуч і праворуч половини блоку міняються місцями. Структура Фейстеля використовує свою кругову функцію лише на половині стану [23]. Таким

чином, головною перевагою структури Фейстеля є використання одного і того ж програмного коду для процесу шифрування та дешифрування. Це зумовлює низьке використання пам'яті. Вона може бути реалізована на апаратних засобах з низькою середньою потужністю. Фейстелівська структура не підходить для конструкцій з малою затримкою. SPN є більш швидким, але без розкладу ключів. Відсутність ключового розкладу робить вразливим до атак. При однаковій величині запасу стійкості та однакових витратах енергії, структура SPN є більш придатною, оскільки вона вимагає меншого раунду виконання. За аналогічних умов SPN матиме менші енерговитрати. PRESENT та CLEFIA - єдині два алгоритми, що затверджені стандартом ISO/IEC 29192 [24,25].

AES є класичним прикладом алгоритму на основі SPN, працює на 128-бітному блоці з 128, 192 та 256-бітними варіантами ключів [26]. Мінімальна вимога еквівалентів воріт (GE), зафіксована для AES, становить близько 2400 GE (на 23% менше, ніж звичайна) [26-27], що все ще є важким для деяких невеликих додатків у реальному часі. Це показує порівняно ефективну продуктивність при забезпеченні додатковими ресурсами. Основними параметрами для оцінювання малоресурсного блочного шифру є розмір ключа, розмір блоку, тип структури та кількість раундів [18].

Малоресурсний шифр повинен відповідати чотирьом вимогам:

- Мінімальна площі кристалу або обсяг пам'яті;
- Низьке енергоспоживання;
- Менша кількість еквівалентів воріт (GE) для ефективної апаратної реалізації;
- Достатній рівень безпеки.

RFID-мітки можуть мати близько 1000-10000 GE, з яких можуть бути доступні 300- 2100 GE для аспектів безпеки [28]. Для впровадження відповідних рішень у сфері забезпечення інформаційної безпеки (ІБ), загальна кількість доступних GE становитиме приблизно 2000-3000. При цьому, блокові шифри мають бути обмежені меншою кількістю GE для того,

щоб відповідати малоресурсним додаткам. AES, PRESENT та CLEFIA – це три шифри є обов'язкові для вибору. Слід підкреслити, що AES є найбільш широко використовуваним шифром, оскільки був встановлений в якості стандарту для шифрування в 2002 році. Він використовується багатьма пристроями IoT, незважаючи на те, що він не є малоресурсним шифром. PRESENT та CLEFIA - це два шифри, які також були стандартизовані, але як малоресурсні шифри. Характеристики цих шифри можна використовувати в якості «опорних» при оцінці властивостей інших шифрів. Наприклад, відомо [25], що для шифру CLEFIA автори змінили розмір S-box з 4-х біт до 8-ми біт, так щоб досягти кращих результатів при виконанні на програмному забезпеченні. В роботі [29] оптимізовано шифри-фіналісти конкурсу AES, же основний акцент зроблено на зменшенни обсягів займаної пам'яті за рахунок зменшення розміру коду з використанням функцій заміни макросів та інших повторень коду. Використання AES призводе до високих GE [26], що робить їх нездійсненними для невеликих додатків, що працюють в реальному часі. Альтернативим рішенням для модифікації існуючого блокового шифру і створення ефективної апаратної моделі, є структура «PRESENT» [24].

Відповідний алгоритм рисунок 2,5 впроваджує малоресурсний блоковий шифр, та є більш меншим, ніж алгоритм AES. Розмір блоку процедур - 64, розмір ключа - 80 або 128, розмір S-box - 4. Один блок даних шифрується (розшифровується) за 31 раунд. Вихідні дані додатково розбиваються на блоки по 8 біт, де 4 біти цього значення складають стовпець, а ще чотири - рядок. Таким чином, вхідне значення замінюється на значення в S-Box. Вихід з S-Box подається в блок перестановок, де біти переставляються місцями. Таким чином реалізовано 31 раунд обчислень. Процес планування ключа буде оновлювати ключ для кожного раунду. Розшифрування виконується у зворотному порядку з інверсією S-Box.

