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

**Інститут електроенергетики**
**Факультет інформаційних технологій**
**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеню магістра

**студента** ***Жука Єгора Владиславовича***

**академічної групи** ***125м-17-1***

**спеціальності** ***125 Кібербезпека***

**спеціалізації**[1]

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

**на тему** ***Кібербезпека систем обліку і моніторингу енергоресурсів в житлово-комунальному господарстві***

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | к.ф-м.н., доц. Гусев О.Ю | | | |
| розділів | ас. Ковальова Ю.В. | | | |
| спеціальний | ас. Ковальова Ю.В. | | | |
| економічний | к.е.н.,доц. Пілова Д.П. | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент** | | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**
**2018**

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

«_____»_____20___року

# ЗАВДАННЯ
# на кваліфікаційну роботу ступеня магістра

**студенту** ***Жуку Є.В.*** **академічної групи** ***125м-17-1***
(прізвище та ініціали) (шифр)

**спеціальності** ***125 Кібербезпека***

**спеціалізації**[1]

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

**на тему** ***Кібербезпека систем обліку і моніторингу енергоресурсів в житлово-комунальному господарстві***

## 1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від __29.11.18___ № 2025-л

## 2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

**Об'єкт досліджень** ***Система бездротової передачі інформації в житлово-комунальному господарстві***

**Предмет досліджень** ***Бездротові мережі моніторингу енергоресурсів***

**Мета** ***Дослідження захищеності бездротових мереж передачі інформації в житлово-комунальному господарстві***

**Вихідні дані для проведення роботи** ***Провести аналіз бездротових мереж в системі ЖКГ, виявити можливі вразливості та атаки на бездротові мережі***

## 3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

**Наукова новизна** ***Аналіз атак і вразливостей бездротових мереж, стратегія розвитку захисту енергоносіїв важливих для держави та сектору енергосбереження***

**Практична цінність** ***впровадження рекомендацій для підвищення рівня інформаційної безпеки для підприємств, що надають комунальні послуги та захисту енергоносіїв в секторі енергозбереження***

## 4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

***результати роботи повинні відповідати вимогам чинного законодавства України та методичним рекомендаціям до підготовки та захисту дипломної роботи для студентів галузі знать «Кібербезпека»***

## 5 ЕТАПИ ВИКОНАННЯ РОБІТ

| **Найменування етапів робіт** | **Строки виконання робіт** (початок-кінець) |
|---|---|
| Огляд джерел за темою та напрям досліджень | 03.09.18-06.10.18 |
| Методи досліджень | 07.10.18-31.10.18 |
| Результати досліджень | 01.11.18-24.11.18 |
| Виконання економічного розділу | 25.11.18-04.12.18 |
| Оформлення пояснювальної записки | 05.12.18-10.12.18 |

## 6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект** ***полягає у зменшенні збитків понесених від хакерських атак та помилок користувачів, та збереженні енергоресурсів***

**Соціальний ефект** ***підвищення рівня довіри клієнтів до об'єкту комунального забезпечення та впевненості керівництва і працівників у захищенні мережі та безпечному обліку енергоносіїв***

## 7 ДОДАТКОВІ ВИМОГИ

**Завдання видано** _____ ____Гусев О.Ю._
(підпис керівника) (прізвище, ініціали)

**Дата видачі: 03.09.18р.**

**Дата подання до екзаменаційної комісії: 14.12.18р.**

**Прийнято до виконання** _____ ____Жук Є.В.___
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 70 с., 9 рис., 2 табл., 4 додатки, 21 джерел.

Об’єкт дослідження: Система бездротової передачі інформації в житлово-комунальному господарстві.

Мета дипломної роботи: підвищення рівня інформаційної безпеки та дослідження захищеності бездротових мереж передачі інформації.

У першому розділі дипломної роботи проаналізовано види бездротових мереж та місце їх використання.

У спеціальній частині дипломної роботи проаналізовані можливі атки на бездротові мережі моніторингу, їх вразливості та способи захисту. Впроваджено додаткове програмне забезпечення та апратуру що дозволить підвищити захист інформації яка передається через бездротові мережі та захист самої мережі.

У економічній частині були розраховані витрати на програмне забеспечення та аппаратуру, розрахунок збитків одержуваних від атак без запропонованого захисту та розрахунок єкономічної доцільності впроваджуваного проекту.

Практична значимість дипломної роботи полягає у впровадженні рекомендацій для підвищення рівня інформаційної безпеки для підприємств, що надають комунальні послуги та захисту енергоносіїв в секторі енергозбереження.

