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

_____Інститут електроенергетики_____
(інститут)
_____факультет інформаційних технологій_____
Кафедра інформаційних технологій та комп'ютерної інженерії___

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня ____бакалавра___
(бакалавра, спеціаліста, магістра)
Студента_____Єфіменка Артема Олександровича_____
(ПІБ)
академічної групи_____123-20зск-1_____
(шифр)
спеціальності _____123 «Комп'ютерна інженерія»____
(код і назва спеціальності)
за освітньо-професійною програмою
_____«Комп'ютерна інженерія»_____
(офіційна назва)
на тему Побудова комп'ютерної мережі із забезпеченням міжмашинної взаємодії та управління елементами Інтернету речей
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Шедловський І.А.			
розділів:				
Аналітична частина	доц. Шедловський І.А.			
Практична частина	доц. Шедловський І.А.			
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
____інформаційних технологій____
___та комп'ютерної інженерії____
(повна назва)
_____ __Гнатушенко В.В.__
(підпис) (прізвище, ініціали)
«_____»_____ 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня _____бакалавра _____
(бакалавра, спеціаліста, магістра)
студенту Єфіменку А.О. **академічної групи** _____123-20зск-1____
(прізвище та ініціали) (шифр)

спеціальності ___123 «Комп'ютерна інженерія»_____

за освітньою-професійною програмою «Комп'ютерна інженерія»
на тему Побудова комп'ютерної мережі із забезпеченням міжмашинної взаємодії та управління елементами Інтернету речей

затверджену наказом ректора НТУ «Дніпровська політехніка» від 11.04.2023 р. № 256-с

Розділ	Зміст	Термін виконання
1 Аналітичний розділ	На основі матеріалів з відповідних джерел та даних проаналізувати методи та засоби побудови комп'ютерних мереж із забезпеченням міжмашинної взаємодії	20.05.2023 р.
2 Практична частина	Розробити засоби підвищення рівня безпеки мереж для міжмашинної взаїмодії та IoT-комунікації	20.06.2023 р.

Завдання видано _____ Шедловський І.А.
(підпис керівника) (прізвище, ініціали)
Дата видачі _____
Дата подання до екзаменаційної комісії 10.07.2023 р.
Прийнято до виконання _____ Єфіменко А.О.
(підпис студента) (прізвище, ініціали)

АНОТАЦІЯ

Текстова частина випускної роботи: 77 сторінок, 15 рисунків, 3 таблиці, 52 джерела.

Об’єкт дослідження: процеси організації та формування спеціалізованих мереж для забезпечення M2M та IoT-комунікації.

Предмет дослідження: методи та засоби побудови спеціалізованих мереж для забезпечення M2M та IoT-комунікації.

Мета роботи: підвищення рівня повноти подання інформації засобами спеціалізованих мереж на основі M2M та IoT-комунікації.

В першому розділі випускної роботи проаналізовано предметну область побудови спеціалізованих мереж для забезпечення міжмашинної та IoT-комунікації, виконано формування узагальнених вимог. В другому розділі роботи розглянута архітектура, складові елементи та концептуальне проєктування спеціалізованих мереж для забезпечення міжмашинної взаємодії. В третьому розділі розглянуто методи та засоби підвищення рівня безпеки мереж для M2M та IoT-комунікації. Четвертий розділ роботи присвячений побудові захищеної комп'ютерної мережі для підприємства з декількома філіями. Проект був змодельований в симуляторі Cisco Packet Tracer.

IOT, M2M, АРХІТЕКТУРА, ДАНІ, ВЗАЄМОДІЯ, МЕРЕЖА, ПЕРЕДАЧА, ПРОТОКОЛ.

ANNOTATION

Graduate work: 77 pp., 15 figures, 3 tables, 52 sources.

Object of research: processes of organization and formation of specialized networks for M2M and IoT-communication.

Subject of research: methods and means of building specialized networks to provide M2M and IoT-communication.

Purpose: to increase the level of completeness of information presentation by means of specialized networks based on M2M and IoT-communication.

In the first section of the thesis the subject area and specialized networks for providing M2M and IoT-communication are analyzed, the formation of generalized requirements is performed. The second section of the thesis discusses the architecture, components and conceptual design of specialized networks to provide M2M and IoT-communication. The third section of the thesis discusses methods and tools to increase the security of networks for M2M and IoT-communication. The fourth section of the work is devoted to building a secure computer network in an enterprise with several branches. The project was modeled in the Cisco Packet Tracer simulator.

Keywords: IOT, M2M, ARCHITECTURE, DATA, INTERACTION, NETWORK, TRANSMISSION, PROTOCOL.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AMI (англ. Advanced Metering Infrastructure) – вдосконаленої інфраструктури вимірювання.

BSS (англ. Business Support systems) – системи підтримки бізнесу.

CE2E (англ. Communicating end-to-end) – наскрізне спілкування.

CH (англ. Cluster Head) – голова кластера.

CPS (англ. Cyberphysical system) – кіберфізична система.

CTS (англ. cyber-transportation systems) – кібертранспортна система.

DRTC (англ. Distributed real-time control) – розподілений контроль у реальному часі.

EDR (англ. Event Data Recorder) – реєстратор даних про події. ELP (англ. Electronic License Plate) – електронний номерний знак.

ETSI (англ. European Telecommunication Standards Institute) – Європейський інститут телекомунікаційних стандартів.

GPS (англ. Global Positioning System) – система глобального позиціонування.

HANs (англ. Home Area Networks) – домашні мережі.

I2V (англ. Infrastructure-to-Vehicle) – від інфраструктури до транспортного засобу.

IEC (англ. International Electrotechnical Commission) – Міжнародна електротехнічна комісія.

IoT (англ. Internet of Things) – інтернет речей.

ITU (англ. International Telecommunication Union) – Міжнародний союз телекомунікацій.

IPS (англ. Indoor Positioning Systems) – системи позиціонування в приміщенні.

M2M (англ. Machine-to-Machine) – машино-машинна взаємодія.

MANETs (англ. Mobile ad-hoc Networks) – мобільні спеціальні мережі.

MCC (англ. Mobile and cloud computing) – мобільні та хмарні обчислення.

MIR (англ. micro-power Impulse Radar) – мікропотужний імпульсний радар.

MHN (англ. Mobile Healthcare Network) – мобільна мережа охорони здоров’я.

NFC (англ. Near-Field Communication) – ближній зв’язок.

OMA (англ. Open Mobile Alliance’s) – Відкритий мобільний альянс.

PHI (англ. Private Healthcare Information) – приватна інформація про охорону здоров’я.

PHR (англ. Personal Health Record) – особиста медична карта.

PKI (англ. Public Key Infrastructure) – інфраструктура відкритих ключів.

PPDs (англ. Personalized Portable Devices) – персоналізованих портативних пристроїв.

QR (англ. Quick-Response) – швидке реагування.

SBCs (англ. Session Border Controllers) – контролери крайових сеансів.

V2I (англ. Vehicle-to-Infrastructure) – від транспортного засобу до інфраструктури.

V2V (англ. Vehicle-to-Vehicle communication) – зв’язок від транспортного засобу до транспортного засобу.

UWB (англ. Ultra Wideband) – ультраширокосмуговий.

VANETs (англ. Vehicular ad-hoc Networks) – автомобільні спеціальні мережі.

VAS (англ. Value added services) – послуги з доданою вартістю. WBAN (англ. Body Area Networks) – мережі зони тіла.

WBSNs (англ. Wireless Body Sensor Networks) – мережі безпровідних давачів тіла.

IT – інформаційні технології.

ЗМІСТ

ВСТУП

На даний час відбувається чергова інформаційна революція. Вона супроводжується бурхливим розвитком різнотипових пристроїв, призначених для відбору даних щодо стану об’єктів фізичного світу та IoT-пристроїв, котрі використовуються практично у всіх сферах людської діяльності. Процедури обміну даними в таких пристроях та системах виконуються з використанням спеціалізованих мереж на основі міжмашинної та IoT-взаємодії. Тому методи та засоби побудови спеціалізованих мереж для забезпечення M2M та IoT-комунікації є актуальним напрямком сучасних досліджень.

Метою даної кваліфікаційної роботи є підвищення рівня повноти подання інформації засобами спеціалізованих мереж на основі міжмашинної взаємодії та IoT-комунікації. Для досягнення поставленої мети було потрібно виконати наступні завдання:

– Проаналізувати стан досліджень в даній предметній області.
– Провести класифікацію спеціалізованих та сенсорних мереж.
– Розробити архітектуру спеціалізованих та сенсорних мереж.
– Виконати концептуальне проєктування M2M-взаємодії.
– Розробити рекомендації щодо покращення рівня безпеки спеціалізованих мереж для M2M та IoT-комунікації.

Об’єкт дослідження: процеси організації та формування спеціалізованих мереж для забезпечення M2M та IoT-комунікації.

Предмет дослідження: методи та засоби побудови спеціалізованих мереж для забезпечення M2M та IoT-комунікації.

Наукова новизна одержаних результатів: отримала подальший розвиток концептуальна модель M2M-взаємодії.

Практичне значення одержаних результатів: сформовано рекомендації щодо покращення рівня безпеки спеціалізованих мереж для M2M та IoT-комунікації.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ФОРМУВАННЯ ВИМОГ

1.1 Спеціалізовані мережі та міжмашинна взаємодія

Термін M2M (Machine-to-Machine) комунікації описує будь-яке програмно-алгоритмічне рішення або технологію, призначену для формування провідного та безпровідного зв’язку між фізичними пристроями для обміну інформацією. Спеціалізовані та сенсорні мережі є ключовим конструктивним елементом для формування зв’язків типу M2M. На даний час інтенсивно розвиваються медичні та кіберфізичні системи (CPS), «розумні» міста та їх складові сутності, зокрема «розумні» будівлі, транспортні засоби, побутова техніка, телефони тощо. Це викликає підвищений інтерес дослідників. Спеціалізовані та сенсорні мережі відіграють важливу роль при ефективному формуванні більшості перспективних напрямків розвитку інформаційних технологій. Тому формування ефективної M2M-реалізації є актуальним напрямком досліджень.

Згідно прогнозів фахівців, до 2025 року кількість інтегрованих та підключених IoT-пристроїв перевищить двадцять сім мільярдів. При цьому більше семидесяти відсотків всіх IoT-з’єднань реалізовані на базі інформаційних та комунікаційних технологій сформовано з використанням короткохвильового діапазону (зокрема WiFi, Zigbee, NFC) та інтегрованих програмованих логічних контролерів. На даний час спеціалізовані та сенсорні мережі «розумних» об’єктів використовуються для збору критичних до часу, оперативних, великих за обсягом типів даних отриманих з різнотипових джерел в метеорології, галузі охороні здоров’я, авіації, транспорті, транспортуванні, будівлях та спорудах, галузевих програмах тощо. Зібрані дані використовуються для аналітичного опрацювання для видобування нових корисних наборів даних та знань про різні предметні області з метою полегшення процедур прийняття рішень. На даний час

обширний перелік галузей людської діяльності (див. рисунок 1.1) використовують багато взаємозв'язаних пристроїв застосовуючи при цьому спеціалізовані та сенсорні мережі.

Рисунок 1.1 – Ринок спеціалізованих мереж

Спеціалізовані та сенсорні мережі спрощують процедури збирання та опрацювання даних, зґенерованих давачами та «розумними» пристроями. При цьому надійність, стійкість, доступність та продуктивність мереж є критично-важливою для забезпечення процесів обміну інформацією, збереження конфіденційності та цілісності даних.

1.2 Безпека M2M-мереж

Із збільшенням галузей використання M2M-засобів та мереж зростає кількість та можливості для атак. Тому в спеціалізованих та сенсорних мережах потрібно активно запобігати виникненню безпекових інцидентів, вирішувати несправності організованих з на їх основі інформаційних систем та мінімізувати пов'язані з цим ризики. Необхідність зменшення можливостей для атаки зростає в критичних середовищах, зокрема в

промислових системах управління, та у випадках оперування конфіденційними даними. Зокрема у галузі охорони здоров'я, банківській справі та соціальних мережах, можуть виникати серйозні безпекові проблеми пов'язані з втратою конфіденційності даних та порушенням етичних норм. Внаслідок чого може відбутися розкриття або компроментування конфіденційних записів та персональних даних пацієнтів.

У сфері телекомунікацій термін «Контроль доступу» був визначений у стандарті [1] як «функція, що виконується контролером ресурсів, яка розподіляє системні ресурси для задоволення користувацьких запитів». Для засобів M2M взаємодії такими ресурсами є підключення IP до базової мережі четвертого (4G) або п'ятого покоління (5G) та надійний зв'язок для динамічно пов'язаних сутностей сервера M2M-застосунків.

На даний час набула поширення трирівнева інформаційно-технологічна архітектура що базується на «Альянсі мобільних мереж наступного покоління» (NGMN) [2]. На першому рівні вона містить фізичні ресурси об'єднані на основі фіксованих мобільних мереж, а саме пристрої 5G, вузлові точки доступу, хмарні та мережеві вузли. Другий рівень містить набір функцій для формування збіжної модульної мережі. Третій рівень бізнес-застосунків містить конкретні програми та послуги розгорнуті на основі 5G-мережі. У цій архітектурі застосовуються процедури наскрізного E2E-управління, котрі можуть створювати виділені базові мережі відповідно до програмних сценаріїв, запускати та організовувати масштабування функцій відповідно до географічного розподілу.

Потребує поглибленого дослідження концепція забезпечення надійної передачі даних з використанням «розумних» пристроїв та доменів безпеки, що функціонують на основі базової мережі з повною IP-адресацією. При цьому доцільно використовувати базову 5G-мережу із забезпеченням зворотної сумісності з мережами 4G. На даний час передача даних між основними мережами досліджена на рівні MAC та IP і не охоплює механізми та інформаційно-технологічні рішення, пов'язані з розподілом однорангових

зв’язків на рівні програмно-алгоритмічних застосунків. Авторами [3] розглянуто ряд дослідницьких завдань, зокрема локальний менеджер мобільних вузлів та використання «розумного» конфігураційного агента. При цьому основна увага зосереджена на використанні сервера управління M2M-доступом, котрий забезпечує надійних міждоменних зв’язків із використанням взаємної автентифікації [4].

1.3 Спеціалізовані та сенсорні мережі п’ятого покоління

У доповіді «5G для промислових підключень та автоматизації» (5G ACIA) [5] опубліковано приклад використання виробничого процесу. Вантажні «розумні» транспортні засоби, підключені до мережі 5G, використовуються для доставки сировини та комплектуючих деталей на «розумну» фабрику на основі отриманих від давачів даних.

У технічному звіті «3GPP (TR) 22804» [6] розглянуто перспективи вхідної логістики для виробництва. Подано узагальнений випадок використання, коли «розумний» піддон, підключений до 5G-мережі, використовується для переміщення сировини. При цьому «розумна» вантажівка та «розумний» піддон мають інтегровані інформаційно-технологічні засоби для забезпечення надійного зв’язку з повсюдною заводською 5G-мережею та мережами загальнодоступного оператора мобільного зв’язку для реалізації транзитної взаємодії.

На основі розглянутих «5G-ACIA» та «3GPP TR 22804» можна сформувати перелік технічних вимог до промислових 5G-мереж:

– висока швидкість передачі даних та низька затримка;
– мобільність для забезпечення повсюдної підключення
– високий рівень безпеки;
– наскрізна E2E-безпека;
– гнучка система автентифікації з розширюваним протоколом автентифікації (EAP) [7];

– потужні та надійні процедури та алгоритми шифрування;

– мережевий розподіл для організації множини логічних віртуальних мереж для опрацювання різних випадків використання.

При цьому сегменти логічної мережі повинні одночасно функціонувати на загальній фізичній інфраструктурі та зберігати прийнятну якість обслуговування (QoS).

1.4 Спеціалізовані та сенсорні мережі в галузі охорони здоров'я

Однією з поточних потреб щодо M2M-взаємодії в «Електронній охороні здоров'я» (англ. eHealth) є розширення можливостей надання медичної допомоги у важкодоступних та віддалених районах, або у випадках коли пацієнт повинен отримувати медичну допомогу на місцевому рівні, оскільки не можливо здійснити безпечне для його життя транспортування до лікарні (див. рисунок 1.2).

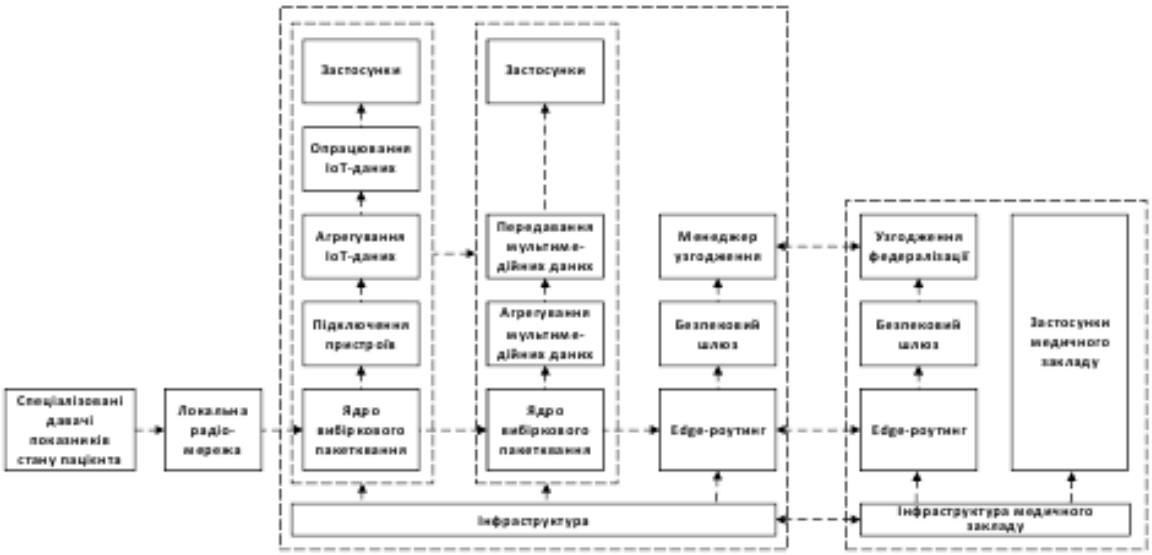

Рисунок 1.2 – Використання спеціалізованих та сенсорних мереж для «електронного здоров'я»

Спеціалізовані давачі взаємодіють з Edge-нодами транспортних засобів наближених до локації пацієнта. Вони обладнані локальною радіо-мережею

та давачами. На основі даних відбувається агрегування мультимедійних даних та ініціалізація мультимедійних сеансів з медичних закладом. За рахунок чого реалізуються функції зворотного зв'язку сформовані на основі 3GPP-мережі, або мережі без 3GPP. Наприклад Wi-Fi, супутникового зв'язку. Це залежить від покриття та вимог зв'язку. Вибір одного з доступних рішень для зв'язку можна здійснити за допомогою узгодження федералізації та відомостей щодо Edge-роутингу від оператора мобільної мережі.