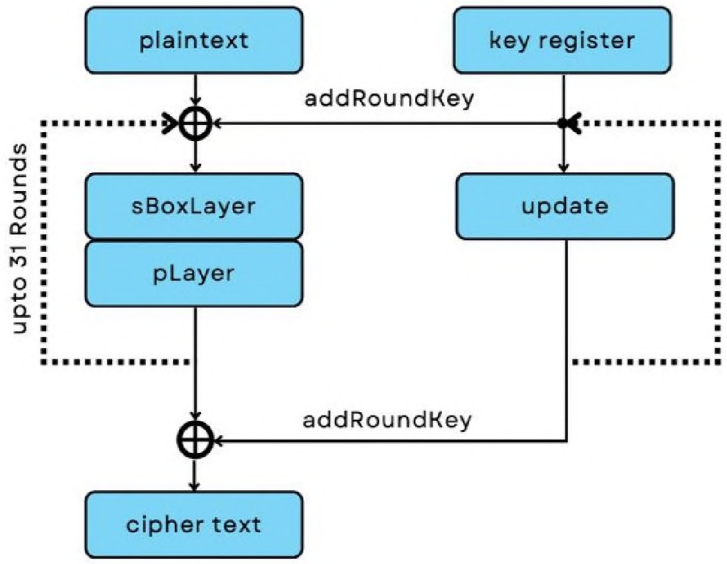

Рисунок. 2.5 Схема малоресурсного блокового шифру

В свою чергу, корпорація SONY представила CLEFIA, що стандартизована NIST у 2007 році. Вона базується на структурі Фейстеля і використовує 128-бітний блок з можливістю вибору ключа 128, 192, 256 біт через 18, 22, 26 раундів відповідно [25,30]. Дана реалізація демонструє високу продуктивність і стійкість до різних атак при порівняно високій вартості, оскільки найкомпактніша версія вимагає 2488 GE (тільки шифрування) для 128-бітового ключа [31]. CLEFIA має відповідні властивості [31], що робить його більш стійким до різних атак, але в той же час, це вимагає більшого об'єму пам'яті та обмежує його використання в надмалих додатках.

Порівняння методів малоресурсної криптографії FELICS - система бенчмаркінгу з відкритим вихідним кодом, призначену для об'єктивного та послідовного оцінювання програмних реалізацій малоресурсних криптографічних примітивів для вбудованих пристроїв [32]. Фреймворк є довільно гнучким завдяки своїй модульній структурі, що дозволяє легко інтегрувати нові метрики, цільові пристрої та сценарії оцінювання. Вона складається з двох модулів, які в даний час можуть оцінювати продуктивність малоресурсних блокових і потокових шифрів на трьох широко використовуваних мікроконтролерах: 8-бітному AVR, 16-бітному MSP та 32-бітному ARM. FELICS має відносно простий користувальницький

інтерфейс і призначений для використання розробниками шифрів для порівняння нових примітивів із існуючими. При цьому, отримані метрики є досить детальними та допомагають розробникам у виборі найкращого рішення, такого, що відповідає вимогам конкретного застосування. Слід відмітити, що FELICS має реалізацію PRESENT, однак, вона не є вдалою [32]. Тому, в межах проведеного аналізу, було обрано 32-бітну реалізацію [24]. Ця реалізація була згодом оптимізована за допомогою 3-ох різних методів. В першу чергу, 4-розрядні S-box були замінені на 8-розрядні S-box для покращення продуктивності програмного забезпечення. Потім були розгорнуті всі перимутації через їх надмірну вартість для програмних реалізацій. Крім того, цикли були також повністю розгорнуті, щоб усунути всі залежності і підштовхнути шифр-код до найшвидшого рівня продуктивності. В кінці, звернення до пам'яті було зведено до мінімуму за рахунок утримання стану шифру в регістрах процесора протягом більшої частини часу виконання шифру. Еталонна реалізація була отримана з сайту CLEFIA та адаптована до фреймворку FELICS [25, 30]. Еталонний алгоритм обчислює константи, які використовуються в планувальнику ключів, що призводить до невиправдано високого часу виконання. Тому була розглянута альтернативна версія 32-бітної реалізації, яка має попередньо обчислені значення всіх констант, що зберігаються в таблиці. Решта сім реалізацій, що були розглянуті, експлуатують використання T-box. У той час як в цих реалізаціях застосовуються стандартні T-box для 8-бітового орієнтованого еталонного алгоритму та його оптимізованої 32-бітової орієнтованої версії відповідно, всі інші реалізації використовують скорочені T-box. Також, варто відмітити, що потокові шифри широко досліджуються в криптографічному середовищі через більш швидке виконання, але вони є вразливими до атак у порівнянні з блоковими шифрами. В таблиці 2.2 наведено стислі відомості щодо результатів порівняння деяких параметрів AES, PRESENT, CLEFIA та DES.

Таблиця 2 – Результати порівняння

Алгоритм	Алгоритм проектуванн	Розмір вхідного	Розмір ключа	Кількість раундів	Площа (GEs)	Пропускна здатність	Особливості
AES	SPN	128	128	1,032	5440	15.53	Високий рівень безпеки, гнучкість.
PRESENT	SPN	64	80	31	10579	201.53	Менша кількість воріт, менше пам'яті. Доцільний для шифрування невеликих обсягів даних.
CLEFIA	GFN	128	128	36	27738	360.44	Висока продуктивність та стійкість до різних атак.