У документі «TR 22804» [8] подано варіант використання потоків даних «Telecare» між домашніми пристроями та віддаленим моніторинговим центром. При цьому використовується зворотне з'єднання засобами прямого або ретрансльованого 5G-зв'язку, через 5G UE. Система підтримує енергоощадний зв'язок для пристроїв з обмеженими можливостями.

1.5 Аналіз існуючих інформаційно-технологічних платформ та застосунків

Для ефективного оцінювання методів та засобів побудови спеціалізованих мереж для забезпечення M2M та IoT-комунікації доцільно провести системне порівняння відомих інформаційно-технологічних засобів згідно наступних категорій критеріїв:

– Системна інтеграція. Якщо застосунки інтегруються з компонентами віртуалізації або SDN та компонентами, що організовують ресурси віртуалізації то застосовується NFV/SDN-інформування. Якщо застосунки використовують базову 3GPP або не 3GPP мережу для забезпечення безпровідного підключення M2M-пристроїв то використовується мережеве ядро. Контроль доступу та безпека. Включає підтримку доменів та передачу довірчих відносин, управління зв'язками з розподілом екземплярів служб управління зв'язками та управління передплатою.

– Автентифікація та авторизація. Група критеріїв щодо взаємодії з іншими відкритими стандартами, зокрема IETF CoAP, oneM2M або OMA

LWM2M та забезпечення портативності на інших апаратних архітектурах або операційних системах.

Одними з найактуальніших проектів щодо організації спеціалізованих мереж для забезпечення M2M та IoT-комунікації є «ARMOR» та «Stack4Things» та «Open5GMTC».

Проект ARMOR фінансується ЄС [9] та забезпечує широкомасштабні експерименти з наданням облікових даних з'єднань. Після одержання облікових відомостей щодо з'єднання пристрій ініціює запит на публікацію або отримання даних. Для цього він отримує маркер доступу, котрий потім перевіряється цільовим сервером з використанням структури «ACE Auth» через CoAP. Проект обслуговував набір із приблизно 2700 постійно запущених пристроїв M2M-пристроїв та інтегрований AAA-сервер для їх автентифікації при підключенні до WLAN. При цьому інформаційно-технологічна платформа продемонструвала високу масштабованість та сумісність.

Інформаційно-технологічне рішення для повсюдної сесорики та управління «Stack4Things» [10] використовує IoT-давачі та виконавчі механізми що інтегруються з використанням адаптера Websocket-зв'язку, реалізованого у формі OpenStack-плагіна. При цьому використовується рольовий контроль доступу (RBAC), рольова служба ідентифікації «OpenStack Keystone». Масштабування відбувається тільки на рівні кількості кінцевих пристроїв та має обмеження масштабування щодо кількості служб. Такі обмеження спричинені відсутністю інтегрованого системного роутера трафіку до декількох екземплярів служб. Оскільки інформаційно-технологічна платформа працює в режимі реального часу для обслуговування в масштабах міста, то можна вважати, що вона має високу масштабованість та певний рівень сумісності.

В проекті «Open5GMTC» управління підписками інтегровано з базовоюмережею «Home Subscriber Server». При цьому IoT-пристрої можуть змінювати домен безпеки. «Open5GMTC» на даний час функціонує на основі

ОС Ubuntu та Raspberrian.

Результати порівняння проектів ARMOR, Stack4Things та «Open5GMTC» подано в таблиці 1.1.

Таблиця 1.1 – Порівняння інформаційно-технологічних платформ забезпечення M2M та IoT-комунікації, відомості щодо яких опубліковано в наукових джерелах

	Інтеграція системи		Управління доступом			Оперативні	
Інформаційно-технологічна платформа	NFV/ SDN	Базова мережа	Безпека	Комунікація	Аутентифікація	Сумісність	Портативність
ARMOUR	Ні	Ні	Ні	Так	Так	Так	Так
Stack4Things	Так	Ні	Так	Так	Так	Так	Так
Open5GMTC	Так	Так	Так	Так	Так	Так	Так

Перелік проектів з відкритим кодом у домені M2M досить обширний завдяки великій кількості доступних протоколів та стандартів. Опубліковано відомості щодо ряду проектів, які підтримують лише один протокол або реалізують лише одну функціональність. Зокрема, брокери MQTT – це відкриті проекти, що мають підтримку виробників у галузі. Наприклад, IoTivity [11]. Окремі проекти, базуються на власному програмно-алгоритмічному ядрі та пропонують стеки інформаційно-технологічних рішень для забезпечення M2M-зв’язку. Наприклад, «Zephyr» [12]. Доступні «парасолькові» проекти, що охоплюють декілька розробок з різних напрямків. Зокрема, інформаційно-технологічна платформа «Eclipse IoT» інтегрує засоби для управління пристроями, безпеки та візуалізації даних [13, 14]. Розглянемо деякі з проектів з відкритим кодом, які є наближеними до повністю інтегрованого комунікаційного рішення або мають високий ступінь стандартної підтримки на основі загальновідомих та відкритих

стандартів.

«Leshan» [15] – це програмно-алгоритмічна реалізація, розроблена на Java в якості OMA LWM2M сервера та клієнта. Вона вважається фактичною реалізацією та однією з перших реалізацій стандарту з відкритим кодом, розробленою в 2014 році. Проект запропоновано «Sierra Wireless» та завдяки сумісності, підтвердженій під час багатьох «Plugfests», підтримано OMA. Інформаційно-технологічна реалізація підтримує транспортні прив'язки UDP, UDP з DTLS та SMS як транспортний рівень. При цьому поза межами зв'язку залишаються тільки SIM-карти зі стандарту OMA LWM2M. Проект підтримує процедуру «Bootstrap», здійснює опрацювання та моніторинг статистики підключення. Окремо реалізовано також об'єкти управління доступом у формі стеку протоколів. При цьому потрібно використовувати код або запускати запити від сервера до клієнта через веб-інтерфейс.

Інформаційно-технологічний проект Zephyr [12] – це спільна розробка започаткована Фондом Linux, який створює масштабовану операційну систему (RTOS) що функціонує в режимі реального часу. RTOS оптимізовано для пристроїв з обмеженими ресурсами, що можуть функціонувати на декількох апаратних архітектурах.

Підтримка OMA LWM2M була програмно реалізована засобами мови програмування C. RTOS характеризується безпечними зв'язком DTLS та енергоефективністю. Сумісність підтверджується тестовим сервером Leshan.

IoTivity [11] – це вільно-поширюване програмне забезпечення з відкритим кодом для забезпечення безперебійного підключення між IoT-пристроями та системами. Проект започатковано «Linux Foundation». Фінансування відбувається за рахунок реалізації стандартів «Фонду відкритих зв'язків» (OCF) [16] за ліцензією Apache.

Програмне забезпечення може функціонувати на основі декількох операційних систем: Android, Tizen, Ubuntu та Windows. Подібно до

«Open5GMTC», зв'язок між пристроями базується на бібліотеці libcoap [13] для стеку протоколів CoAP та використовує інтегровану структуру ACE

для авторизації та делегування IoT-запитів.

Окрема модель взаємодії призначена для реалізації функцій управління щодо передачі прав власності на пристрій, оскільки це важливо для виробників IoT-пристроїв. Для управління пристроями OCF сформував власний протокол управління пристроями на основі CoAP, відмінний від OMA LWM2M. Проект «IoTivity Cloud» реалізовано на основі хмарної інфраструктури. Його функціонал не охоплює управління підключенням.

Проект «Anjay LWM2M SDK» [14] має інтегровану програмно-алгоритмічну реалізацію OMA LWM2M написану засобами мови програмування C. При цьому ініціюється запуск циклу опрацювання подій з для забезпечення високих показників енергоефективності завдяки реалізації декількох алгоритмів для опрацювання повторних передач та кешування відповідей.

Для доповнення стандартної сумісності проект забезпечує підтримку всіх інтерфейсів OMA LWM2M для транспортування CoAP через UDP, DTLS та SMS. Програмно-алгоритмічний комплекс може функціонувати на базі операційних систем Ubuntu, CentOS 7 та macOS Sierra.

В приміщеннях організації «Anjay» інтегровано DHCP-сервер з управлінням підключень для Wi-Fi.

З метою узагальнення характеристик інформаційно-технологічних програмно-алгоритмічних проєктів з відкритим кодом, в таблиці 1.2 подано їх порівняну характеристику.

Таблиця 1.2 – Порівняння інформаційно-технологічних проектів з відкритим кодом для забезпечення M2M та IoT-комунікації

	Інтеграція системи		Управління доступом			Оперативні	
Інформаційно-технологічна платформа	NFV/ SDN	Базова мережа	Безпека	Кому-нікація	Аутен-тифі-кація	Суміс-ність	Порта-тив-ність
Leshan	Ні	Ні	Так	Так	Так	Так	Так
Zephyr	Ні	Ні	Ні	Ні	Ні	Так	Так
IoTivity	Так	Ні	Так	Так	Так	Так	Так
Anjay	Ні	Так	Ні	Так	Ні	Так	Так

1.6 Загальні вимоги до спеціалізованих мереж для забезпечення M2M та IoT-комунікації

Для надійної M2M-взаємодії пристроїв між різними доменами, що функціонують в основних 4G або 5G мережах потрібно сформувати вимоги, які дозволять реалізувати вищезазначені варіанти використання. Для цього потрібна відповідність до наступного переліку вимог:

– Передавання та завантаження відомостей про право власності на дані. Право власності – це право управління пристроєм. У випадку повного завантаження весь зв’язок IoT-пристрою буде однозначно скеровано на цільовий домен безпеки.

– Взаємна автентифікація. IoT-пристрій повинен використовувати та виконувати рекомендації цільового домену безпеки для виконання процедур надсилання даних на відповідний рівень зв’язку чи сервера даних. Перед ініціалізацією процедур обміну даними з новим рівнем зв’язку повинна відбутися процедура взаємної автентифікації, котра повинна бути виконана та можлива без обов’язкового підключення до сервера. Підключення та управління передплатою. IoE-пристрої повинні адаптувати свої функціональні можливості щодо підключення відповідно до отриманих

від поточної базової мережі рекомендацій.

– Самоорганізація та самовідкриття потрібно реалізовувати з метою забезпечення високої щільності M2M-взаємодії IoT-пристроїв та оптимізації розподілу ресурсів для збільшення масштабування у пікові моменти і зменшення при низькому використанні. В процедурах контролю доступу ці функції перекладаються на процедури розподілу екземплярів сервера застосунків з метою інформування пристрою про відповідність сервера даних.

1.7 Висновок до першого розділу

В першому розділі розглянуто спеціалізовані мережі та особливості міжмашинної взаємодії. Досліджено безпеку M2M-мереж. Описано спеціалізовані та сенсорні мережі п’ятого покоління. Проаналізовано існуючі інформаційно-технологічні платформи та застосунки. Сформовано загальні вимоги до спеціалізованих мереж для забезпечення M2M та IoT-комунікації.

2 ПРОЄКТУВАННЯ СПЕЦІАЛІЗОВАНИХ МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ МІЖМАШИННОЇ ВЗАЄМОДІЇ ТА IOT-КОМУНІКАЦІЇ

2.1 Класифікація спеціалізованих та сенсорних мереж

Термін M2M використовується для стеку технологій, які дозволяють здійснювати взаємодію між пристроями без втручання людини або за умов обмеженого її втручання [17]. M2M-взаємодія потребує наявності проводового або безпровідного фізичного з'єднання між вузлами. M2M в здебільшого зосереджується на машинному типі зв'язку (MTC) при якому відбувається наскрізна взаємодія пристроїв. Ключовими компонентами сформованих на даний час M2M-моделей є фактично змонтовані на локаціях безпровідні пристрої з інтегрованими сенсорами та давачами або мережі безпровідного зв'язку, котрі сформовані на основі функціональних наборів радіочастотної ідентифікації (RFID).

Безпровідні спеціальні мережі для M2M-взаємодії, відомі під назвою «WANET», в залежності від призначення можна класифікувати на наступні типи [18]:

– Мережі безпровідних мереж (WMN) [19] використовують топологію сітки, сформовану на основі радіовузлів. Вузлами можуть бути mesh-клієнт, mesh-маршрутизатори або mesh-шлюзи. Мережевими клієнтами WMN здебільшого є ноутбуки, мобільні телефони тощо. Мережеві клієнти водночас виконують функції хостів та мережевих маршрутизаторів. Кожен клієнт сприяє розширенню діапазону мережі. Більшість практичних реалізацій WMN формуються в локаціях з суворими кліматичними умовами або при оперативному розгортанні польових операції військових сил, супутниковому зв'язку в космосі, моніторингу громадського транспорту або автомобільній телеметрії в режимі реального часу. Аналогічно вони використовуються в широкосмугових домашніх, громадських та

муніципальних мережах.

– Мобільна спеціалізована мережа (MANET) – це мережа, що формується «на вимогу». Здебільшого мережі такого типу формуються з використанням мобільних пристроїв, зокрема смартфонів, планшетів тощо. Кожен вузол виконує функції маршрутизатора, переадресовуючи трафік, не пов’язаний із власними застосунками. Завдяки незалежному переміщенню вузлів, цей тип мережі має низькі характеристики надійності та динамічну топологію. Окремі реалізації MANET є військовими спеціальними мережами між солдатами на місцях, транспортними засобами та штабами. Вони сформовані на основі спеціального мобільного зв’язку по типу «корабель-корабель». До зазначеного типу мереж також відносяться персональні мережі (PAN) [20] тощо.

– Мережа безпровідних давачів (WSN) [21] – це мережа сформована на базі «розумних» вузлів давачів. «Розумний» вузол давача – це пристрій, оснащений процесором, пам’яттю, безпровідним мережевим інтерфейсом та одним або декількома давачами та виконавчими механізмами. Давачі надають пристрою можливість контролювати декілька фізичних або екологічних величин. Інтегрована пам’ять має обмеження щодо опрацювання, так, що всі отримані окремим вузлом дані передаються безпровідним способом до базової станції для подальшого зберігання та опрацювання.

З використанням WSN базова станція або будь-який вузол мережі може надсилати дані назад на вузол давача. Це можуть бути команди для для виконавчих механізмів. На даний час WSN-застосунки практично використовуються в галузі охорони здоров’я, військовій справі, виробничих, промислових та державних системах, для контролю характеристик навколишнього середовища, «розумних» будинках та «розумних» містах (див. рисунок 2.1).

25

Рисунок 2.1 – Класифікація WSN-застосунків

Кореляції між M2M, WSN, кіберфізичними системами та IoT-пристроями показані на рисунку 2.2. Застосунки на основі кіберфізичних систем інтегровані з масовими безпровідними мережами та IoT-пристроями за рахунок інформаційних масивів зібраних з навколишнього середовища.

Рисунок 2.2 – Співвідношення між M2M та WSN [22]

Швидкий розвиток засобів основі M2M-зв’язку створює нові перспективи та можливості для галузі інформаційних технологій, зокрема «розумні» роботи, «розумні» транспортні системи, M2M-телеметрія та прогнозтична аналітика, «розумні» мережі та кіберфізичні системи, котрі є наслідком еволюційного розвитку M2M-систем [23]. Аналітичне опрацювання інформації є важливим елементом інформаційних систем, сформованих на основі IoT-пристроїв [24].

2.2 Архітектура спеціалізованих та сенсорних мереж

Європейський інститут телекомунікаційних стандартів (ETSI) [25] розглядає M2M-мережі як структуру, що складається з трьох частин:

– Зазвичай інтегрований Домен M2M-пристрїв.

– Домен M2M-мережі, котрий забезпечує зв’язок між пристроями, давачами та шлюзами, підключення до мережі.

– Домен застосунків. На основі якого відбувається оперування данимита використання конкретними бізнес-застосунками.

Автори [26] додали ще два домени для операційних завдань та застосункових задач автоматизації бізнес-процесів. Зокрема:

– Операційний домен включає фізичну безпеку, системи управління тасервісні утиліти.

– Домен продуктів та бізнес-процесів містить цільові категорії.

Наприклад, зокрема охорона здоров’я, транспорт, освіта, «розумні» міста.

Перелічені елементи формують різні взаємопов’язані домени [27], котрі призначені для полегшення процедур опрацювання даних різними сервісними застосунками та забезпечують повну взаємодію мереж та послуг. Повна картина п’яти елементів подана на рисунку 2.3.

Домені M2M-пристроїв сформовано з групи спеціалізованих та сенсорних мережевих вузлів для переадресації даних.