Всі розглянуті шифри були реалізовані на модулі FELICS, для умов використання 8-розрядних мікроконтролерів AVR [33]. Як і очікувалось, стандартизовані реалізації показують доволі повільні результати, за винятком PRESENT [24], де найповільніший час виконання має реалізація з невеликим обсягом коду. Це свидчить про те, що більшість оптимізацій дозволяє покращити час виконання навіть тоді, коли основна увага приділяється зменшенню розміру коду. PRESENT є «недружнім» малоресурсним шифром при націленості на програмні реалізації і тому, навіть з урахуванням декількох удосконалень та доопрацювань, все ще залишається дуже «важким» для програмного забезпечення (особливо для умов мобільних платформ). Ще одним результатом є те, що для збалансованих шифрів час

виконання близький до 1000 тактів майже для кожного шифру, і лише PRESENT дає далекі від цього значення. Він має біт-орієнтовані перестановки, які важко обчислювати в програмному забезпеченні [24]. В той же час, як AES та CLEFIA підтримують блоки в 128 біт [25,30].

CLEFIA - алгоритм шифрування, котрий має серед досліджуваних алгоритмів найбільшу довжину блоку з довжиною блоку 128 біт [25,30], в той час як в інших алгоритмах перевага віддається довжині блоку 64 біт. Це важливо для пристроїв, що обмінюються даними в мережі Інтернет з об'єктами малої ємності. Ефективніше шифрувати блоки невеликого розміру, а також ті, що застосовують архітектуру Фейстеля. З іншого боку, збільшення розміру ключа знижує енергоефективність. Звичайно, чим більший розмір ключа, тим краще забезпечується безпека. Однак, в умовах роботи IoT, більш вдалими слід вважати ключі від 80 біт до 128 біт (принаймні поки). Вибір структур простим способом, який не потребує занадто багато енергії, підвищує ефективність. Енергоємні структури, такі як процеси редукції та змішані удари, що використовуються в алгоритмах CLEFIA підтверджує цю ситуацію. PRESENT має певну перевагу над CLEFIA: - нелінійний S-box використовує 4-бітову структуру, що призводить до меншого GE і меншого енергоспоживання. Додаткові властивості S-box допомагають PRESENT досягти бажаного лавинного ефекту, а результати роботи [24] свідчать про те, що PRESENT має компактний S-box. Також в PRESENT є 16 S-box, які розділені на чотири групи. Деякі важливі відмінності цих S-box наведені нижче [24]: 1. Вхідний біт до S-box надходить з 4 чітко визначених S-box тієї ж групи. 2. Вхідні біти до групи з чотирьох S-box надходять з 16 різних S-box. 3. Чотири вихідні біти з певного S-box надходять у чотири чітко визначені S-box, кожен з яких належить до окремої групи S-box у наступному раунді. 4. Вихідні біти S-box у різних групах подаються до різних S-box. Апаратна реалізація AES для IoT, з точки зору ІБ, може залучати деякі апаратні атаки. Тому важливо спостерігати за цими спробами і своєчасно знаходити потрібні рішення. В цілому, AES та CLEFIA

є двома найбільш вдалими прикладами шифрів, які витрачають багато ресурсів (на розмір коду) для досягнення їх більш швидкої роботи. 4. Висновки Зростання масштабів використання IoT, обумовлює потребу в більш широкому запровадженні механізмів (алгоритмів) малоресурсного шифрування.

2.9 Висновок

В другому розділі були виконані поставлені задачі, були виділенні основні критерії, що необхідно розглядати при виборі IoT шлюзів. а саме:

- Підтримка перефирійних/туманних обчислень;
- Підтримуванні технології обміну даними;
- Функції маршрутизатора;
- Функції управління кінцевими пристроями мережею і додатками;
- Функції безпеки пристроїв, мережі і додатків.

Якщо декілька шлюзів задовольняють умовам описаним вище, то необхідно дивитись на такі характеристики, як: обчислювальна потужність, форм-фактор та умови, в яких шлюз можна використовувати.

Для пристроїв із певними ресурсними обмеженнями, наявні стандарти криптографічних алгоритмів можуть бути занадто складними та/або занадто енерговитратними. Крім того, кіберзлочинці можуть скористатися недоліками паролів, які відносно легко підбираються, якщо немає жорстко декларованих вимог до паролів, які створюються користувачами. Для пристроїв з обмеженими ресурсами, зокрема пристроїв IoT, малоресурсна криптографія є ефективним напрямом забезпечення безпеки їх мережевої взаємодії.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою економічного розділу є аналіз економічної ефективності від експлуатації IoT пристроїв. Для цього необхідно здійснити розрахунок:

- капітальні витрати на розробку і налагодження складових ситем інформаційної безпеки екосистеми IoT пристроїв;

- річних експлуатаційних витрат на утримання та обслуговування IoT екосистеми;

- річного економічного ефекту;

- показників економічного ефекту від модернізації IoT екосистеми та продовження термінів експлуатації;

3.1 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку IoT пристроїв.