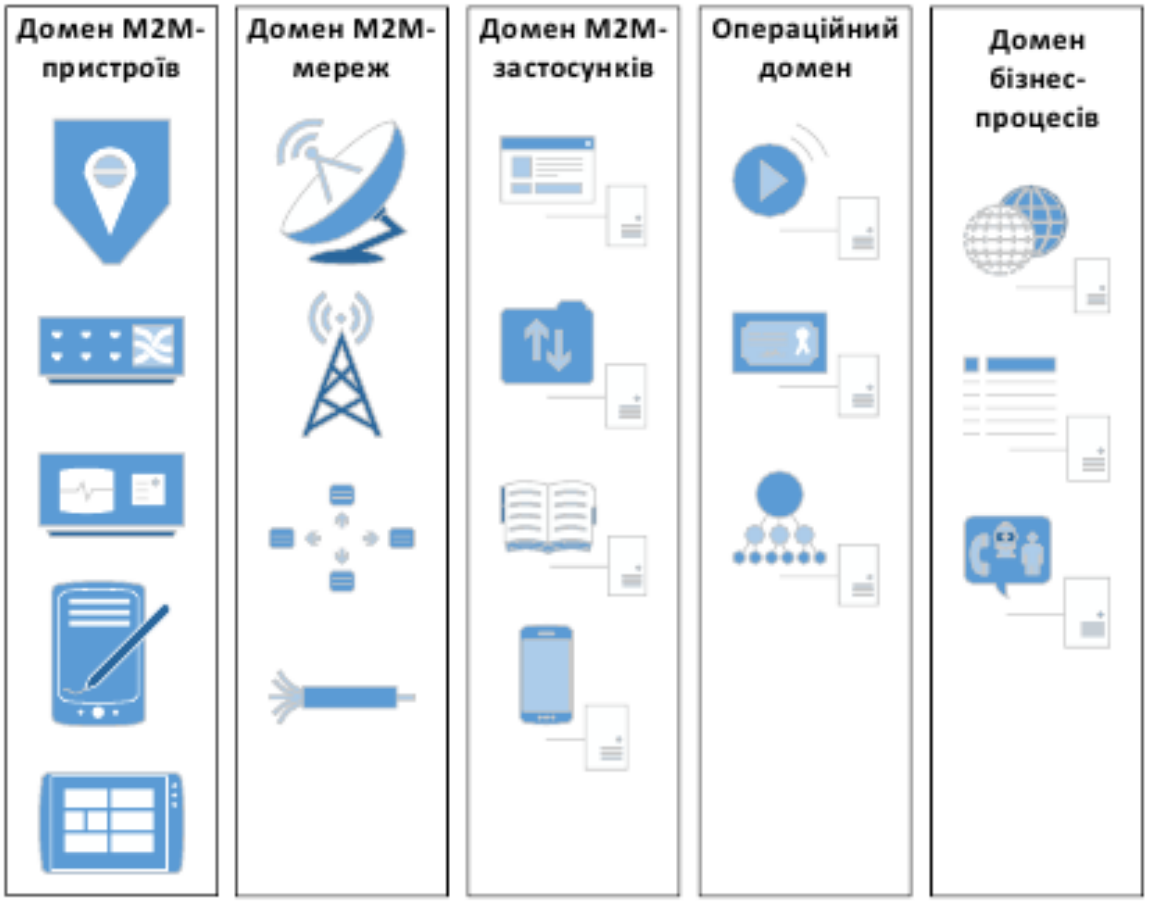

Рисунок 2.3 – M2M-Архітектура [34]

Ці пристрої оснащені спеціалізованими сенсорними технологіями для моніторингу в режимі реального часу для прийняття рішень щодо передачі даних на шлюз, тобто переадресації даних з одним або декількома переходами. M2M-шлюз збирає пакети M2M-вузлів та передає в іншу мережу і. Зазначена мережа забезпечує зв'язок між усіма типами «розумних» пристроїв та давачів і шлюзів.

У домені M2M-мережі комунікаційні мережі забезпечують зв'язок та передають сенсорні дані між шлюзами та програмами.

У домені M2M-застосунків інтегровано різнотипові служби та сервіси прикладних застосунків, котрі використовуються механізмами бізнес-обробки застосунків. Ці служби та сервіси відповідають за зберігання та надання даних M2M-застосункам для управління. В поданій архітектурній моделі M2M-комунікації подано операційний домен та домен бізнес-

процесів. Вони призначені для розширення можливостей управління потоками даних та їх використання в режимі реального часу [28]. Наведена діаграма архітектури M2M-систем, сформована на основі конвергенції різних сімейств інформаційних такомунікаційних технологій.

2.3 Класифікація сутностей M2M-архітектури

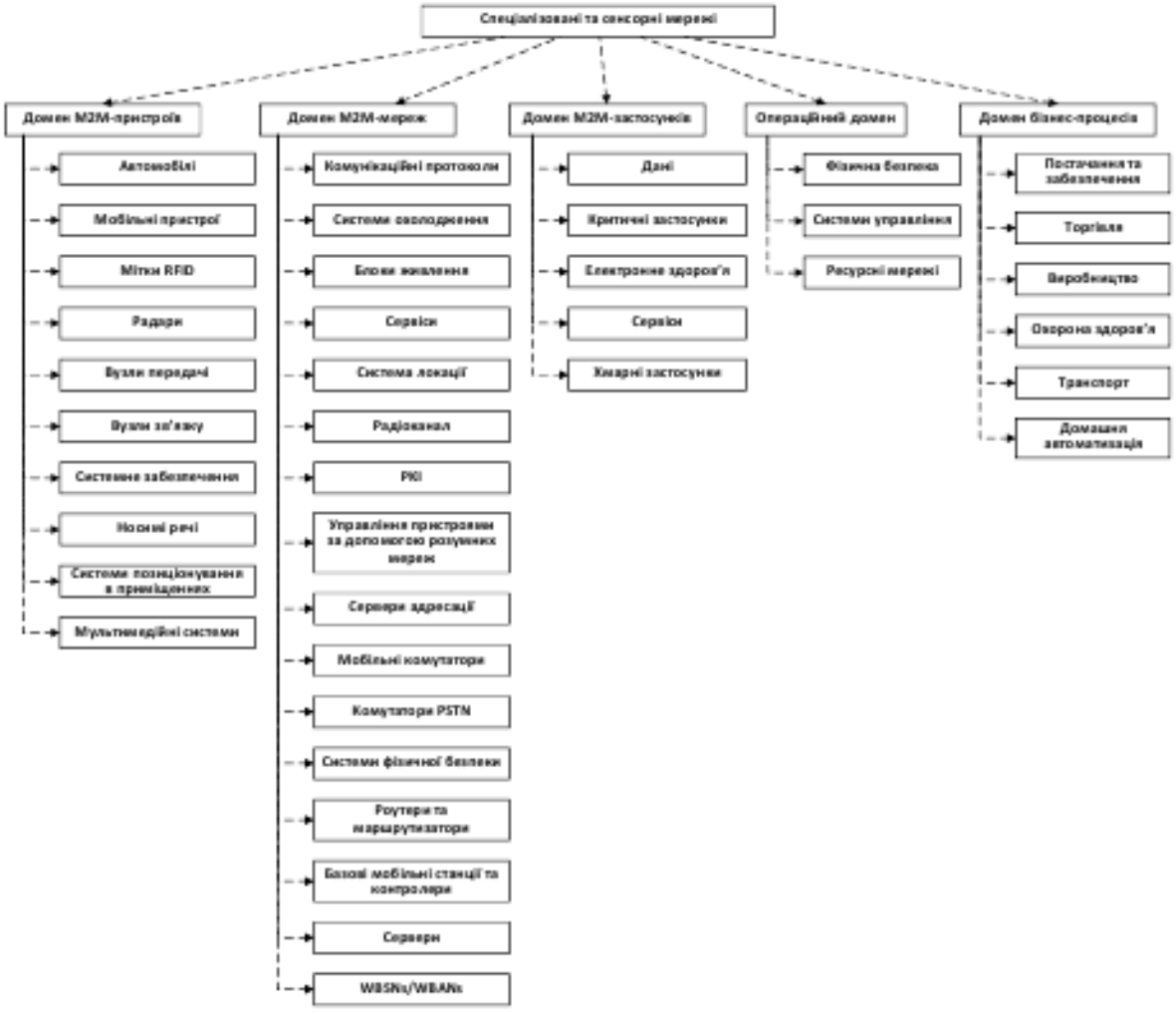

Рисунок 2.4 – Класифікація M2M-сутностей

Виходячи з поданої вище M2M-архітектури розробимо класифікацію сутностей подану на рисунку 2.4.

Згідно відомостей Європейського інституту телекомунікаційних стандартів (ETSI), M2M20-архітектуру сформовано на основі домена

пристрою, мережевого домена та домена застосунків. Подана в попередньому параграфі модель, розширена шляхом додавання операційного домена та домена бізнес-процеси. Розглянемо детальніші описи зазначених доменів.

2.3.1 Домен M2M-пристроїв

Домен M2M-пристроїв – це поєднання M2M-пристроїв та регіональних M2M-мереж. Домен M2M-пристроїв – це група пристроїв, здатних відповідати на запити, що містяться в даних або передавати ці дані автономно. Зв’язок між M2M-пристроями та M2M-шлюзами – M2M-мережа.

Домен M2M-пристроїв містить наступні сутності:

– Автомобілі. Автомобільні спеціальні мережі (VANET) [29] є підкласом мобільних спеціалізованих мереж (MANET). Апаратним забезпеченням VANET здебільшого є бортове обладнання, інтегроване в транспортних засобах. Воно забезпечує засоби зв’язку з іншими транспортними засобами. Зокрема, зв’язок від транспортного засобу до транспортного засобу – V2V. Або взіємодію з мережевою інфраструктурою, від транспортного засобу до інфраструктури – V2I та від інфраструктури до транспортного засобу – I2V [30].

– Мобільні пристрої, котрі підключається до локальної мережі за допомогою інтегрованих давачів. Вони мають інтегровані різнотипові давачі, зокрема камери, гіроскопи, термометри, пристрої GPS тощо. Та вбудовані інтерфейси, зокрема, GSM-антени, Wi-Fi, Bluetooth тощо. До цього підкласу відносяться персоналізованих портативні пристрої.

– RFID-мітки, є піддоменом M2M-пристроів, сформованим на основі RFID-систем та включають теги, зчитувачі та програмне забезпечення для забезпечення RFID-ідентифікації. Теги RFID – це невеликі наклейки, котрі поміщаються на предмети, тварин або людей, щоб долучити до них інформацію або зробити їх ідентифікованими серед інших. Схема RFID-міток складається з блоку управління та антени.

– Радари. Мікропотужні імпульсні радари [31] використовуються у багатьох сферах для детектування руху або як далекоміри. Радари широко використовуються у військовій галузі для захисту територій, у рятувальних програмах, в автоматизації транспортних засобів, зокрема для допомоги при паркуванні, круїз-контролю тощо. Також радари активно використовуються у системах домашньої безпеки, зокрема для замків без ключів, автоматичних дверей тощо. Крім того радари активно використовуються виробництві для промислової автоматизації.

– Вузли передачі – використовуються у кластерній архітектурі де вони згруповані в кластери. При цьому кожен кластер обрає свій головний вузол [32]. Цей вузол передає всі дані вузлів кластера на базову станцію. Такий підхід мінімізує споживання енергії, зменшуючи при цьому перевантаження трафіку та колізії мережевих даних.

– Вузли зв’язку. Відповідно до M2M-архітектури, вузол зв’язку є шлюзом між пристроями та мережею зв’язку. Він виконує функції M2M-шлюза. Вузол зв’язку управляє пакетами та забезпечує ефективні маршрути їх передачі на віддалений сервер через домен M2M-мереж.

– Системне забезпечення. Через складність та великі обсяги мережевого трафіку в спеціалізованих та сенсорних мережах виникає потреба у відповідних сервісних системах для забезпечення стабільності функціонування, стану готовності, інтеграції та оперативності. Системне забезпечення – це набір програмних рішень, що використовуються провайдерами зв’язку для виконання своїх внутрішніх операцій. Термін включає білінгове програмне забезпечення, засоби управління клієнтами, проєктування та управління застосунками та програмними продуктами, маркетингу, а також замовлення та активацію замовлень. Носимі речі [33] – це речі, які можна носити протягом тривалого періоду часу. Носимі речі використовуються для контролю біометричних показників, зокрема, температури тіла, кров’яного тиску, рівня цукру, транспірації, сатурації, частоти серцебиття тощо. Зазвичай, носима річ має інтегровані засоби

комунікації та забезпечує доступ користувачів до даних в режимі реального часу. Значна частина носимих речей має функціональні можливості введення даних та локальне сховище даних. На даний час на ринку доступно обширний перелік носимих речей, зокрема, годинники, окуляри, контактні лінзи, «електронний» одяг та «розумні» тканини, прикраси, слухові апарати у формі сережок.

– Системи позиціонування в приміщеннях надають можливість ідентифікувати місце розташування предмета або особи всередині будівлі за допомогою радіохвиль, магнітних полів, акустичних сигналів або іншої сенсорної інформації.

– Мультимедійні системи – до яких відносяться користувацькі електронні пристрої, зокрема, DVD, відеокамери, телевізори, ігрові приставки тощо. Найчастіше дей піддомен пристроїв використовує сигнали зв'язку Ultra Wideband (UWB) та є частиною комплексних систем домашньої автоматизації.

2.3.2 Домен M2M-мереж

M2M-шлюз забезпечує взаємодію та взаємозв'язок між пристроями та мережею зв'язку. Основною частиною домену M2M-мережі є апаратно-програмні засоби для забезпечення зв'язку між M2M-шлюзами та доменом M2M-застосунків. Зв'язок здійснюється через дротові мережі, зокрема xDSL та PLC, або безпровідні мережі, зокрема, стільникові мережі 3G/4G, Wi-Fi та WiMAX. Наступний перелік сутностей, приналежних до цього домена не є вичерпним, він постійно оновлюється та розширюється: Протоколи зв'язку є ключовим компонентом у розвитку спеціалізованих та сенсорних мереж. Вони часто піддаються різнотиповим загрозам та атакам. Протокол зв'язку може мати різні характеристики безпеки, недоліки коду, слабкі відповіді та небезпечні послуги транспортного та мережевого рівня.

– Системи охолодження. Енергоефективні та безпечні системи

охолодження забезпечують доступність та надійне функціонування спеціалізованих та сенсорних мереж.

– Блоки живлення. Системи живлення маршрутизаторів, комутаторів, серверів та комп'ютерів є критично важливими мережевими елементами, які надзвичайно вразливі до фізичних атак або збоїв.

– Системи геолокації користувачів та визначення місцезнаходження. Реєстри мобільних користувачів та місцезнаходження використовуються для геолокації інформування вузлів з метою їх позиціонування.

– Радіоканал. Оскільки більшість спеціалізованих та сенсорних мереж базуються на безпровідному зв'язку, то радіоканал є основним носієм інформації та базовим елементом у домені мережі.

– PKI. Інфраструктура відкритих ключів (PKI) – це найсучасніший механізм забезпечення конфіденційності (шифрування) та автентифікації практично для більшості спеціальних та сенсорних мережевих застосунків і зв'язку.

– Управління пристроями за допомогою «розумних» мереж. Завдяки останнім досягненням в галузі спеціалізованих та сенсорних мереж, користувачі тепер можуть ефективно контролювати послуги та дистанційно керувати різноманітними приладами та пристроями.

– Сервери адресації. Процедура реєстрації та присвоєння адреси є важливим етапом у спеціалізованих та сенсорних мережах. Вона суттєво впливає на інші послуги та операції, зокрема маршрутизацію. Для підвищення ефективності функціонування спеціалізованих та сенсорних мереж доцільно застосовувати ефективні та гнучні програмно-алгоритмічні рішення адресації.

– Мобільні комутатори. Постачальники послуг зв'язку зазвичай є операторами стільникових мереж. Інформаційні система провайдерів складається з реєстрів мобільних користувачів та місцезнаходження, мобільних базових станцій, контролерів тощо.

– Комутатори PSTN. Інфраструктурні мережі зазвичай формуються на основі компонентних мереж. Для цього можуть ефективно використовуватись магістральні PSTN-комутатори.

– Системи фізичної безпеки та управління. Фізична безпека часто недооцінюється і не враховується в контексті спеціалізованих та сенсорних мереж. Відповідний план із необхідними системами управління є критично-важливим з метою уникнення компрометації давачів у мережі.

– Маршрутизатори та комутатори. Ця група апаратно-програмних комплексів є ядром домену M2M-мереж. Маршрутизатори, DSLAM, контролери крайових сеансів (SBCs) та мережеві комутатори утворюють мережу даних, яка пов’язує домени M2M-пристроїв та M2M-застосунків.

– Базові мобільні станції та контролери. Топологія базових мобільних станцій і контролерів суттєво впливає на маршрутизацію в спеціалізованих та сенсорних мережах, визначаючи ефективність обміну сенсорними даними. Більшість програмних засобів можуть скористатися вузловою топологією давачів та маршрутизацією даних до інших вузлів давачів, зовнішньої базовоїстанції або контролера.

– Сервери. Серверна система, яка допомагає при встановленні та використанні мережевих зв’язків є важливим елементом домена M2M-мереж. Ключовими сервісами цього піддомену є адресація та DNS, ідентифікація приватних ключів пристроїв або користувачів, моніторинг та адміністрування мережевого трафіку тощо. WBSN / WBAN. Мережі натільних безпровідних давачів (WBSN) або мережі зони тіла (WBAN) – це новий тип безпровідних мережі носимих персональних обчислювальних пристроїв. Цей тип мереж активно впроваджується в галузі охорони здоров’я для дистанційного вимірювання медичної інформації, допомоги пацієнтам та літнім людям, автоматизації будинків та моніторингу стану людського організму.

2.3.3 Домен M2M-застосунків

Домен M2M-застосунків містить службові та клієнтське програмне забезпечення. Це проміжний рівень між кінцевим користувачем та даними, що зібрані на основі домену M2M-пристроїв, після опрацювання різнотиповими програмно-алгоритмічними службами та сервісами. Необхідно зазначити, що поданий в класифікації перелік програмних засобів цього домена, не є остаточним та вичерпним. Зокрема:

– Піддомен даних. У цьому піддомені знаходяться зібрані за допомогою M2M-взаємодії дані. По відношенню до них можуть відбуватись процедури зберігання, керування та подання користувачам за допомогою програмних засобів або веб-інтерфейсів. Дані можна використовувати лише для інформування, статистичного аналізу та контролю.

– Критичні застосунки – це програмні засоби спеціального призначення, що поєднують дані та знання отримані з різнотипових джерел, зокрема давачів, IoT-пристроїв, мережі Інтернет, баз та сховищ даних).

– Електронне здоров’я об’єднує мобільній мережі в системі охорони здоров’я [34]. Котрі є комбінаціями стаціонарних, переносних та мобільних пристроїв, смартфонів та обладнання для моніторингу життєво важливих ситуацій і функцій. Зазначене обладнання може надати лікарям, медичному персоналу або окремому пацієнту повну та вичерпну інформацію щодо стану здоров’я та особисті медичні записи [35]. Важливою частиною піддомена електронного здоров’я є програми eHealth, які зберігають, передають, подають та опрацьовують зібрані дані для отримання статистичних результатів та вибірок. При необхідності зберігання даних з піддомена електронного здоров’я використовуються державні та приватні бази та сховища медичних даних з особливими вимогами щодо конфіденційності, розмежування прав доступу та захисту. Дані подаються з використанням спеціалізованих медичних застосунків, протоколів, eHealth-порталів, веб-застосунків або мобільних застосунків.

– Хмарні застосунки – це інтеграція сенсорних мереж та інформаційних технологій на основі хмарних обчислень [36] котра використовує переваги та можливості хмарних систем опрацювання та зберігання даних. Ці системи сформовані на основі парадигми «вимірювальний сенсор-хмара як послуга» (SSaaS) дозволяє забезпечити можливості одночасного доступу декількох застосунків до даних отриманих за допомогою інтегрованого з хмарною інфраструктурою сенсора.

Модель хмарних давачів покращує характеристики використання ресурсів давача, підвищує ефективність управління давачами та забезпечує середовище для розробки програмних застосунків та інтерфейсів для забезпечення стійкої взаємодії між давачами, елементами кібернетичних систем та реальним світом.

Мобільні застосунки все частіше використовуються для інтеграції та управління ресурсами сенсорних мереж. Тому останні досягнення інформаційних технологій на основі мобільних хмарних застосунків використовують Open Mobile Alliance (OMA) веб-сервер «розумних» карток [37], який інтегрований з мобільними пристроями. Зокрема, карткою модуля ідентифікації абонента (SIM), яка безпосередньо з’єднується з оператором для завантаження застосунків на смартфони, мобільні телефони та пристрої. Окремим прикладом є TokTok, технологія, яка дозволяє отримувати доступ до хмарних сервісів Gmail та Google Calendar, та здійснювати розпізнавання голосу за допомогою мобільного телефону.

2.3.4 Операційний домен

Автоматизація операцій донедавна була прерогативою людей. Вона, дозволяє забезпечити високі показники ефективності задоволення вимог замовників при мінімізації витрат ресурсів. Розглянемо типові елементи операційного домена:

– Фізична безпека – це елемент який використовується для

моніторингу спеціалізованих та сенсорних мереж, захисту доступу до областей або зон, об’єктів або людей. Зокрема, системи сигналізації, відеоспостереження тощо.

– Системи управління, які використовуються для забезпечення доступу до будинків, будівель або певних територій, є одним з функціональних елементів спеціалізованих та сенсорних мереж. Наприклад, використання «розумної» мережі для формування систем управління приладами. Ці системи складаються [38] з акумулюючих енергію пристроїв, передаючих кабелів, «розумних» підстанцій та трансформаторів, вдосконаленої вимірювальної інфраструктури та домашніх мереж (HANs).

В загальному випадку, зазначені системи використовуються як системи домашньої автоматизації, зокрема, опалення, вентиляції та кондиціонування повітря, системи автоматизації будівель чи містечок тощо.

– Ресурсні мережі можуть надавати готові інформаційно-технологічні рішення для автоматизації процесів постачання, вимірювання та формування рахунків за спожиті фізичні ресурси, зокрема, воду, електроенергію, газ, тепло і т.д.

Перелік сутностей в операційному домені на даний час не є остаточно сформованим, він активно розширюється та доповнюється.

2.3.5 Домен продуктів та бізнес-процесів

Спеціальні та сенсорні мережі можуть забезпечити рішення для автоматизації для обширного переліку різних сфер організації, діяльності та бізнесу. Перелік сутностей в домені продуктів та бізнес-процесів на даний час не є остаточно сформованим:

– Постачання та забезпечення. Давачі та виконавчі механізми використовуються для автоматизації процесів доставки вантажів, пакування продукції тощо.

– Торгівля. Програмне забезпечення в області торгівлі, наприклад,

системи підтримки бізнесу – BSS, забезпечує моніторинг та управління людськими ресурсами компанії. Значного поширення набули торгові автомати.

– Виробництво. У середовищі сучасних виробничих підприємств, виробничі інформаційні системи активно використовують спеціалізовані та сенсорні мережі для підвищення якості обслуговування, ефективності управління виробничими ресурсами та досягнення практично майже нульового простою виробничого обладнання.

– Охорона здоров’я. У галузі охорони здоров’я різноманітні спеціалізовані та сенсорні мережі широко використовуються для моніторингу та архівування даних. Ці програмно-апаратні комплекси зосереджують увагу на безпекових аспектах їх використання завдяки високим вимогам щодо захисту даних та конфіденційності. Різнотипові давачі інтегровані та вбудовані в прилади контролю стану здоров’я громадян, що забезпечують сенсорику та пакетне передавання даних практично в режимі реального часу.

– Транспорт. Завдання управління транспортними парками є важливим для бізнес структур та організацій. Воно відчутно впливає на ефективність постачання продукції, вартість товару та економічні показниики в цілому. Завдяки автоматизації та контролю транспортних засобів зменшуються забруднюючі викиди та забруднення довкілля, підвищується рівень безпеки дорожнього руху.

– Домашня автоматизація. Впродовж останнього періоду часу відбувається активне зростання частоти використання спеціалізованих та сенсорних мереж в задачах автоматизації будинків. З’явився ряд готових рішень, зокрема для дистанційного контролю витрат електроенергії, регулювання подачі води, контроль споживання газу та управління приладами, що обладнані інтегрованими давачами.

2.4 Концептуальне проєктування M2M-взаємодії

Базові первинні мережі розгортаються з набором зарезервованих сертифікатів, підписок та ключів. Мережеві компоненти, а також екземпляри служби домену M2M-застосунків розгортаються на основі менеджера VNF (VNFM) під час первинної інсталяції або при наявності відповідної потреби. Мережеві компоненти забезпечують контроль доступу до підключення та зв'язку M2M та IoT-пристроїв до відповідних екземплярів служби домену застосунків. При формуванні та використанні надійної передачі даних між двома безпековими доменами, зокрема, вихідним та цільовим безпековими доменами, M2M або IoT-пристрій одночасно переключатиметься між двома серверами контролю доступу M2M (MAC) (див. рисунок 2.5).

Із збільшенням мобільності M2M та IoT-пристроїв, вони перемикаються між фізичними та безпечними межами зв'язку, які визначаються відповідним доменом безпеки. M2M-пристрій виконує передачу в цільовий домен безпеки, зареєструвавшись на відповідному сервері управління M2M-доступом (MAC). Після чого він отримує відомості щодо локальної політики підключення, яке буде використовуватися, та відповідного вузла, зокрема однорангового зв'язку або сервера застосунків.

Для забезпечення функціональності 5G M2M потрібно використовувати елементи міжшарового управління, для яких задіяно MAC-сервер. MAC-сервер розподіляє ресурси, використовуючи інформацію, що стосується запуску серверів застосунків, отриману від VNF-менеджера, і надає інформацію про відповідність сервера додатків на основі можливостей пристрою, тим самим відповідаючи на вимогу самовідкриття. Сервер MAC здійснює управління підключенням, надаючи смарт-пристрою облікові дані підключення, які будуть використовуватися.

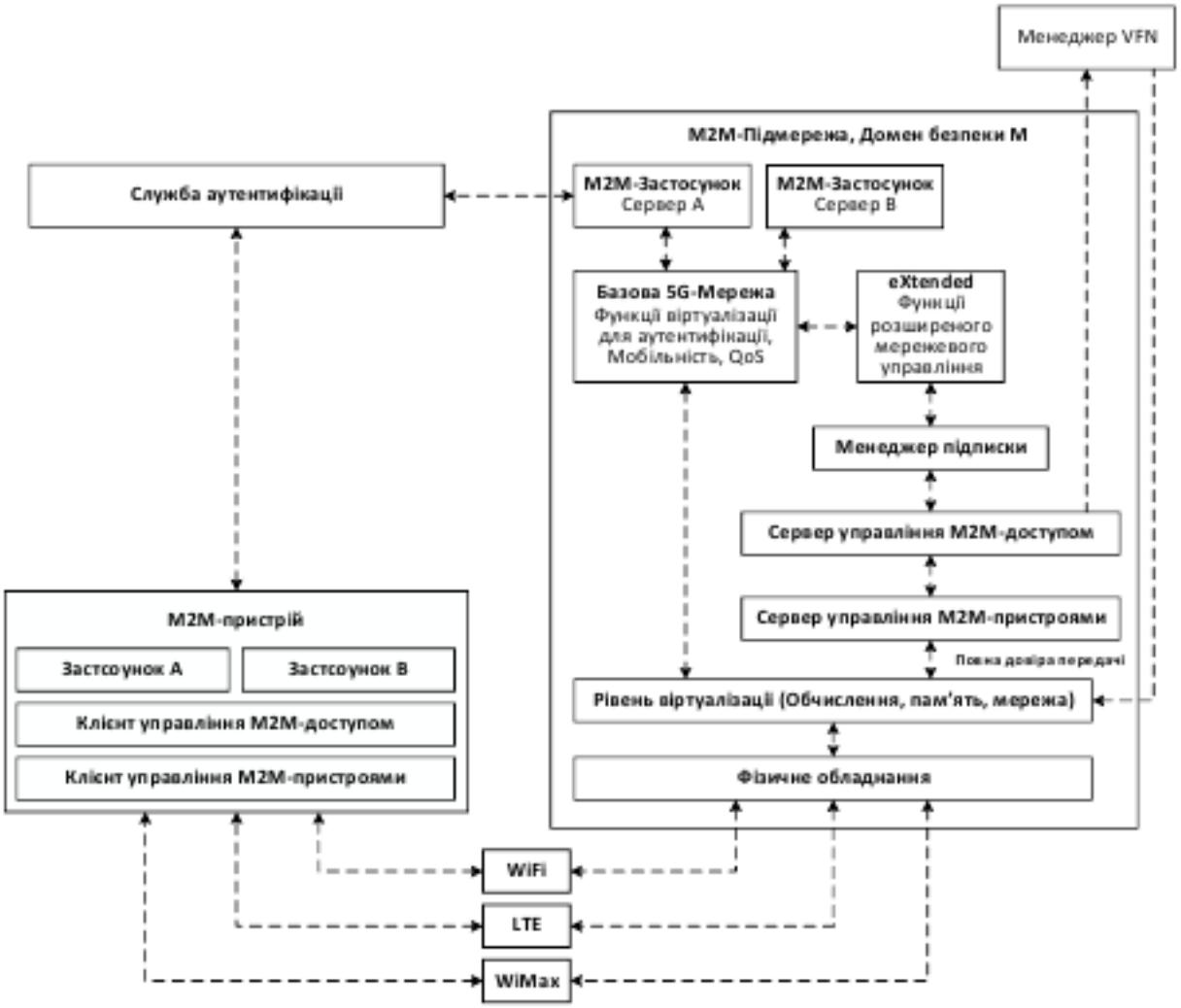

Рисунок 2.5 – Концептуальна модель 5G M2M [34]

Концепція модель містить процедуру управління підпискою, в якій задіяно MAC-сервер з використанням інтерфейсу до функції розширеного мережевого управління 5G eXtended. Щоб виконати автоматичне включення пристрою шляхом генерації нових ідентифікаторів та облікових даних для підключення «розумних» пристроїв через 3GPP.

Оскільки стандартна базова 5G мережа не підтримує жодного сервісного інтерфейсу, то сервер абонентів потрібно розширити з використанням HTTP REST інтерфейсу на основі протоколу SCIM [39]. А управління UDM-підпискою потрібно розширити подібним чином через службу «ParameterProvision». NEF надає послугу додавання користувачів шляхом передачі запитів до UDM. При ґенерації ідентифікаторів основна

мережа використовує політики розподілу ідентифікатора класу QoS на основі виявлених характеристик пристрою, зокрема виробник, назва товару.

Одним з протоколів управління пристроями, який можна використовувати для розподілу та завантаження прав доступу та власності, є протокол OMA LWM2M [40], сформований на основі протоколу CoAP [41].

Таким чином, для взаємного автентифікованого початкового завантаження «розумного» пристрою, який відокремлюється від системи, котра його створила, наприклад, виробник чи постачальник «розумного» пристрою, і підключається до системи, яка в подальшому буде ним керувати (покупець смарт-пристрою), буде використовуватись JSON Web Tokens (JWT) згенерований сторонньою службою автентифікації, котра може бути додана під час процедури завантаження, з метою забезпечення надійної взаємодії та передачі між доменами безпеки на базі мереж 4G або 5G.

2.5 Висновок до другого розділу

В другому розділі кваліфікаційної роботи описано класифікацію спеціалізованих та сенсорних мереж. Досліджено архітектура спеціалізованих та сенсорних мереж. Запропоновано класифікацію сутностей M2M-архітектури та описано основні складові її доменів. Виконано концептуальне проєктування M2M-взаємодії.

3 МЕТОДИ ТА ЗАСОБИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ МЕРЕЖ ДЛЯ МІЖМАШИННОЇ ВЗАЄМОДІЇ ТА IOT-КОМУНІКАЦІЇ

3.1 Аналіз загроз що виникають в мережах для M2M та IoT-взаємодії

Метою формування класифікації загроз є фіксація поточної ситуації щодо загроз для мереж, що призначені для M2M та IoT-взаємодії. Це дозволить динамічно розставити пріоритетність загроз, упорядкувати їх, змінити та деталізувати процедури визначення та діагностування. Класифікація загроз є динамічною сутністю, коту доцільно використовувати для систематизації розуміння процесів виникнення загроз на основі накопиченої інформації.

Поточна класифікація загроз (див. рисунок 3.1) базується на таксономії загроз ENISA, яка зібрала та об’єднала численні загрози з різних джерел в єдиний та структурований каталог загроз [42]. Під час формування класифікації загроз було проаналізовано обширний перелік відомих на даний час каталогів загроз для консолідації інформації щодо безпеки та управління ризиками в мережах для для забезпечення M2M та IoT-комунікації.

Подамо короткий опис вразливостей та ризиків для спеціалізованих та сенсорних мереж для забезпечення M2M та IoT-комунікації.

3.1.1 Вразливості спеціалізованих та сенсорних мереж

Спеціальні та сенсорні мережі, подібні до будь-якої іншої IT-системи, страждають від нових загроз та незадокументованих вразливих місць у кожному з п’яти вище перелічених доменів. Здебільшого загрози спеціалізованих та сенсорних мереж пов’язані із втратою конфіденційності, цілісності, доступності та достовірності [43].

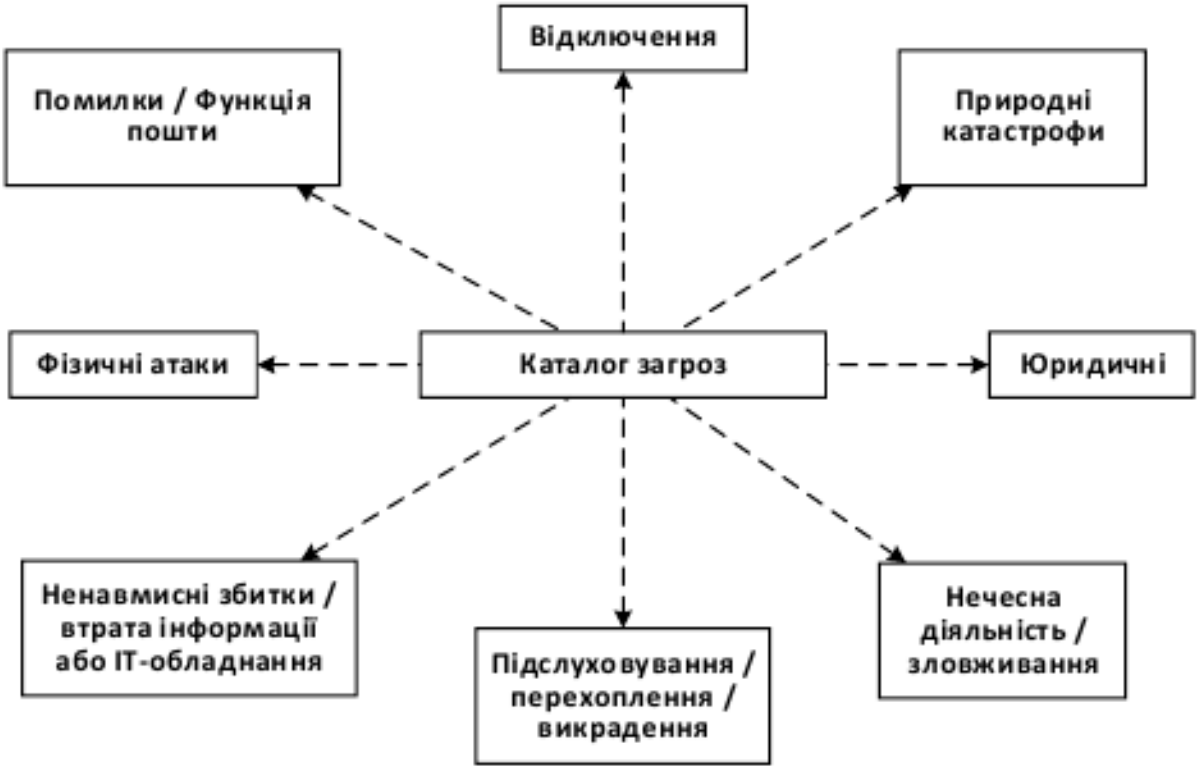

Рисунок 3.1 – Класифікація загроз в мережах для забезпечення M2M та IoT-комунікації

Конкретніше, основні вразливі місця в цих мережах стосуються безпеки пристроїв, захисту даних, цілісності та доступності засобів зв’язку, зокрема, протоколів та апаратного забезпечення, доступності бізнес-процесів, конфіденційності та стабільності функціонування. Захист M2M та IoT-пристроїв, в основному, забезпечується за допомогою методів автентифікації та відповідних інструментів контролю. Методи автентифікації разом з класифікацією даних спрямовані на забезпечення захисту даних. Завдяки належному та своєчасному управлінню та спеціалізованим методам протоколів мережевий зв’язок може бути забезпечений належним чином. Процедури управління ризиками також призводять до доступності бізнес-процесів та стабільності роботи.

Вичерпання ресурсів пристроїв є вразливістю спеціалізованих і сенсорних мереж через природу цих пристроїв. Зазвичай це пристрої невеликих розмірів з низьким рівнем енергоспоживання [44]. Це можна

усунути за допомогою адекватної та своєчасної класифікації даних, відповідного забезпечення необхідних процедур управління, моделювання, візуалізації та тестування.