Визначення трудоекості розробки IoT пристроїв.

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного програміста):

$$t= t_{тз} + t_{в} + t_{пр} + t_{д}, \text{ годин} \qquad (3.1)$$

де $t_{тз}$ - тривалість складання технічного завдання на розробку програми, год;

$t_{в}$-тривалість вивчення ТЗ, літературних джерел за темою тощо, год,

$t_{пр}$- тривалість розробки програми та засобів програми, год;

$t_{д}$- тривалість документування та оформлення результатів, год.

$$t=24год +50год +100год +200год=374 год$$

Витрати на розробку програми підвищення обізнаності персоналу на промисловому підприємстві $К_{пз}$ складаються з витрат на заробітну плату спеціаліста з ІБ (розробника програми) $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки програми підвищення обізнаності персоналу на підприємстві $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$З_{зп} = t*З_{іб}, \text{ грн}, \quad (3.3)$$

де t – загальна тривалість розробки програми підвищення обізнаності персоналу на інформаційно-телекомунікаційному підприємстві, год;

Зіб – середньогодинна заробітна плата спеціаліста з ІБ з нарахуваннями грн/год.

$$З_{зп} = 374*210 = 78540 \text{ грн}$$

Вартість машинного часу для розробки програми підвищення обізнаності персоналу на ПК визначається за формулою 3.4:

$$З_{мч} = t_{пр} * С_{мч} + t_{д}, \text{ грн} \quad (3.4)$$

де $t_{пр}$ - трудомісткість розробки програми та засобів програми підвищення обізнаності персоналу на ПК, год;

$t_{д}$ - тривалість документування та оформлення результатів, год;

$С_{мч}$ - вартість 1години машинного часу ПІК, грн/год.

Вартість 1години машинного часу ПК визначається за формулою 3.5:

$$C_{МЧ} = 1•5•5,64 + \frac{9350•0,3}{1920} + \frac{5800•0,1}{1920} = 29,96 \text{ грн}, \quad (3.5)$$

де Р- встановлена потужність ПК, кВт;

$t_{нал}$ - кількість задіяних робочих станцій при розробці програми, год;

$С_{е}$ - тариф на електричну енергію, грн/кВт*год;

$Ф_{зал}$- залишкова вартість ПК на поточний рік, грн;

$Н_а$ - річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ - річна норма амортизації на ліцензійне ПЗ, частки одиниці;

$К_{лпз}$ - вартість ліцензійного ПЗ, грн;

$Е_р$ -річний фонд робочого часу (за 40-годинного робочого тижня Fр=1920).

На промислових підприємствах середня потужність дорівнює Р = 0,4, а тариф на електричну енергію становить 5,64 грн/кВт*год, отже:

$$З_{мч} = t_{пр} * С_{мч} + t_д = 100 * 29.96 + 200 = 3196,20 \text{ грн}$$

$$К_{пр} = З_{зп} + З_{мч} = 78540 + 3196,20 = 81736,20 \text{ грн}$$

Капітальні (фіксовані) витрати на розробку та впровадження програми підвищення обізнаності складають:

$$К= К_{пр} +К_{зпз} +К_{рп} +К_{аз} +К_{дм} +К_{навч} +К_н \quad (3.6)$$

де $К_{пр}$ - вартість розробки програми підвищення рівня обізнаності та залучення для цього зовнішніх консультантів,грн. Сторонні організації не наймалися, тому даний коефіцієнт не враховується при розрахунках;

$К_{зпз}$ - вартість закупівель ліцензійного основного та додаткового ПЗ, складає 3000 грн;

$К_{рп}$ - вартість розробки програми підвищення обізнаності складає 35 500 грн;

$К_{аз}$ - вартість закупівлі апаратного забезпечення, 8 640 грн. Для даної програми покупка апаратного забезпечення не потрібна;

$К_{дм}$ - вартість допоміжних матеріалів: 5200грн;

$К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, 12 400 грн. Дані витрати не враховуються під час розрахунку формули, тому що фахівці не проходили платного навчання.

$К_н$ - витрати на встановлення обладнання та налагодження системи ІБ, 20 800 грн. Даних витрат не було, оскільки програма націлена на підвищення рівня знань у працівників підприємства.

$$К = 81736,20 + 3000 + 35500 + 5200 = 125436,20 \text{ грн}$$

3.2 Розрахунок річних експлуатаційних витрат

Річні поточні (експлуатаційні) витрати на функціонування програми складають:

$$С= С_в + С_к + С_{ак} \text{ , грн} \quad (3.7)$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування програмою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів.