Використання безпровідного зв’язку [45] в спеціалізованих та сенсорних мережах для забезпечення M2M та IoT-комунікації потенційно може спричинити певні вразливості, пов’язані з природою фізичного середовища каналу зв’язку. Водночас присутні вразливості внаслідок перехоплення та перешкод, що використовуються у випадку використання RFID, Bluetooth, NFC та Zigbee [46].

Ще одним типовим прикладом є порушення контролю доступу, яке використовує вразливості, що виникають через незашифровані передачі, спричинені окремими конкретними протоколами, що використовуються для бездротового зв’язку між пристроєм зчитування контролю доступу (наприклад, пристроєм зчитування RFID) та пристроєм контролера.

3.1.2 Ризики спеціалізованих та сенсорних мереж

Множина ризиків впливає на елементи та діяльність спеціалізованих та сенсорних мереж що використовуються для M2M та IoT-комунікації. Ці мережі часто можна використовувати для недоброзичливих дій та атак внаслідок підслуховування, що призводять до високого ризику втрати даних. Оскільки зазначені мережі мають різні типи фізичних локацій та середовищ, зокрема можуть бути встановлені під водою, під землею тощо, то ризик втрати пристроїв у разі природних або екологічних катастроф, наприклад землетрус, повені чи торнадо є значним [47].

Різноманітність фізичного розташування спеціалізованих та сенсорних мереж, обмеженість ресурсів пристроїв та топологія мереж можуть призвести до витоку особистих або конфіденційних даних. Слід відзначити, що поведінка, пов’язана з витоком конфіденційності [48] в спеціалізованих та сенсорних мережах, може загрожувати навіть людським життям.

Запобігання проявам нечесної діяльності може бути здійснено за допомогою жорсткішого управління ризиками та оперативного контролю, а також за допомогою наявності спеціалізованих інструментів та методів, що дозволяють їх мінімізувати. Крім того, можуть бути застосовані різні інші методи управління ризиками, наприклад, ранжування та рейтингування ризиків, матриці ризиків, формування ланцюжків послідовностей при визначенні пріоритетів ризиків, представлення складних даних про ризики та полегшення процедур проведення оглядів та перевірок для розподілу доступних ресурсів та методів.

Слід зазначити, що оцінювання ризиків є постійною та неперервною процедурою, а постійний моніторинг мережі є обов'язковою необхідністю. Постійний зворотний зв'язок та оцінка ризиків від зацікавлених сторін, безумовно, будуть спричинятимуть додаткові фінансові витрати в будь-який момент цієї процедури.

3.1.3 Процедури валідації в спеціалізованих мережах для забезпечення M2M та IoT-комунікації

В процедурах валідації в спеціалізованих мережах для забезпечення M2M та IoT-комунікації приймають участь M2M-клієнт та MAC-сервер 5G котрі можна реалізувати на основі прототипів Open5GMTC, а Open5GCore [49]. При цьому їх функціонал доцільно розширити для підтримки протоколу SCIM як для HSS в EPC, так і для UDM в компонентах 5G-систем, які обробляють автентифікацію «розумних» пристроїв з функціональним наборами для забезпечення M2M та IoT-комунікації.

Елементи функціональної функціональної архітектури, сформованої на основі Open5GMTC подано на рисунку 3.2.

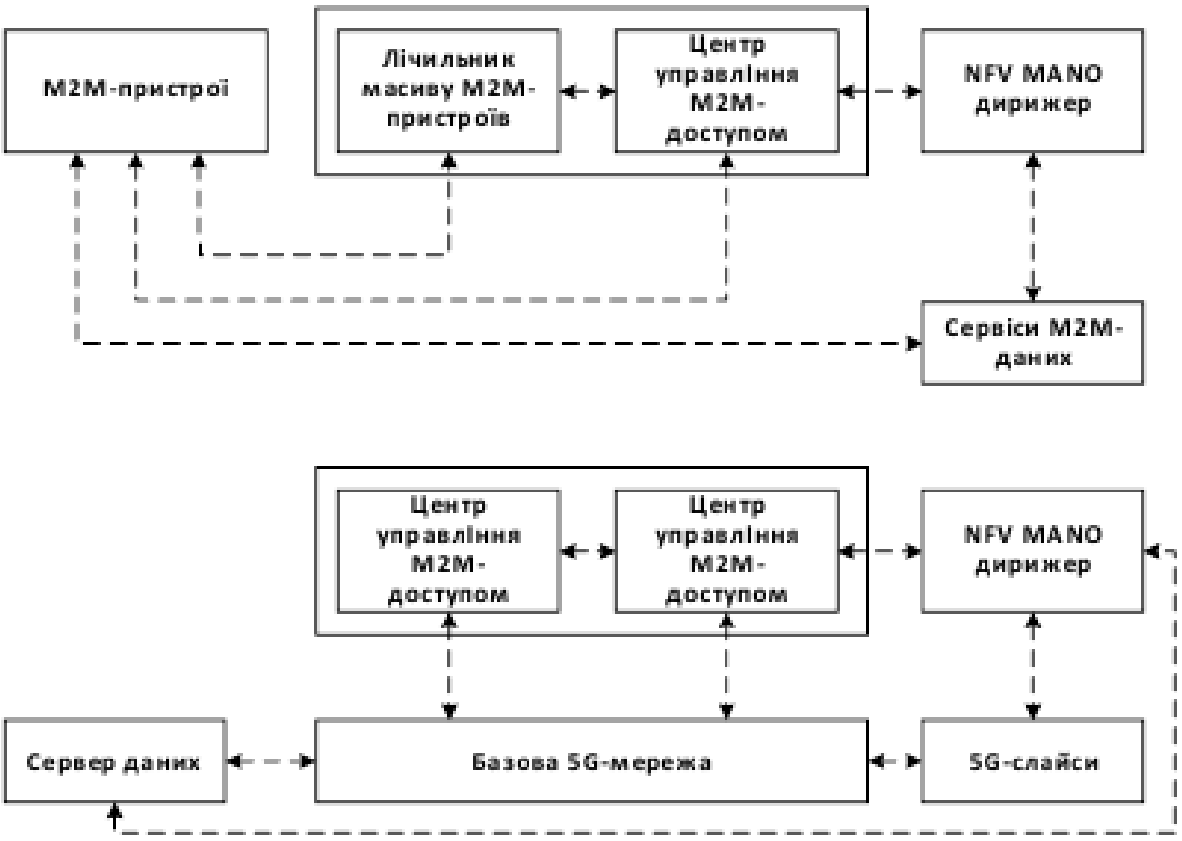

Рисунок 3.2 – Функціональна архітектура, сформована на основі Open5GMTC

Прототип Open5GMTC [50] дозволяє гнучке налаштування підтримуваного функціоналу для конкретного випадку використання. Він може використовуватися разом з розширеним NEF для надання динамічних ідентифікаційних даних або використання статичних даних для мереж на кшталт WiFi.

3.1.4 Процедури та потоки повідомлень в спеціалізованих мережахдля забезпечення M2M та IoT-комунікації

На рисунку 3.3, під час процедури завантаження, клієнт контролю доступу M2M реєструється на сервері контролю доступу M2M. Останній визнає, що кінцевий пристрій підтримує інтерфейс 4G або 5G, перевіряючи при цьому зареєстровані об’єкти управління. Для цього відбувається HSS-запит для 4G або NEF та UDM для 5G виділити та додати користувача.

Облікові дані користувача будуть передані клієнту контролю M2M-доступу. Далі клієнт контролю M2M-доступу пройде процедуру встановлення IP-з'єднання шляхом автентифікації до базової мережі з отриманими обліковими даними. Це відбудеться в узагальненій формі, як запит на приєднання, автентифікацію та приєднання завершено, у випадку EPC.

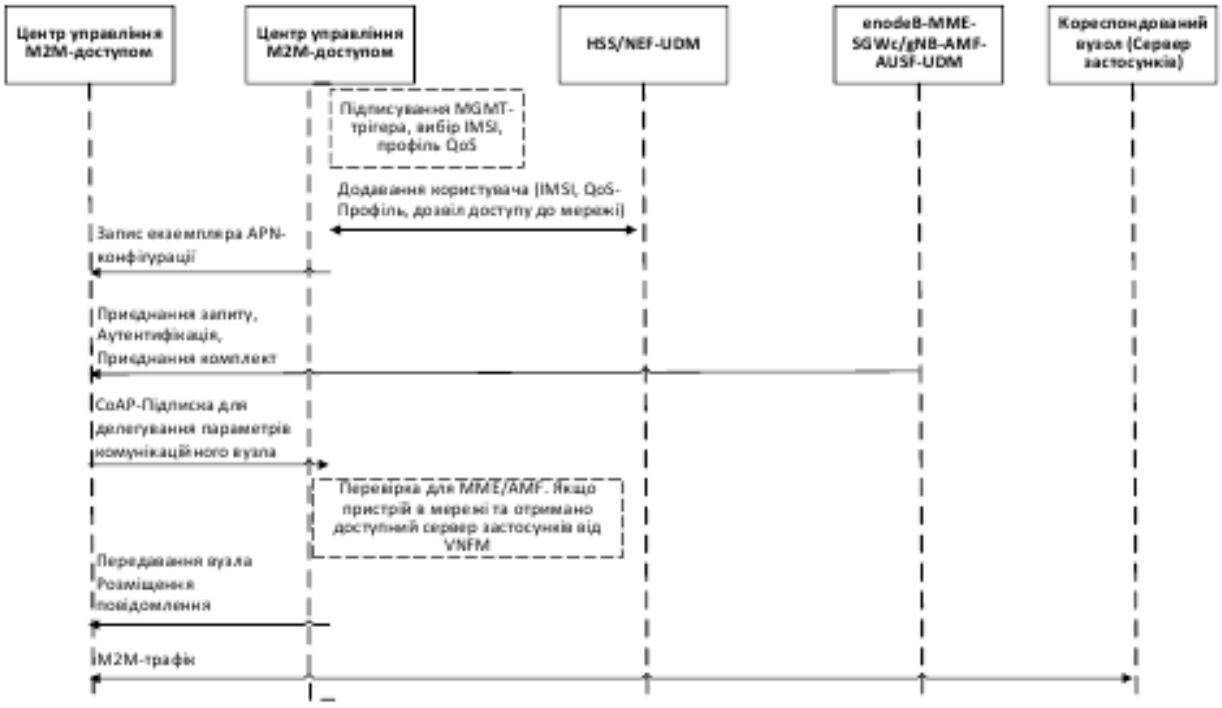

Рисунок 3.3 – Потік повідомлень для забезпечення надійного передавання даних в спеціалізованих мережах M2M та IoT-комунікації

Для виявлення відповідного вузла клієнт контролю M2M-доступу підписується на нестандартний об'єкт управління політикою управління транспортом і отримує повідомлення, що містить параметри зв'язку, призначені сервером контролю M2M–доступу. Наприклад, IP-адреса, протокол, порт. Для розподілу відповідного вузла сервер контролю M2M-доступу повине виконати VNFM-запит про виділені сервери застосунків, які пов'язали ім'я служби з отриманою підпискою. За бажанням, сервер управління M2M-доступом перевірить, чи використовувана клієнтом контролю M2M-доступу IP-адреса, пов'язана з наданими обліковими даними.

На наступному етапі програма, що працює на кінцевому пристрої, може ініціювати M2M-зв’язок у напрямку до відповідного вузла.

3.1.5 Класифікація сутностей та сенсорів

Сутності можуть бути абстрактними, віртуальними (наприклад, дані), фізичними активами (кабелі, обладнання), людськими чи фінансовими ресурсами тощо [51]. Внаслідок проведено аналізу конкретних випадків використання, можна зробити висновок, що існує дуже велика кількість взаємопов’язаних пристроїв та значна кількість типів сутностей у спеціалізованих безпровідних та сенсорних мережах M2M та IoT-комунікації.

У домені M2M-пристроїв зафіксуємо пристрої, які здатні обробляти дані. Водночас у домені M2M-мереж зафіксуємо сутності, що забезпечують зв’язок між програмними застосунками. Додамо операційні аспекти та моделювання бізнес-процесів, щоб поєднати класичні функції та процеси із спеціальними розширеннями та можливостями мережевих систем. Програми обміну даними, системи управління, моніторингу та вимірювання можуть бути частиною декількох складніших бізнес-процесів, що забезпечують стандартизацію та взаємодію реалізацій рішень M2M та IoT-взаємодії. Спеціальні та сенсорні ресурси мережі ідентифікуються та класифікуються на основі будівельних блоків поданих вище доменів. Класифікація сутностей подана в таблиці 3.1.

3.2 Рекомендації щодо покращення рівня безпеки спеціалізованих мереж для M2M та IoT-комунікації

Подані вище недоліки безпеки спеціалізованих мереж для M2M та IoT-комунікації, потребують набору рекомендацій, які можуть покращити загальні показники безпеки.

Таблиця 3.1 – Класифікація сутностей

Домен	Сутність	
1	2	3
Домен M2M-застосунків	Дані	eHealth
	Критичні програми	Хмарні застосунки
Домен M2M-пристроїв	Автомобілі / транспортні засоби	Точка взаємозв’язку
	Мобільні пристрої	Системи підтримки
	RFID-мітки	Носимі пристрої
	RFID-зчитувачі	Системи позиціонування при приміщенні
	Радари	Пристрої комп’ютерної електроніки
	Вузли передачі	
Домен M2M-мереж	Протоколи зв’язку	Домашня автоматизація
	Системи охолодження	Радіо
	Блоки живлення	Інфраструктура відкритих ключів
Операційний домен	Фізична безпека	Комунальні послуги
	Системи управління	
Домен продуктів / бізнес-процесів	Постачання та забезпечення	Охорона здоров’я
	Виробництво	Транспортування

3.2.1 Організаційні рекомендації

В контексті атрибутів безпеки, спеціальний розвиток та розвиток сенсорної мережі можна посилити за допомогою нормативних документів, що містять відомості щодо стандартів та відповідності. Для цього доцільно сформувати функціональні, політичні та регулятивні рекомендації, які повинні містити чіткі та однозначні вказівки зацікавленим організаціям.

3.2.2 Функціональні рекомендації

В контексті атрибутів безпеки розвиток спеціалізованих та сенсорних мереж для забезпечення M2M та IoT-комунікації можна посилити за допомогою практик, які задокументовані відповідно до стандартів.

Зростає занепокоєння щодо привілеїв фізичних осіб, які мають доступ до сенсорних наборів даних для виконання різноманітних операцій управління (тобто операторів постачальника M2M-послуг). Це занепокоєння стосується більшості проблем управління даними спостереження в районах, що контролюються системами охорони замкнутого контуру, а також даних про позиціонування в приміщенні, в основному на ланцюгах поставок та потоках даних, що полегшує дистанційне M2M-управління побутовою технікою. Для цього дуже важливо визначити, хто отримує доступ до даних, та умови, які вони потребують для доступу до даних. Повинні бути визначені відповідні ролі для асоціювання кінцевих користувачів (наприклад, працівників постачальника послуг M2M, клієнтів) із конкретними сегментами зібраних даних та надання їм особливих привілеїв щодо обчислювальних операцій. Цю процедуру слід поєднувати із суворим контролем за спеціалізованими та сенсорними мережами з метою убезпечення процедур збирання конфіденційних даних. Окрім того, розробку та розгортання M2M-застосунків в хмарному у середовищі слід здійснювати шляхом адаптації та розширення вказівок щодо безпеки застосунків

організацій, що займаються стандартизацією, та охоплювати потреби та вимоги поданої вище M2M-архітектури.

3.2.3 Рекомендації щодо політики

У зв’язку з проблемами конфіденційності, які слід розглядати в спеціалізованих та сенсорних мережах, обмінюючись персональними, конфіденційними, конфіденційними даними, слід встановити конкретні правила щодо процедур санкціонування та обміну даними щодо сенсорних даних. З метою забезпечення належного рівня прозорості, слід розглянути політику, яка стосується визначення зобов’язань та опису управлінських операцій. Крім того, політика конфіденційності повинна чітко сформулювати причини та методи, які організовані для відбору та опрацювання сенсорних даних і механізмів, що пом’якшують загрози функціональним та операційним процедурам. Дотримання конфіденційності повинно забезпечуватися в контексті надійного та послідовного M2M-застосунка. Слід дотримуватися стандартизованої документації щодо дотримання конфіденційності. При цьому типовими прикладами є Аналіз порогового рівня конфіденційності (PTA) або Оцінка впливу на конфіденційність (PIA). Крім рівня конфіденційних даних, політика конфіденційності також пов’язана з додатковими документами. Наприклад, у секторі охорони здоров’я документи з поінформованою згодою пов’язані з цілями конфіденційності, які визначені інтегрованими спеціальними мережами, розгорнутими в лікарнях. Пацієнти мають повноваження контролювати та затверджувати концентрацію, а також обробку своєї конфіденційної інформації. Пацієнти можуть погодитись на розкриття своїх даних медперсоналу та лікарям.

На рівень безпеки програм M2M сильно впливають вразливості внутрішніх серверів. З цією метою згадані сервери слід оновлювати за допомогою виправлень безпеки, і вони також повинні підлягати управлінню

вразливостями. Складовими цього управління має бути технічна оцінка, а також переоцінка компетентної політики, яка визначає прийнятні методи проведення самої оцінки.

Безпека проектів повинна бути впроваджена для кожного рівня спеціалізованої мережі, а це означає, що на вищому рівні абстракції розробка політики управління паролями має велике значення для пом'якшення різних загроз. Однак до адаптації цього типу політики слід вирішити багато проблем, зокрема мутації паролів та інтервали часу, протягом яких відбуватиметься зміна паролів. Оперативне впровадження цієї політики повинно забезпечуватися в контексті її відповідності шляхом організації відповідного контролю та оцінок. Крім того, технічні практики, що використовуються для забезпечення RFID-взаємодії повинні відповідати стандартам та найсучаснішим механізмам безпеки.

3.2.4 Нормативні рекомендації

Збір та опрацювання персональних даних повинні виконуватися, з дотриманням обмежень. Зокрема слід орієнтуватись на європейську практику, а саме Директиви, такі як Загальний регламент про захист даних 2016/679 [52]. Однак основна інфраструктура програм та операцій M2M повинна відповідати нормативним рамкам безпеки та операцій щодо захисту персональних даних. Провайдери послуг спеціалізованих мереж повинні інформувати кінцевих споживачів про їх обов'язки (наприклад, надійні облікові дані, використання цифрових підписів) щодо приховування ідентифікаційних даних під час роботи мереж, особливо у випадках, коли організовуються MHN.