Витрати на керування програмою підвищення обізнаності персоналу складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_{єв} + С_{тос}, \text{ грн} \quad (3.8)$$

Річний фонд амортизаційних відрахувань ($С_а$):

$$С_а = \frac{15 * 27\,500}{5} + \frac{60\,000}{10} = 88\,500 \text{ грн}$$

Річний фонд заробітної плати персоналу, що обслуговує програму ($С_з$) складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.9)$$

Основна заробітна плата спеціаліста з інформаційної безпеки на місяць – 23 000 грн, додаткова заробітна плата -25% від основної зарплати:

$$С_з = 23\,000 * 12 + 23\,000 * 12 * 0.25 = 345\,000 \text{ грн}$$

Ставка ЄСВ для всіх категорій платників складає 22%:

$$С_{єв} = 345\,000 * 0,22 = 75\,900 \text{ грн}$$

Вартість електроенергії, що споживається ноутбуками протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р * F_р * Ц_е, \text{ грн} \quad (3.10)$$

де Р- встановлена потужність ПК, кВт;

$Ц_е$ - тариф на електричну енергію, грн/кВт*год.

$F_р$- річний фонд робочого часу.

$$С_{ел}= 1 * 1920 * 5,64=10\,828,8 \text{ грн}$$

Витрати на технічне й організаційне адміністрування програми визначаються в відсотках від капітальних витрат - 2% ($С_{тос}$ = 125436,20 * 0,02 = 2508,72 грн).

Витрати на керування програмою підвищення обізнаності персоналу ($С_к$) дорівнюють:

$С_к$ = 37 900 + 88 500 + 345 000 + 75 900 + 10 828,8 + 2508,72 = 560637,5

Таким чином, річні поточні витрати складають:

С= 25 000 + 560 723,7= 585 637,52 грн

3.3 Визначення річного економічного ефекту від впровадження

Загальний ефект від провадження програми ІБ визначається з урахуванням ризиків порушення ІБ підприємства і становить:

$$E = B * R – C, \quad (3.11)$$

де В - загальний збиток від атак на мережу підприємства, грн;

R- очікувана ймовірність атаки на мережу підприємства, частки одиниці;

С - щорічні витрати на оновлення програми підвищення обізнаності персоналу, грн.

Загальний збиток від атаки на мережу підприємства складає:

$$B = \Sigma_i \Sigma_n U, \text{ грн}, \quad (3.12)$$

де І - число атакованих мереж підприємства;

N - середнє число атак на рік;

U- упущена вигода від простою атакованої мережі підприємства.

Упущена вигода від простою атакованою мережі підприємства становить:

$$U= П_п + П_в + V, \quad (3.13)$$

де $П_п$, - оплачувані втрати робочого часу та простої співробітників атакованої мережі підприємства, грн;

$П_в$ - вартість відновлення працездатності мережі підприємства;

V - втрати від зниження обсягу продажів за час простою атакованої мережі підприємства, грн.

Втрати від зниження продуктивності співробітників атакованої мережі підприємства являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_{П} = \frac{\Sigma Зс}{F} * t_{П}, \quad (3.14)$$

де F- місячний фонд робочого місяця (при 40-а годинному робочому тижні становить 176 ч);

$З_{с}$ - заробітна плата співробітників атакованої мережі на підприємства, грн намісяць;

$t_{П}$ - час простою мережі підприємства внаслідок атаки, год.

Витрати на відновлення працездатності мережі підприємства включають:

$$П_{В} = П_{ВИ} + П_{ПВ} + П_{ЗЧ}, \quad (3.15)$$

де $П_{ВИ}$ - витрати на повторне уведення інформації, грн;

$П_{ПВ}$ - витрати на відновлення мережі підприємства, грн,

$П_{ЗЧ}$ - вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації розраховуються:

$$П_{ВИ} = \frac{\Sigma Зс}{F} * t_{ВИ}, \quad (3.16)$$

де $t_{ВИ}$ - час повторного введення загубленої інформації співробітниками атакованої мережі підприємства, год.

Витрати на відновлення мережі підприємства визначаються:

$$П_{ПВ} = \frac{\Sigma Зо}{F} * t_{В}, \quad (3.17)$$

де $t_{В}$ - час відновлення після атаки персоналом, що обслуговує мережу підприємства, год,

$З_{о}$ - заробітна плата обслуговуючого персоналу, грн на місяць.

Втрати від зниження очікуваного обсягу продажів за час простою атакованої мережі підприємства визначаються:

$$V = \frac{O}{F_Г} \cdot (t_П + t_В + t_{ВИ}) \quad (3.18)$$

де О- обсяг продажів атакованої мережі підприємства, грн у рік;

$F_г$ - річний фонд часу роботи підприємства становить 2080 ч.

Визначення річного економічного ефекту:

$$V = \frac{3400000}{2080} \cdot (5 + 3 + 6) = 22884,62 \text{ грн}$$

$$П_{ПВ} = \frac{370\,300}{176} * 6 = 12\,623,9 \text{ грн}$$

$$П_{ВИ} = \frac{270\,500}{176} * 4 = 6\,147,7 \text{ грн}$$

$$П_В = 12\,623,9 + 6\,147,7 = 18\,771,6 \text{ грн}$$

$$П_П = \frac{270\,500}{176} * 2 = 3\,073,9 \text{ грн}$$

$$U = 18\,771,6 + 3\,073,9 + 22884,62 = 44730,12 \text{ грн}$$

$$В = \Sigma_2\ \Sigma_{14}\ 33287,81 = 2 * 14 * 44730,12 = 1252443,23 \text{ грн}$$

$$Е = 1252443,23 * 0.5 - 585\,637,52 = 40584,1 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності програми підвищення рівня обізнаності, здійснюється на основі визначення та аналізу наступний показників:

1. Сукупна вартість володіння (ТСО);

2. Коефіцієнт повернення інвестицій (ROSI);

3. Термін окупності капітальних інвестицій $Т_о$.

Коефіцієнт повернення інвестицій (ROSI) показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження програми підвищення обізнаності персоналу.

$$ROSI = \frac{E}{K}, \text{ частки одиниці} \quad (3.19)$$

де Е - загальний ефект від впровадження програми підвищення обізнаності персоналу, грн;

К- капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$ROSI = \frac{E}{K} = \frac{40584,1}{125436,20} = 0.32$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину банківської кредитної ставки з урахуванням інфляції:

$$ROSI > (N_{кр} + N_{інф})/100 ,$$

де $N_{кр}$ – банківська кредитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

$$0,32 > (13 - 10,60)/100 \Rightarrow 0,32 > 0.024 ,$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження програми підвищення обізнаності персоналу:

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0.32} = 3,125 \text{ років,} \approx 3\text{р. та } 45 \text{ днів.} \qquad (3.20)$$

3.5 Висновки про економічну доцільність проєктного рішення

В результаті розрахованих витрат на розробку та впровадження програми запропонованого рішення в питаннях, пов'язаних з інформаційною та кібербезпекою було доведено економічну доцільність розробки програми, методів та засобів підвищення кібербезпеки на запропонованому обьекті. Такі висновки зроблені, виходячи з коефіцієнту повернення інвестицій ROSI, який складає 1 та означає, що на 1 грн. капітальних витрат приходиться 0,32 грн. економічного ефекту. Період окупності при цьому складе 3роки та 45 днів. Капітальні витрати складають 40 484,1 грн, а експлуатаційні - 585 637,52 грн.

ВИСНОВКИ

У першому розділі було проведено аналіз загроз при використанні Інтернет речей IoT вдома та в промисловості IIoT, в залежності від застосування і відрізняється рівень загрози та архітектура обладненя мережі, а також склад самих пристроїв. Детально розглятута екосистема пристроїв, усі засоби, сервіси і технології, які використовуються в Інтернеті речей. Розглянувши архітектуру пристроїв дозволило виявити сильні та слабки сторони, та взаімодію між елементами. Неможна уявити Передача даних в IoT система.

Інтернету речей не існувало б без надійних технологій передачі даних з віддаленіших областей в найбільші центри збору даних компаній Google, Amazon, Microsoft і IBM. Словосполучення «Інтернет речей» містить слово «Інтернет», тому необхідно вивчати питання, що стосуються мережевих технологій, обміну даними. Розглянуті питаня безпеки Інтернет речей та терміну експлуатації.

В другому розділі розглянуті питання сумістності пристроїв між собою та наявність пристроїв з низьким енергоспоживанням (розрахованих на роботу місяцями і роками без підзарядки) і частий обмін даними по мережах з втратою пакетів. З урахуванням складності IoT має сенс створення архітектури, яка б специфікувала основні компоненти і їх взаємозв'язок. Архітектура IoT може надати такі переваги:

- дати адміністраторам мережі або IT-менеджеру корисний контрольний список для оцінки функціональності і повноти пропозицій від різних постачальників;

- служити орієнтиром для розробників в плані того, які функції потрібні в IoT і як вони взаємодіють;

- служити основою для стандартизації, стимулюючи сумісність і скорочення витрат.

Розглятута еталонна модель IoT від Міжнародного союзу електрозв'язку (МСЕ-Т) описана в Рекомендації Y.2060.

Особливу увагу приділено ролі шлюзу в IoT мережі. Він працює транслятором між протоколами. Шлюзи вирішують одну з головних проблем при проектуванні IoT, а саме проблему сумісності, як між різними пристроями, так і між пристроями та Інтернетом або корпоративною мережею.