3.2.5 Рекомендації щодо бізнес-процесів / продуктів

Виробництво певної продукції, наприклад, GPS-приймачів чи

медичних давачів, повинно керуватися загрозами, щоб мінімізувати потенційні вразливості, які дозволять атакувати на етапах розгортання та розробки. Виробничі підприємства приймачів GPS також повинні знати про постійно зростаючу поверхню атаки своєї продукції. Операція GPS заснована на передачі сигналів між приймачем GPS та чотирма або більше супутниками. Ця транзакція сигналів відбувається так, що приймач GPS може встановити свої поточні три координати та синхронізувати годинник з атомними годинниками супутників. Метод, за яким працює GPS, може бути використаний через вразливості, які дозволяють підробляти атаки. Захисні прийоми, які можуть бути використані для створення захищеного від втручання GPS приймача, можуть застосовуватися лише під час їх виготовлення через відсутність у людей знань та ресурсів. Більше того, наскрізне шифрування має бути впроваджено під час зв'язку приймачів GPS та супутників. Тому це питання рекомендується вирішувати компаніям під час процедур проектування та моделювання.

У контексті вирішення шахрайських дій в M2M-архітектурі слід організувати активні функціональні процедури, протоколи та політику, спрямовані на забезпечення запобігання шахрайству та гарантій для кінцевих користувачів. Більш конкретно, кодекс поведінки та політика контролю за ризиком шахрайства складаються з мінімальних гарантій, які повинні бути визначені та включені в M2M-архітектуру за допомогою політики авторизації щодо зібраних даних. Ці попереджувальні гарантії на функціональному рівні повинні бути посилені механізмами виявлення шахрайства. Технічні рекомендації

З метою вдосконалення та надійної реалізації мереж давачів у зв'язку M2M, доцільно подати різні технічні рекомендації, з особливим акцентом на методи автентифікації та авторизації, активні та реактивні засоби захисту.

Рекомендації щодо автентифікації / авторизації. Потрібно прагнути підвищити безпеку в процесі аутентифікації, застосовуючи сильні або багатофакторні методи автентифікації (MFA), де це застосовно. Однак, що

стосується автентифікації пристроїв у спеціалізованих та сенсорних мережах длязабезпечення M2M та IoT-комунікації, будь-який пристрій може покладатися на автентифікацію на основі сертифікатів та на методи, які посилюють процедуру експлуатації, використовуючи безпечну мережеву реєстрацію. Крім того, еластичний тип механізму контролю доступу рекомендується включати в спеціальні та сенсорні мережі для M2M та IoT-комунікації. Зокрема доцільно проводити управління доступом на основі атрибутів. Посилені захищені пристрої можуть бути встановлені в незахищених місцях та без нагляду. В контексті зв'язку RFID між мітками та зчитувачами рекомендується виконання процесів аутентифікації на вищих пристроях, щоб асоціювати унікальні паролі з особами.

3.2.6 Рекомендація щодо активного захисту

В останні роки зростає занепокоєння щодо DdoS-атак та флудів, а також щодо витонченості сучасних методів атаки. Ботнети використовуються в DDoS-атаках на спеціальні та сенсорні мережі; через приховану природу ботів, ботнети можуть стати непередбачуваним супротивником. Водночас, спеціалізовані та сенсорні мережі орієнтовані на сферу дії, яку потрібно скомпрометувати, а пристрої зареєстровано в ботнетах, які виконують DDoS-атаки. Цього методу дотримувались під час американського інциденту, пов'язаного з критично важливою Інтернет-інфраструктурою, яка була вражена IoT-ботнетом на основі Mirai. Таким чином, незважаючи на організацію WIDS в контексті спеціалізованих мереж, рекомендується використовувати IDS по всіх вузьких місцях M2M-архітектури, зокрема на M2M-шлюзах. Після коригування цього показника будь-який вхідний небажаний трафік з M2M-пристроїв, націлений на сутності поза межами спеціальної мережі та мережі давачів, можна ідентифікувати та запобігти. З цією метою здійснюється моніторинг мережевого трафіку кожного підключеного до Інтернету пристрою та організовується попереджувальне

виявлення. Крім того, рекомендується забезпечувати постійне оновлення набору правил давачів IDS через строгі часові інтервали та дотримуючись надійних джерел підписів. Крім того, зважаючи на характеристики протоколів маршрутизації MANET, настійно рекомендується, щоб оцінка безпеки мережі в першу чергу була зосереджена на вразливостях протоколів маршрутизації.

3.2.7 Рекомендація щодо реактивної оборони

На основі WIDS неможливо реалізувати ідентифікацію експлойтів з нульовим днем. Робота захисних механізмів, що виконують глибоку перевірку пакетів (DPI), базується на підписах відомих атак. Таким чином, рекомендується створити захисну зону, що складається з медової мережі, поряд із спеціальною та сенсорною мережами. Ця мережа складається з каструль, що імітують роботу давачів. Медова мережа являє собою тип темної мережі, яка здатна виявити нові методи атак щодо нульових днів. Хмарні обчислення Mobile Edge рекомендується організувати так, щоб розвивати мережу. Робота медових мереж дозволяє відстежувати зловмисні дії з метою їх аналізу та збору інформації про напади та поведінку зловмисників. Слід використовувати мережу віртуальних сутностей, що імітують роботу давачів, та, у разі загрозливого інциденту, шкідливий трафік може бути розвантажений у хмарі Mobile Edge Cloud (MEC), щоб цей трафік реєструвався та контролювався. Через те, що процес розвантаження збільшує накладні витрати енергії, слід використовувати віртуальні машини, які працюють всередині МЕК, щоб уникнути обмежень продуктивності, що суперечать випадку використання давачів.

3.3 Висновок до третього розділу

В третьому розділі кваліфікаційної роботи проведено аналіз загроз, що

виникають в мережах для M2M та IoT-взаємодії. Описано процедури валідації в спеціалізованих мережах для забезпечення M2M та IoT-комунікації. Розглянуто процедури та потоки повідомлень в спеціалізованих мережах для забезпечення M2M та IoT-комунікації. Запропоновано класифікацію сутностей та сенсорів. Розроблено рекомендації щодо покращення рівня безпеки спеціалізованих мереж для M2M та IoT-комунікації.

4 РОЗРОБКА МОДЕЛІ КОМП’ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ПІДПРИЄМСТВА

Згідно завдання розробимо комп’ютерну мережу в середовищі моделювання Cisco Packet Tracer.

4.1 Побудова моделі захищеної комп’ютерної мережі

Комп'ютерна мережа організації складається з 3 маршрутизаторів, 6 комутаторів, 3 сервера, 3 точки доступу Wi-Fi (рис. 4.1).

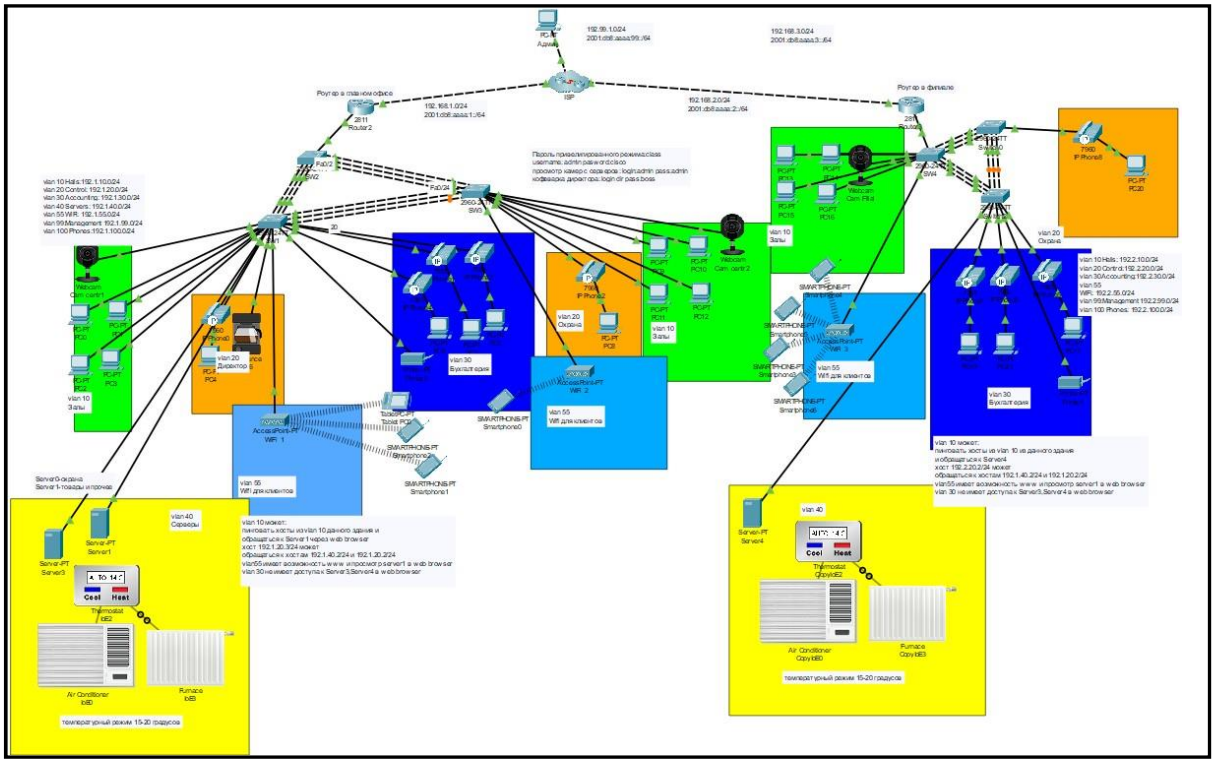

Рисунок 4.1 – Модель захищеної комп’ютерної мережі в програмі Cisco Packet Tracer

Маршрутизатори забезпечують маршрутизацію пакетів між різними фізичними мережами, вихід в інтернет, а також віддалений доступ для адміністратора. Комутатори працюють на рівнях "доступу" і "розподілу", вони комутують пакети між користувачами як з однієї підмережі VLAN, так і з різних.

Сервер являє собою високопродуктивну робочу станцію і настроюється під потреби користувачів організації. Він може представлятись як файлове сховище, центр обробки даних, DHCP-сервер, сервер камер відеоспостереження.

Точка доступу Wi-Fi використовує ЕМВ певної частоти, щоб надати користувачам доступ в локальну мережу.

Передбачається, що в організації є головний офіс та одна філія.

В головному офісі розташовується:

– два робочих кабінети по чотири комп’ютери та по одній IP-камері;

– кабінет бухгалтерії з трьома комп’ютерами та трьома IP-телефонами;

– кабінет охорони з одним комп’ютером та одним IP-телефоном;

– кабінет директора має один комп’ютер, один IP-телефон та кавову машину;

– серверна кімната з двома серверами (перший сервер призначений для охорони, другий для бази даних клієнтів та товарів) та з контролем температури в проміжку 15-20 градусів.

В філіалі розташовується:

– робочій кабінет з чотирма комп’ютерами та з однією IP-камерою;

– кабінет бухгалтерії з трьома комп’ютерами та трьома IP-телефонами;

– кабінет охорони з одним комп’ютером та одним IP-телефоном;

– серверна кімната з одним сервером та з контролем температури впроміжку 15-20 градусів.

Корпоративна мережа для даного підприємства є розподіленою мережею. Вона включає в себе високу пропуску здатність, має IP телефонію, а також високий ступінь захищеності.

4.2 Маршрутизація між мережами VLAN

VLAN (Virtual Local Area Network, віртуальна локальна мережа) – це функція в роутерах і комутаторах, що дозволяє на одному фізичному мережевому інтерфейсі (Ethernet, Wi-Fi інтерфейсі) створити кілька віртуальних локальних мереж. VLAN використовують для створення логічної топології мережі, яка ніяк не залежить від фізичної топології. Дана технологія дозволяє гнучко налаштувати використання мережевих ресурсів в залежності від завдань користувачів конкретного VLAN.

При введенні VLAN необхідно налаштувати маршрутизацію, щоб користувачі з різних підмереж могли взаємодіяти один з одним. В даному бюджетному рішенні застосовується статична маршрутизація, що підходить для малих підприємств, у яких рідко з'являються і / або видаляються пристрої.

Статична маршрутизація – це вид маршрутизації, при якому маршрути вказуються в явному вигляді при конфігурації маршрутизатора.

При установці статичного маршруту вказується:

– Адреса мережі (на яку маршрутизується трафік), маска мережі;

– Адреса шлюзу (вузла), який сприяє подальшій маршрутизації (абопідключений до маршрутизації мережі безпосередньо).

Для забезпечення узгодженості дій всіх маршрутизаторів в мережі, мінімізації помилок і спрощення роботи адміністратора застосовуються мережеві протоколи маршрутизації, які регламентують вибір найбільш оптимального маршруту слідування пакету даних в мережах.

Розрізняють два види маршрутизації: програмна та апаратна.

– Програмна маршрутизація – це спеціалізоване програмне забезпечення, встановлене на комп’ютері з кількома мережевими інтерфейсами, які входять до складу різних мереж.

– Апаратна маршрутизація здійснюється спеціальним обладнанням, здатним аналізувати і перенаправляти вхідні потоки даних.

Динамічна маршрутизація – вид маршрутизації, при якому таблиця маршрутизації редагується програмно.

Демони маршрутизації обмінюються між собою інформацією, яка дозволяє їм заповнити таблицю маршрутизації найбільш оптимальними маршрутами. Протоколи, за допомогою яких проводиться обмін інформацією між демонами, називаються протоколами динамічної маршрутизації.

Кожен протокол маршрутизації працює з пакетами даних, які відносяться до одного з існуючих протоколів. У процесі обробки інформації протокол визначає формат пакета даних, виділяє адресу одержувача і будує маршрут подальшого проходження сигналу.

В даному бюджетному рішенні застосовується протокол EIGRP (Enhanced Interior Gateway Routing Protocol) – вдосконалений дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco.

EIGRP має безліч переваг в порівнянні з протоколом RIP (Routing Information Protocol) і своїм безпосереднім попередником, протоколом IGRP (Interior Gateway Routing Protocol). По суті, EIGRP – це розширена версія протоколу IGRP. Як і RIP, IGRP відомий як дистанційно-векторний протокол, але в порівнянні з ним він має поліпшені характеристики алгоритму розрахунку оптимального шляху до пункту призначення.

Метрики IGRP ґрунтуються на таких параметрах як смуга пропускання і затримка, в той же час для протоколу RIP важливим є довга маршруту, виражена в «хопах», тобто кількості вузлів на шляху прямування.

Основними перевагами EIGRP є:

– низьке споживання мережевих ресурсів в режимі нормальної експлуатації (в умовах стабільної мережі передаються тільки пакети"hello")

– при виникненні змін по мережі передаються тільки зміни, що відбулися в маршрутної таблиці, а не вся таблиця цілком. Це дозволяє зменшити навантаження на мережу, створювану протоколом маршрутизації

– малий час конвергенції в разі зміни в топології мережі (в

окремих випадках збіжність забезпечується майже миттєво).

4.3 Налаштування розширених списків контролю доступу ACL

Списки контролю доступу є список правил для обробки мережевого пакету, який визначає необхідні дії для його обробки. Списки контролю доступу корисні для фільтрації, приорітизації інформації, а також для її вибіркової обробки в залежності від необхідності. Перевага розширених ACL полягає в тому, що вони можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і TCP / UDP порти, а не тільки адреси джерел

4.4 Налаштування зв'язку між філіями

Проводиться об'єднання кількох філій в рамках одного міста в масштабну локальну мережу (рис. 4.2) – WAN. Для забезпечення надійності також налаштовується резервний канал зв'язку між філіями.

4.5 IP-телефонія

IP-телефонія (або VoIP – Voice over Internet protocol) – технологія (рисунок), яка використовує мережу з пакетною комутацією повідомлень на базі протоколу IP для передачі голосу в режимі реального часу (рис. 4.3).

При розмові наші голосові сигнали перетворюються в пакети даних, які потім стискаються. Далі ці пакети даних посилаються через Інтернет приймальній стороні. Коли пакети даних досягають адресата, вони декодуються в аналоговий голосовий сигнал.

IP-телефонія в чистому вигляді може застосовуватися в якості ліній передачі голосу, для чого можуть використовуватися спеціально виділені цифрові канали. На відміну від аналогової телефонії, IP-телефонія створює "підключення по запиту" і не має зарезервованих ліній зв'язку, що зменшує витрати на телефонні розмови.

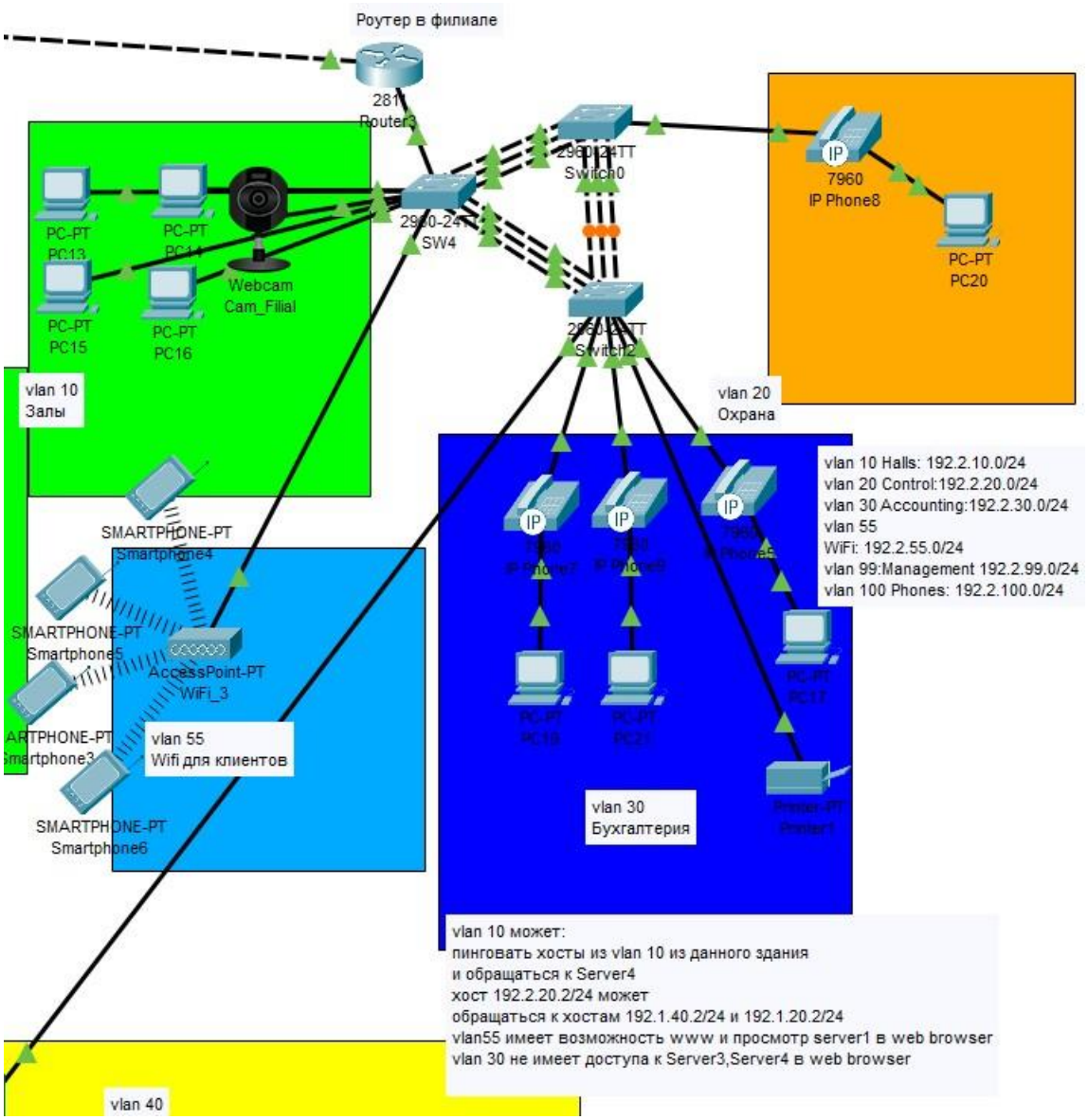

Рисунок 4.2 – Налаштування зв'язку між філіями

Переваги, особливості та підтримувані функції:

– Передача голосового та факсимільного трафіку через IP. Як транспорт можуть використовуватися будь-які середовища (виділені лінії, ISDN, Frame Relay, Ethernet, Token Ring, ATM).

– Рішення засновані на єдиній лінії маршрутизаторів Cisco і не вимагають додаткового апаратного забезпечення.

– Модульна, нарощувана архітектура.

– Передача голосу і факсів через один порт.

– Сумісність зі стандартом H.323.

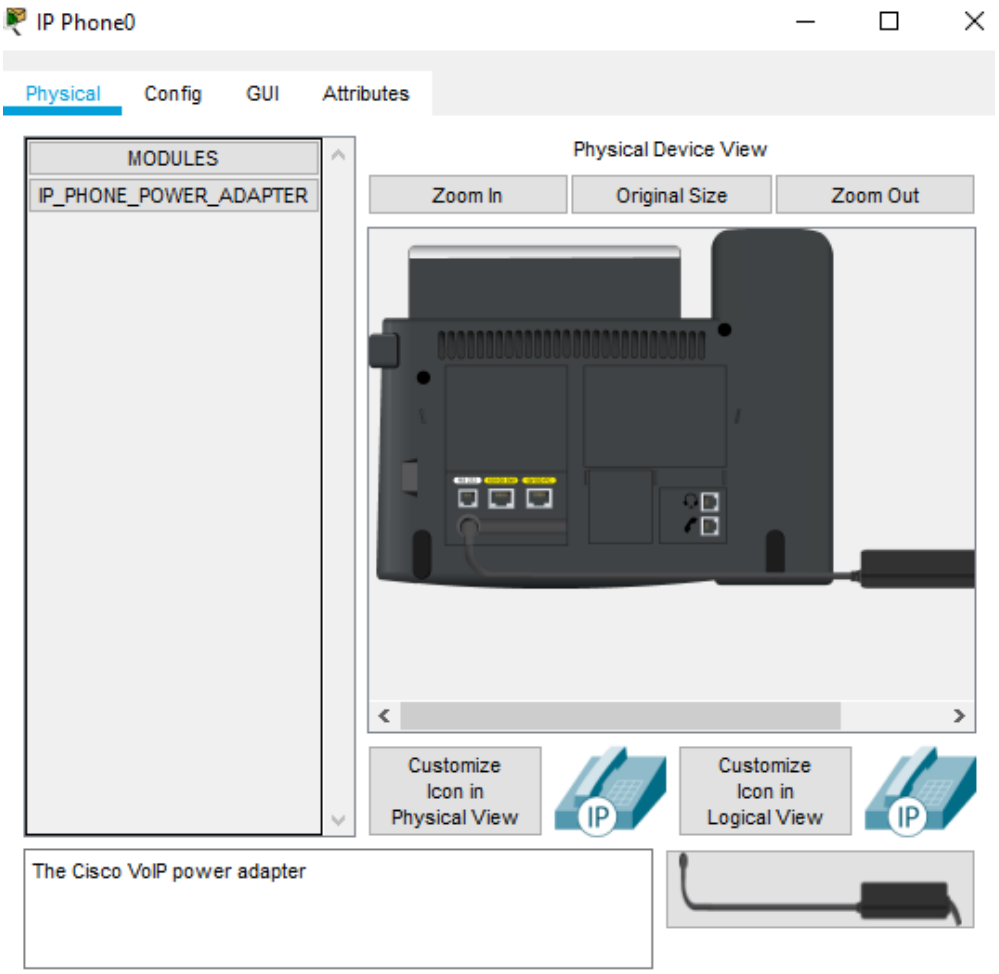

Рисунок 4.3 – Вигляд IP-телефонії в Cisco Packet Tracer

– Висока продуктивність, заснована на використанні DSP (цифрових сигнальних процесорів).

– Підтримка протоколів компресії голосу G.729 і G.711, дозволяє передавати один голосовий канал зі швидкістю 8 kbps.

– Висока якість голосових з'єднань засноване на використанні RSVPархітектури і черг з пріоритетами.

– Придушення пауз.

– Симуляція шумів в лінії.

– Розвинуте управління планом внутрішньої нумерації і відображенням IP-адрес на цей план.

– Підтримка DTMF.

– Підтримка протоколу T.30. (Передача факсів).

– Виділена телефонна лінія (наскрізне з'єднання).

При звичайному способі передачі мови (аналогової телефонії) використовується канал пропускною спроможністю 64 Кбіт / с незалежно від того, розмовляє абонент або мовчить під час з'єднання. У разі передачі мови по IP-мереж, за рахунок оцифровки і компресії (стиснення), мова передається у вигляді цифрової інформації, причому якщо абонент мовчить або робить паузи в розмові, цифрова інформація в канал не передається і канал не заповнюється. Це дозволяє в одному каналі 64 Кбіт / с передавати від 8 і більше з'єднань одночасно, що в свою чергу забезпечує зниження тарифів, і, відповідно, оплата зменшується.

4.6 Налаштування протоколів захисту

4.6.1 Налаштування віддаленого доступу адміністратора по протоколу SSHv2

У разі неполадок в мережі адміністратора не обов'язково знаходиться поруч з обладнанням – ви можете надати йому віддалений доступ з безпечного протоколу SSHv2

4.6.2 Налаштування протоколу DHCP

DHCP – протокол прикладного рівня моделі TCP / IP, служить для призначення IP-адреси клієнта. Це випливає з його назви – Dynamic Host Configuration Protocol. IP-адресу можна призначати вручну кожного клієнта, тобто комп'ютера в локальній мережі. Але у великих мережах це дуже трудомісткий, до того ж, чим більше локальна мережа, тим вище зростає ймовірність помилки при налаштуванні. Тому для автоматизації призначення IP був створений протокол DHCP.

Протокол DHCP дозволяє здійснювати автоматичну настройку мережевих пристроїв. Налаштування DHCP сервера на маршрутизаторі вигідна тим, що дозволяє по максимум задіяти працює маршрутизатор, повісивши на нього максимальну кількість функціоналу (інтернет, NAT, DHCP і т.п.). DCHP дозволить маршрутизатора автоматично налаштовувати

на клієнтах наступні основні параметри:

– IP адреса;
– Основний шлюз;
– Маска підмережі;
– DNS сервера;
– ім'я домену.

Робота протоколу DHCP здійснюється за принципом клієнт-сервер. Для отримання налаштувань використовується схема DORA (Discover-Offer-Request-Acknowledge). Сам процес складається з наступних етапів:

– Виявлення (Discover). Після підключення клієнта починається процес його ініціалізації в мережі. Він знаходить відповідний DHCP-сервер шляхом відправки спеціального запиту DHCPDISCOVER на адресу 255.255.255.255. З огляду на відсутність власного IP, в такому запиті вказується 0.0.0.0 і MAC. Запит надходить на всі ПК у відповідному сегменті мережі. При цьому відповідь на нього автоматично відправляється тільки DHCP-серверами.

– Пропозиція (Offer). Отримавши від клієнта запит, DHCP-сервер здійснює його обробку і виконує підбір мережеву конфігурацію. Ця конфігурація направляється клієнту прийде в повідомленні DHCPOFFER, яке, як правило, передається на вказаний MAC. Однак в деяких випадках застосовується широкомовлення. При знаходженні декількох серверів в межах мережі клієнтові приходить відповідну кількість DHCPOFFER, з яких він вибирає один (зазвичай перший за часом отримання).

– Запит (Request). Після отримання DHCPOFFER клієнт передає серверу спеціальне повідомлення DHCPREQUEST, яке містить запит налаштувань. У цьому запиті дублюється інформація з DHCPDISCOVER, а також вказує IP-адреса обраного на попередньому етапі DHCP-сервера.

– Підтвердження (Acknowledge). Після отримання DHCPREQUEST обраний DHCP-сервер виконує фіксацію відповідної прив'язки для клієнта і направляє йому у відповідь повідомлення DHCPACK.

У ньому підтверджуються надані автоматично настройки. Це повідомлення передається на адресу MAC клієнта, яка була вказана на попередньому етапі. Отримавши DHCPACK, клієнт проводить автоматичну перевірку наданих налаштувань і застосовує конфігурацію мережі, отриману від сервера.

4.6.3 Налаштування протоколу NAT

Мережі зазвичай проектуються з використанням приватних IP адрес. Це адреси 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16. Ці приватні адреси використовуються всередині організації або майданчика, щоб дозволити пристроям спілкуватися локально, і вони не маршрутизуються в інтернеті. Щоб дозволити пристрою з приватним IPv4-адресою звертатися до пристроїв і ресурсів за межами локальної мережі, приватний адресу спочатку повинен бути переведений на загальнодоступний публічний адресу.

І ось якраз NAT переводить приватні адреси, в загальнодоступні. Це дозволяє пристрою з приватною адресою IPv4 звертатися до ресурсів за межами його приватної мережі. NAT в поєднанні з приватними адресами IPv4 виявився корисним методом збереження загальнодоступних IPv4-адрес. Один загальнодоступний IPv4-адрес може бути використаний сотнями, навіть тисячами пристроїв, кожен з яких має приватний IPv4-адрес. NAT має додаткову перевагу, що полягає в додаванні ступеня конфіденційності і безпеки в мережу, оскільки він приховує внутрішні IPv4-адреси з зовнішніх мереж.

Маршрутизатор з підтримкою NAT можуть бути налаштовані з одним або декількома дійсними загальнодоступними IPv4-адресами. Ці загальнодоступні адреси називаються пулом NAT. Коли пристрій з внутрішньої мережі відправляє трафік з мережі назовні, то маршрутизатор з підтримкою NAT переводить внутрішній IPv4-адрес пристрою на загальнодоступний адреса з пулу NAT. Для зовнішніх пристроїв весь трафік, що входить і виходить з мережі, виглядає мають загальнодоступний IPv4 адресу.

4.6.4 Налаштування обладнання на протоколі IPv4 та IPv6

Налаштоване обладнання для адресації по протоколам IPv4, а також по більш сучасному IPv6.

Основна зовнішня відмінність четвертої і шостої версії протоколу – структура IP-адреси. IPv4 використовує чотири однобайтових десяткових числа, між якими ставиться крапка (172.268.0.1). IPv6 – шістнадцяткові числа, розділені двокрапкою (fe70 :: d5a9: 4521: d1d7: d8f4b11) [4].

4.6.5 Налаштування протоколу STP

STP (Spanning Tree Protocol) – мережевий протокол (або сімейство мережевих протоколів) призначений для автоматичного видалення циклів (петель комутації) з топології мережі на канальному рівні в Ethernet-мережах (рис. 4.4).

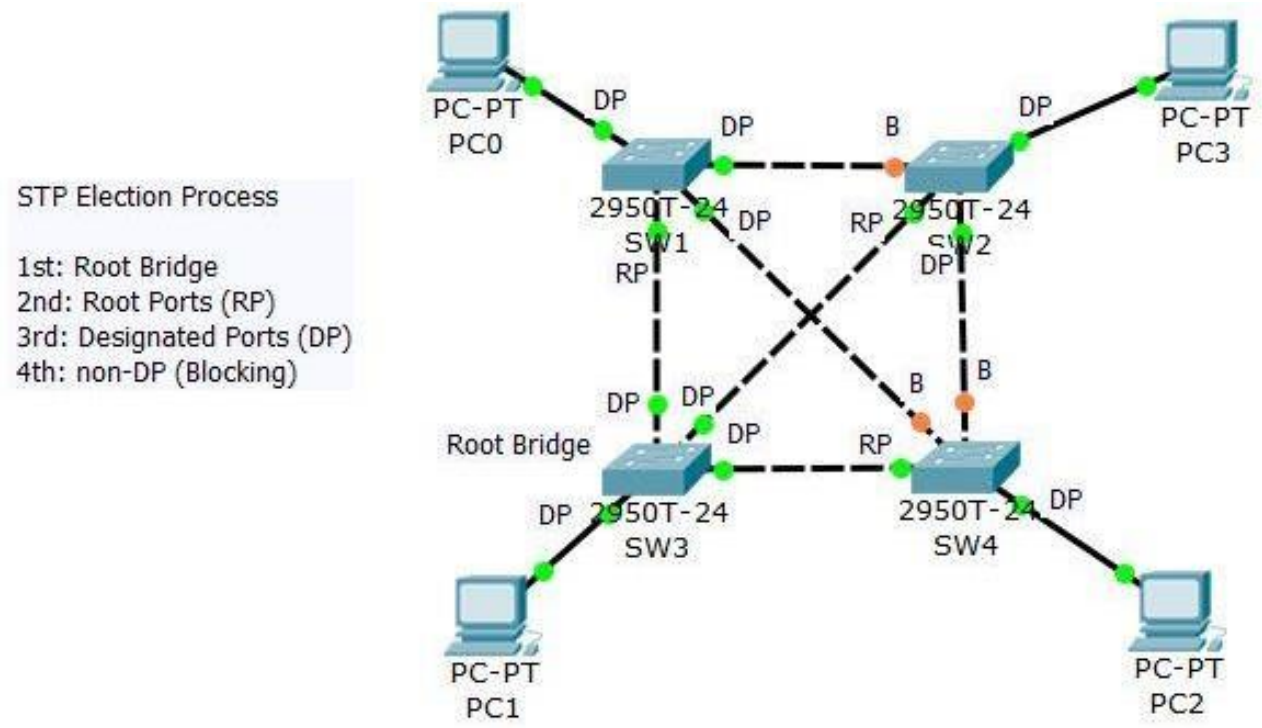

Рисунок 4.4 – Алгоритм дії протоколу STP

Алгоритм дії STP:

– Після включення комутаторів в мережу, за замовчуванням кожен комутатор вважає себе кореневим (root).

– Кожен комутатор починає посилати по всіх портах конфігураційні Hello BPDU пакети раз в 2 секунди, максимальний проміжок 20 секунд.

– Якщо міст отримує BPDU з ідентифікатором моста (Bridge ID) меншим, ніж свій власний, він припиняє генерувати свої BPDU і починає ретранслювати BPDU з цим ідентифікатором. Таким чином в кінці кінців в цій мережі Ethernet залишається тільки один міст, який продовжує генерувати і передавати власні BPDU. Він і стає кореневим мостом (root bridge).

– Решта мости ретранслюють BPDU кореневого моста, додаючи в нихвласний ідентифікатор і збільшуючи лічильник вартості шляху (pathcost).

– Для кожного сегмента мережі, до якого приєднані два і більше портів мостів, відбувається визначення designated port – порту, через який BPDU, що приходять від кореневого моста, потрапляють в цей сегмент.

– Після цього всі порти в сегментах, до яких приєднані 2 і більше портів моста, блокуються за винятком root port і designated port.

– міст продовжує посилати свої Hello BPDU раз в 2 секунди.

RSTP або як його ще називають у більш розгорнутому вигляді Rapid spanning tree protocol, по суті той же STP але більш швидкий де час збіжності мить, ви втратите один пакет. Включити RSTP можна командою з режимі глобального конфігурування, де потрібно змінити режим на rapid-pvst.

4.6.6 Налаштування протоколу EtherChannel

Etherchannel (рис. 4.5) – це технологія, що дозволяє об'єднувати (агрегувати) кілька фізичних проводів (каналів, портів) в єдиний логічний інтерфейс. Як правило, це використовується для підвищення відмовостійкості і збільшення пропускної здатності каналу. Зазвичай, для з'єднання критично важливих вузлів (комутатор-комутатор, комутатор-сервер).