Розглятуті хмарні та туманні обчислення та складена відповідна таблиця з їх порівнянням. Розлятуті проблеми обробки даних та операції, що виконуються на рівні накопичення даних:

- перетворення «даних в русі» в «дані в спокої»;
- перетворення формату з мережевих пакетів в реляційні таблиці БД;
- перехід від обчислень щодо подій до обчислень за запитом;
- значне зниження обсягу даних за рахунок фільтрації і вибіркового зберігання.

Існуючі в даний час платформи IoT використовують переважно централізовану модель, але багато досліджень свідчать, що IoT повинен використовувати насамперед децентралізовану модель для забезпечення безпечного обміну даними. При цьому ключовими проблемами реалізації традиційної криптографії в пристроях IoT вважаються наступні:

- низький рівень наявної обчислювальної потужності;
- обмеженість ресурсів наявної пам'яті IoT пристроів ;
- невелика фізична площа кристалу для реалізації збірки;
- наявність автономного живлення від батареї;
- реакція в реальному часі.

Запропоновано використання малоресурсної або ж легкої криптографії як компромісом між такими категоріями, як вартість реалізації, швидкість, безпека, продуктивність та енергоспоживання на пристроях з обмеженими ресурсами. За останій час запропоновано низку малоресурсних

криптопримітивів, які мають переваги у продуктивності порівняно з стандартними криптографічними стандартами.

У третьому розділі, розраховані витрати на розробку та впровадження модернізованого програмного забезпечення для підвищеня кібербезпеки интерннет пристроїв було доведено економічну доцільність розробки програми, методів та засобів. Такі висновки зроблені, виходячи з коефіцієнту повернення інвестицій ROSI, що на 1 грн. капітальних витрат приходиться 0,32 грн. економічного ефекту. Період окупності при цьому складе 3 роки та 45 днів. Капітальні витрати складають 40 484,1 грн, а експлуатаційні - 585 637,52 грн.

ПЕРЕЛІК ПОСИЛАНЬ

1. Tripathy B. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. – Florida: CRC Press, 2017. – 334 с.

2. Sutaria, R., and Raghunath, G., "Making sense of interoperability: Protocols and Standardization initiatives in IoT," International Conference on Recent Trends in Communication and Computer Networks – ComNet 2013, 2013.

3. Lake, D., Rayes, A., and Morrow, M., "The Internet of Things," The Internet Protocol Journal, Volume 15, No. 3, September 2012.

4. ITU-T, "Overview of the Internet of Things," Recommendation Y.2060, June 2012.

5. Ferguson, J., and Redish, A., "Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body," Expert Review of Medical Devices, Volume 6, No. 4, 2011, [Електронний ресурс]. Режим доступу: http://www.expert-reviews.com.

6. ITU-T, "Common Requirements and Capabilities of a Gateway for Internet of Things Applications," Recommendation Y.2067, June 2014.

7. Cisco Systems, "The Internet of Things Reference Model," White Paper, 2014. [Електронний ресурс]. Режим доступу: http://www.iotwf.com/

8. Frahim, J., et al., "Securing the Internet of Things: A Proposed Framework," Cisco White Paper, March 2015.

9. Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT). 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). [Електронний ресурс]. Режим доступу: https://doi.org/10.1109/cecnet.2012.6201508

10. Технологія Intel IoT Gateways. (2018). Офіційний сайт компанії Intel. [Електронний ресурс]. Режим доступу: https://software.intel.com/ru-ru/iot/hardware/gateways

11. Huawei AR Series Agile Gateways Brochures. (2017). Офіційний сайт компанії Huawei. [Електронний ресурс]. Режим доступу: http://www.huawei.com/minisite/iot/img/hw_ar_series_agile_gateways_brochure/en.pdf

12. Cisco IoT Networking. (2017). Офіційний сайт компанії Cisco. [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/brochure-c02- 734481.pdf

13. IoT Gateway. (2018). Офіційний сайт компанії NEXCOM. [Електронний ресурс]. Режим доступу: http://www.nexcom.com/Products/industrial-computing-solutions/iot-solutions/iot-gateway

14. Dell змінює економіку Інтернету речей з новими компактними шлюзами Edge Gateway. (1 березня 2017). Офіційний сайт компанії Dell. [Електронний ресурс]. Режим доступу: www.dell.com/learn/ua/ru/uacorp1/press-releases/dell-changing-economy-of-iot-with-new- compact-gateways-edge-gateway

15. Короткий огляд апаратних платформ, типових архітектурних рішень і послуг для корпоративних інформаційних систем. (2018, весна). Офіційний сайт компанії Hewlett Packard. [Електронний ресурс]. Режим доступу: https://h20195.www2.hpe.com/v2/GetPDF.aspx/c04771945.pdf

16. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. [Електронний ресурс]. Режим доступу: https://doi.org/10.1016/j.future.2013.01.010