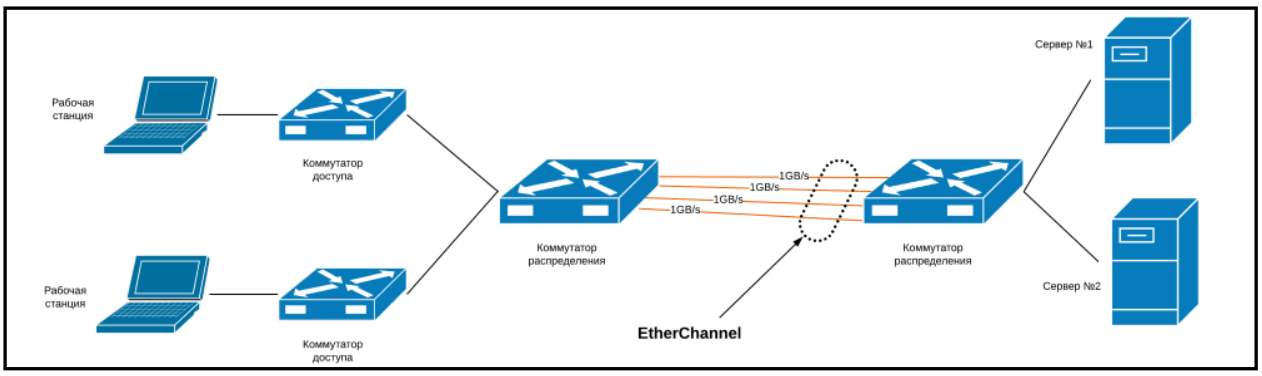

Рисунок 4.5 – Налаштування протоколу EtherChannel

Технологія EtherChannel має багато переваг.

– Більшість завдань конфігурації виконується на інтерфейсі EtherChannel, а не на окремих портах. Це забезпечує узгоджену конфігурацію на всіх каналах.

– EtherChannel використовує існуючі порти комутатора. Для забезпечення більш високої пропускної здатності не потрібно дорога заміна каналу на більш швидкий.

– Між каналами, які є частиною одного і того ж EtherChannel, відбувається розподіл навантаження. Залежно від використовуваного обладнання може бути реалізований один або кілька методів балансування навантаження.

– EtherChannel створює об'єднання, яке розглядається, як один логічний канал. Якщо між двома комутаторами існує декілька об'єднань EtherChannel, протокол STP може блокувати одне з об'єднань, щоб уникнути петель комутації.

– EtherChannel надає функції надмірності, оскільки загальний канал вважається одним логічним з'єднанням. Крім того, втрата одного фізичного з'єднання в межах каналу не призводить до зміни в топології. Тому перерахунок дерева найкоротших шляхів не потрібно.

– EtherChannel продовжує працювати навіть в тому випадку, якщо загальна пропускна здатність знижується через втрати з'єднання в межах EtherChannel.

4.6.7 Налаштування протоколу SSHv2

SSH або Secure Shell (безпечна оболонка) – мережевий протокол прикладного рівня, що дозволяє виробляти віддалене управління операційною системою і тунелювання TCP-з'єднань (наприклад, для передачі файлів). SSH робить віддалене управління операційною системою безпечним, так як шифрує весь трафік, включаючи і передаються паролі. При цьому можливий вибір різних алгоритмів шифрування.

Крім віддаленого управління, SSH дозволяє безпечно передавати в незахищеній середовищі практично будь-який мережевий протокол. Таким чином, можна не тільки віддалено працювати на комп'ютері через командну оболонку, але і передавати по шифрованому каналу звуковий потік або відео (наприклад, з веб-камери), виробляти роботу з базами даних та іншими сховищами, а також використовувати будь-які інші протоколи. Також SSH може використовувати стиснення переданих даних для подальшого їх шифрування, що зручно для віддаленого запуску клієнтів X Window System.

Захист SSH базується на досить простих правилах, дотримання яких істотно знижує ризик злому:

– Заборона віддаленого root-доступу за паролем.

– Заборона підключення з порожнім паролем або відключення входу по паролю (використання ключів).

– Вибір нестандартного порту для SSH-сервера (стандартний – 22).

– Використання довгих SSH2 RSA-ключів (2048 біт і більше) для аутентифікації.

–Обмеження списку IP-адрес, з яких дозволений доступ (наприклад, блокуванням порту на рівні брандмауера).

–Відмова від використання поширених або широко відомих системних логінів для доступу по SSH.

– Блокування спроб перебору паролів (бан по IP, наприклад).

– Регулярний перегляд повідомлень про помилки аутентифікації.
– Установка систем виявлення вторгнень (IDS).
– Використання пасток, що підроблюють SSH-сервіс (honeypot).

4.7 Елементи розумного будинку

Налаштування програмованих датчиків температури і вологості для забезпечення комфортних умов навколишнього середовища для серверної кімнати (рис. 4.6).

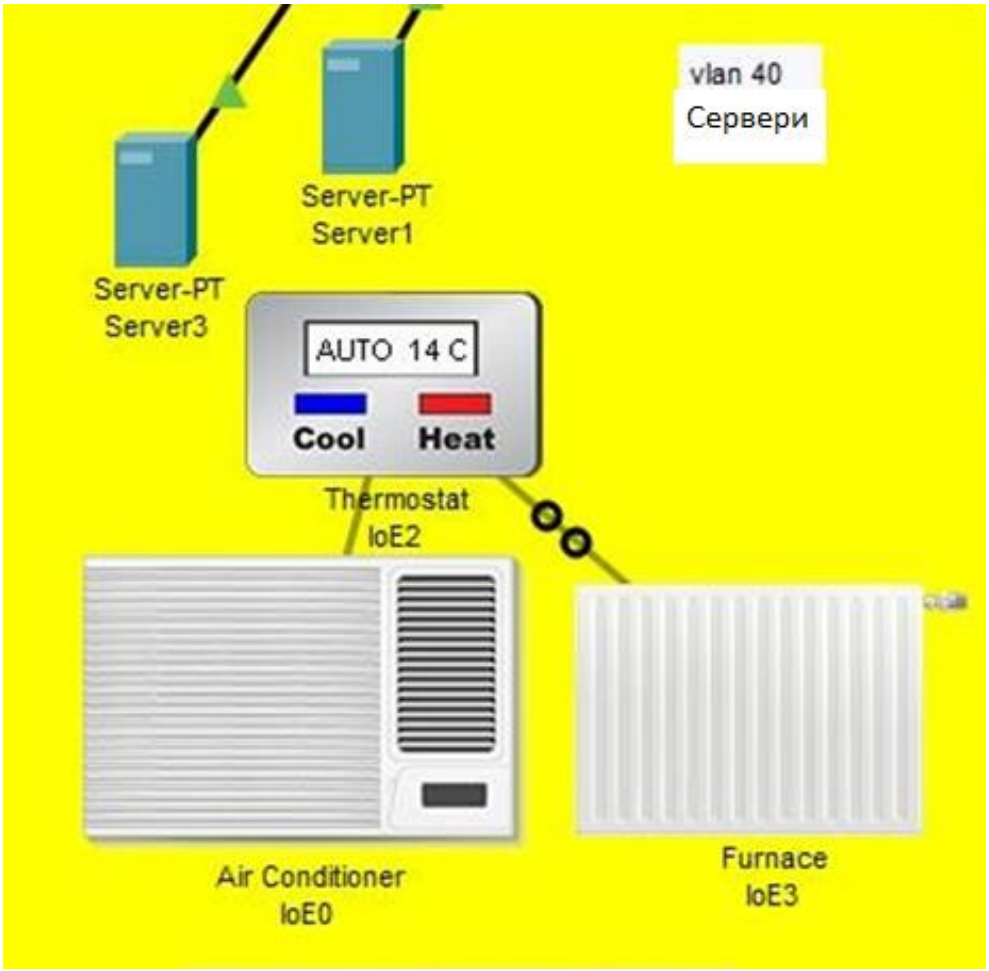

Рисунок 4.6 – Налаштування датчиків температури і вологості

4.8 Налаштування бездротової локальної мережі Wi-FI

Гостьова локальна мережа ізольована від внутрішньої мережі організації в окремому VLAN. Відвідувачі отримують IP-адреса, адреса DNS сервера і маршрут за замовчуванням від DHCP-сервера.

4.9 Установка систем відеоспостереження

Встановлюються IP-камери в важливих місцях підприємства для забезпечення безпеки і моніторингу, що відбувається. Як і в звичайних камерах, в IP-моделях об'єктив фокусує зображення на матриці, яка в свою чергу перетворює світло в електричний сигнал. Він передається на процесор, який обробляє кольору, яскравість і інші параметри зображення. Після цього відео надходить на компресор, який стискає дані для передачі їх через мережевий контролер.

Кожній IP-камері при підключенні присвоюється власна IP-адреса, щоб камера могла синхронізуватися з реєстратором, що відбувається за допомогою спеціальної програми або команди. Без IP-адреси забезпечити спільну роботу і доступ до камери з мобільних гаджетів буде не можна.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи описано спеціалізовані мережі та особливості міжмашинної взаємодії; досліджено безпеку M2M-мереж; описано спеціалізовані та сенсорні мережі п’ятого покоління; проаналізовано існуючі інформаційно-технологічні платформи тазастосунки; сформовано загальні вимоги до спеціалізованих мереж длязабезпечення M2M та IoT-комунікації.

В другому розділі роботи описано класифікацію спеціалізованих та сенсорних мереж; досліджено архітектуру спеціалізованих та сенсорних мереж; запропоновано класифікацію сутностей M2M-архітектури та описано основні складові її доменів; виконано концептуальне проєктування M2M-взаємодії.

В третьому розділі проведено аналіз загроз що виникають в M2M та IoT-мережах; описано процедури валідації в спеціалізованих мережах для забезпечення M2M та IoT-комунікації; розглянуто процедури та потоки повідомлень в спеціалізованих мережах для забезпечення M2M та IoT-комунікації; запропоновано класифікацію сутностей та сенсорів; розроблено рекомендації щодо покращення рівня безпеки спеціалізованих мереж для M2M та IoT-комунікації.

В четвертому розділі спроектовано захищену комп’ютерну мережу для підприємства з декількома філіями. Проект був змодельований в симуляторі Cisco Packet Tracer.

ПЕРЕЛІК ПОСИЛАНЬ

1. Telecommunications: Glossary of Telecommunication Terms, US General Services Administration, 1997.

2. NGMN 5G White Paper, NGMN Alliance, 2015, https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf

3. Wang, H. and Prasad, A. R. and Schoo, P., “Research Issues for Fast Authentication in Inter-Domain Handover”, Wireless World Research Forum (WWRF), 2004 February.

4. A Global Strategy for the European Union http://europa.eu/globalstrategy/en/global-strategyforeign-and-security-policy-european-union.

5. “5G for Connected Industries and Automation”, 5G Alliance of Connected Industries and Automation (5G-ACIA), Second Edition, 2019 February.

6. TR 22.804 – “Study on Communication for Automation in Vertical Domains”, 3GPP, December 2018, www.3gpp.org.

7. B. Aboba et al., Extensible Authentication Protocol (EAP), IETF RFC3748, 2004.

8. TR 22.804 – “Study on Communication for Automation in Vertical Domains”, 3GPP, December 2018, www.3gpp.org.

9. S. Pérez et al. “ARMOUR: Large-scale experiments for IoT securityamp; trust”, 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).

10. D. Bruneo et al. “IoT-cloud authorization and delegation mechanisms forubiquitous sensing and actuation”. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).

11. IoTivity project, Linux Foundation; OCF, https://iotivity.org/.

12. Zephyr project, Linux Foundation, www.zephyrproject.org/about/.

13. Olaf Bergmann, LibCoAP library, https://libcoap.net/.

14. Anjay project, https://github.com/AVSystem/Anjay.

15. Leshan project, https://www.eclipse.org/leshan/.

16. Open Connectivity Foundation. Tech. rep. 2018. https://openconnectivity.org/developer/specifications.

17. Mehmood, Y., Görg, C., Muehleisen, M., Timm-Giel, A. (2015). Mobile M2M communication architectures, upcoming challenges, applications, and future directions. Journal on Wireless Communications and Networking, 1, pp.1-37 [12] Rani, V., Dhir, R. (2013). A Study of Ad-Hoc Network: A Review. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 3(3), pp.135-138.

18. Di Pietro, R., Guarino, S., Verde, N., Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks – A survey. Elsevier, the International Journal of Computer Communications, 51, pp.1-20.

19. Pinar, Y., Zuhair, A., Hamad, A., Resit, A., Shiva, K., Omar, A. (2016). Wireless Sensor Networks (WSNs): The Shortcomings of Wireless Sensor Networks, IEEE Long Island Systems, Applications and Technology Conference, pp.1-8.

20. Ahmed, E., Ali, B., Osman, E., Ahmed, T. (2016). Performance Evaluation and Comparison of IEEE 802.11 and IEEE 802.15.4 ZigBee MAC Protocols Based on Different Mobility Models. International Journal of Future Generation Communication and Networking, vol. 9, no. 2, pp.9-18.

21. Pinar, Y., Zuhair, A., Hamad, A., Resit, A., Shiva, K., Omar, A. (2016). Wireless Sensor Networks (WSNs): The Shortcomings of Wireless Sensor Networks, IEEE Long Island Systems, Applications and Technology Conference, pp.1-8.

22. Mehmood, Y., Görg, C., Muehleisen, M., Timm-Giel, A. (2015). MobileM2M communication architectures, upcoming challenges, applications, and future directions. EURASIP Journal on Wireless Communications and Networking, 2015(1), pp.1-37.

23. Pticek, M., Podobnik, V. and Jezic, G. (2016). Beyond the Internet of Things: The Social Networking of Machines. International Journal of Distributed Sensor Networks, SAGE Publications, pp.1-15.

24. Mišić, V. and Mišić, J. (n.d.). Machine-to-machine communications. CRC Press (eds.), ISBN-13: 978-1466561236.

25. European Telecommunications Standards Institute (ETSI). (2013). Machine-to-Machine communications (M2M); Functional architecture. Technical Specification, ETSI TS 102 690 V1.1.1 (2011-10). http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf.

26. Narasimhasastry, Suma Manuvinakurike, et al. "M2M Communication in Ad-Hoc WSNs for Industrial Application Using MQTT Protocol." Advances in Wireless Communications and Networks 3.4 (2017): 39.

27. Lu, R., Li, X., Liang, X., Shen, X., & Lin, X. (2011). GRS: The green, reliability, and security of emerging machine to machine communications. IEEE communications magazine, 49(4), pp.28-35.

28. Galetić, V., Bojić, I., Kušek, M., Ježić, G., Dešić, S., Huljenić, D. (2011). Basic principles of Machine-to-Machine communications and its impact on telecommunication industry, MIPRO, Proceedings of the 34th International Convention, 23-27 May, Opatija, Croatia, pp.380-385.

29. Aswad, R. and Abdala, M. (2016). Performance Enhancement of VANET Routing Protocols. Journal of Telecommunications, 32(1), pp.5-10.

30. Wei, C., Jianding, Y. and Xiangjun, L. (2012). The design of electronic license plate recognition terminal system based on nRF24LE1. 5th International Symposium on Computational Intelligence and Design (ISCID). 28-29 Oct, Hangzhou, China, pp.127-129.

31. Azevedo, S. and McEwan, T.E. (1997). Micropower impulse radar. IEEE Potentials, 16(2), pp.15-20.

32. Joshi, G. and Kim, S. (2016). A Survey on Node Clustering in Cognitive Radio Wireless Sensor Networks. Sensors, 16(9), pp.1465-1484.

33. Tehrani, K. and Michael, A. (2014). Wearable technology and wearable devices: Everything you need to know. Wearable Devices Magazine. https://www.wearabledevices.com/what-is-a-wearable-device/.

34. Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X. and Luo, H.H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wireless Communications, 22(4), pp.104-112.

35. Kahn, J., Aulakh, V. and Bosworth, A. (2009). What It Takes: Characteristics of The Ideal Personal Health Record. Health Affairs, 28(2), pp.369-376.

36. Dinh, T. and Kim, Y. (2016). An Efficient Interactive Model for On-Demand Sensing-As-A-Services of Sensor-Cloud. Sensors — Open Access Journal, 16(7), pp.1-28.

37. Open Mobile Alliance (OMA). (2016). OMA Smart Card Web Server. http://openmobilealliance.org/oma-smart-card-web-server/.

38. Syal, M.M. and Ofei-Amoh, K. (2013). Smart-grid technologies in housing. Cityscape: A Journal of Policy Development and Research, 15(2), pp.283-288.

39. Chuck Mortimore et al., “System for Cross-domain Identity Management: Protocol”, IETF RFC 7644, 2015 September.

40. OMA Lightweight M2M (OMA LWM2M), Open Mobile Alliance, OMA LWM2M v1.1, 2018, http://openmobilealliance.org/RELEASE/ LightweightM2M/V1_1-20180612-C/OMA-TS-LightweightM2M_Core-V1_1-20180612-C.pdf.

41. Carsten Bormann and Klaus Hartke and Zach Shelby, “The ConstrainedApplication Protocol (CoAP)”, RFC 7252, 2014 June.

42. European Union Agency for Network and Information Security (ENISA). (2016). Threat Taxonomy – A tool for structuring threat information.https://www.enisa.europa.eu/topics/threat-riskmanagement/threats-and-trends/ enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuringthreat- information.

43. Ashraf, Q. and Habaebi, M. (2015). Autonomic schemes for threat mitigation in Internet of Things. Journal of Network and Computer Applications, 49, pp.112-127.

44. International Electrotechnical Commission – IEC. (2014). Internet of Things: Wireless Sensor Networks. Available at: http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf.

45. Scarfone, K., Dicoi, D., Sexton, M. and Tibbs, C. (2008). Guide to Securing Legacy IEEE 802.11 Wireless Networks. National Institute of Standards and Technology (NIST). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890006.

46. Karygiannis, T., Eydt, B., Barber, G., Bunn, L. and Phillips, T. (2007). Guidelines for Securing Radio Frequency Identification (RFID) Systems. National Institute of Standards and Technology (NIST). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51156.

47. Cerrudo, C. (2015). An Emerging US (and World) Threat: Cities WideOpen to Cyber Attacks. IOActive. Available at: http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_cyber-security_ CesarCerrudo.pdf.

48. Feng, N., Hao, Z., Yang, S. and Wu, H. (2016). Supporting BusinessPrivacy Protection in Wireless Sensor Networks. Journal of Sensors,2016, pp.1-11.

49. Fraunhofer FOKUS Open5GCore, www.open5gcore.org.

50. Fraunhofer FOKUS Open5GMTC, www.open5gmtc.org.

51. European Union Agency for Network and Information Security (ENISA). (2015). Guideline on Threats and Assets. Technical guidance on threats and assets in Article 13a. https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets/at_download/fullReport.

52. General Data Protection Regulation: officially Regulation 2016/679 on the protection of natural persons in regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://eur-lex.europa.eu/legalcontent/en/TXT/?uri= CELEX%3A32016R0679.