17 Suo, H., Wan, J., Zou, C. and Liu, J. (2012) Security in the Internet of Things: A Review. IEEE International Conference on Computer Science and Electronics Engineering, Hangzhou, 23-25 March 2012, 648-651. [Електронний ресурс]. Режим доступу: https://doi.org/10.1109/ICCSEE.2012.373

18. McKay, K. A., Bassham, L., Turan, M. S., & Mouha, N. (2017). Report on lightweight cryptography. [Електронний ресурс]. Режим доступу: https://doi.org/10.6028/nist.ir.8114

19. ISO/IEC 29192-2:2012. (2012). Information technology Security techniques Lightweight cryptography Part 2: Block ciphers. Retrieved from [Електронний ресурс]. Режим доступу: https://www.iso.org/obp/ui#iso:std:iso-iec:29192:-2:ed-2:v1:en.

20. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Regazzoni, F. (2015). Midori: A Block Cipher for Low Energy. Advances in Cryptology – ASIACRYPT 2015, 411–436. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/978-3-662-48800-3_17

21. Eisenbarth, T., Gong, Z., Güneysu, T., Heyse, S., Indesteege, S., Kerckhof, S., Koeune, F., Nad, T., Plos, T., Regazzoni, F., Standaert, F.-X., & van Oldeneel tot Oldenzeel, L. (2012). Compact Implementation and Performance Evaluation of Block Ciphers in ATtiny Devices. Progress in Cryptology - AFRICACRYPT 2012, 172–187. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/978-3-642-31410- 0_11

22. Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014). A comparative survey of Symmetric and Asymmetric Key Cryptography. 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE). [Електронний ресурс]. Режим доступу: https://doi.org/10.1109/icecce.2014.7086640

23. Diehl, W., Farahmand, F., Yalla, P., Kaps, J.-P., & Gaj, K. (2017). Comparison of hardware and software implementations of selected lightweight block ciphers. 2017 27th International Conference on Field Programmable Logic and Applications (FPL). [Електронний ресурс]. Режим доступу: https://doi.org/10.23919/fpl.2017.8056808

24. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems -

CHES 2007, 450–466. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/978-3-540-74735-2_31

25. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., & Iwata, T. (2007). The 128-bit blockcipher CLEFIA. In International workshop on fast software encryption, 181-195. Springer, Berlin, Heidelberg.

26. Federal Information Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES). (2001). Retrieved from [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

27. Moradi, A., Poschmann, A., Ling, S., Paar, C., & Wang, H. (2011). Pushing the Limits: A Very Compact and a Threshold Implementation of AES. Advances in Cryptology – EUROCRYPT 2011, 69–88. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/978-3-642-20465-4_6

28. Juels, A., & Weis, S. A. (2005). Authenticating Pervasive Devices with Human Protocols. Advances in Cryptology – CRYPTO 2005, 293–308. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/11535218_18

29. Grossschadl, J., Tillich, S., Rechberger, C., Hofmann, M., & Medwed, M. (2007). Energy Evaluation of Software Implementations of Block Ciphers under Memory Constraints. 2007 Design, Automation & Test in Europe Conference & Exhibition. [Електронний ресурс]. Режим доступу: https://doi.org/10.1109/date.2007.364443

30. Akishita, T., & Hiwatari, H. (2012). Very Compact Hardware Implementations of the Blockcipher CLEFIA. Selected Areas in Cryptography, 278–292. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/978-3-642-28496-0_17

31. Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2017). A review of lightweight block ciphers. Journal of Cryptographic Engineering, 8(2), 141–184. [Електронний ресурс]. Режим доступу: https://doi.org/10.1007/s13389-017-0160-y

32. Dinu, D., Biryukov, A., Großschädl, J., Khovratovich, D., Le Corre, Y., & Perrin, L. (2015). FELICS - Fair Evaluation of Lightweight Cryptographic Systems. Retrieved from [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/csrc/media/events/lightweight-cryptographyworkshop-2015/documents/papers/session7-dinu-paper.pdf

33. Meiser, G., Eisenbarth, T., Lemke-Rust, K., & Paar, C. (2008). Efficient implementation of eSTREAM ciphers on 8-bit AVR microcontrollers. 2008 International Symposium on Industrial Embedded Systems. [Електронний ресурс]. Режим доступу: https://doi.org/10.1109/sies.2008.4577681 Received: on July 2022. Accepted: on July 2022

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	2	
3	А4	Зміст	2	
4	А4	1 Розділ	15	
5	А4	2 Розділ	39	
6	А4	3 Розділ	8	
7	А4	Висновки	3	
8	А4	Перелік посилань	5	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

Відгук керівника кваліфікаційної роботи:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Перелік матеріалів на оптичному носії

Ткач_М.О._125м-22з-1.docm

Ткач_М.О._125м-22з-1.pptx