БЕЗПЕКА МЕРЕЖ, ТЕХНОЛОГІЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ, БЕЗДРОТОВІ МЕРЕЖІ МОНІТОРИНГУ, ZIGBEE, АСКОЕ.

# РЕФЕРАТ

Пояснительная записка: 70 с., 9 рис., 2 табл., 4 приложения, 21 источников.

Объект исследования: Система беспроводной передачи информации в жилищно-коммунальном хозяйстве.

Цель дипломной работы: повышение уровня информационной безопасности и исследования защищенности беспроводных сетей передачи информации.

В первой главе дипломной работы проанализированы виды беспроводных сетей и место их использования.

В специальной части дипломной работы проанализированы возможные аткы на беспроводные сети мониторинга, их уязвимости и способы защиты. Внедрено дополнительное программное обеспечение и апратуру что позволит повысить защиту информации, которая передается через беспроводные сети и защиту самой сети.

В экономической части были рассчитаны затраты на программное обеспечение и аппаратуру, расчет убытков получаемых от атак без предложенного защиты и расчет економичнои целесообразности впроваджуваного проекта.

Практическая значимость дипломной работы заключается во внедрении рекомендаций по повышению уровня информационной безопасности для предприятий, предоставляющих коммунальные услуги и защиты энергоносителей в секторе энергосбережения.

БЕЗОПАСНОСТЬ СЕТЕЙ, ТЕХНОЛОГИИ ПЕРЕДАЧИ ИНФОРМАЦИИ, БЕСПРОВОДНЫЕ СЕТИ МОНИТОРИНГА, ZIGBEE, АСКУЭ.

# ABSTRACT

Explanatory note: 70 p., 9 fig., 2 tab., 4 appendices, 21 sources.

Object of study: The system of wireless transmission of information in the housing and communal services.

The aim of the thesis: to increase the level of information security and research security of wireless information transfer networks.

The first chapter of the thesis analyzes the types of wireless networks and their place of use.

In the special part of the thesis, possible attacks on wireless monitoring networks, their vulnerabilities and methods of protection were analyzed. Introduced additional software and hardware that will increase the protection of information transmitted through wireless networks and the protection of the network itself.

In the economic part, the costs of software and hardware, the calculation of losses incurred from attacks without the proposed protection, and the calculation of the economic feasibility of the advanced project were calculated.

The practical significance of the thesis is the implementation of recommendations to improve the level of information security for companies providing utilities and energy protection in the sector of energy conservation.

NETWORK SECURITY, INFORMATION TRANSFER TECHNOLOGIES, WIRELESS MONITORING NETWORKS, ZIGBEE, ASMAE.

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

АСКОЕ – автоматизована система контролю і обліку енергоресурсів.

БММ – бездротові мережі моніторингу.

ЖКГ – житлово-комунальне господарство.

ІзОД – інформація з обмеженим доступом.

НСД — несанкціонований доступ.

ПЗ – програмне забезпечення.

ПК – персональний комп’ютер.

ВОК – вимірювально-обчислювальні комплекси.

ПІП – первинні вимірювальні перетворювачі.

PLC – power line communication.

FSK – frequency shift keying.

ЗМІСТ

# ВСТУП

Завдання побудови всіляких систем, що використовують бездротові канали там, де раніше в якості ліній зв'язку використовувалися дроти, актуальні в самих різних прикладних областях. Особливо важливим є питання переходу на бездротовий зв'язок в розподілених системах збору даних, управління і автоматизації, де число пристроїв в мережі може досягати сотень і тисяч.

Бездротові мережі привертають увагу користувачів і розробників з моменту своєї появи масу переваг, якими вони володіють у порівнянні з "класичними" провідними мережами. Це і гнучка архітектура, і зниження витрат при монтажі. У деяких ситуаціях прокладка дротових ліній взагалі неможлива за технологічними або організаційних причин. У цих випадках зв'язок без проводів вирішує масу проблем. Тому бездротові системи передачі даних виглядають більш ніж привабливо для вирішення великого кола завдань.

Практичне використання бездротових систем довгий час було важко через низьку надійності радіоканалу в порівнянні з провідним з'єднанням, високу вартість і високого енергоспоживання елементної бази, а також через труднощі з установкою і налаштуванням системи на об'єкті установки. Зараз бездротові системи збору даних, управління і автоматизації і їм подібні стали реальністю завдяки технологіям бездротових мереж малого радіусу дії і появі на ринку наборів мікросхем, радіомодулів і модемів, а також розвиненого програмного забезпечення, що підтримує стандартні протоколи управління і передачі даних.

На сьогоднішній день "в побуті" ми найчастіше застосовуємо як мінімум три стандарти бездротового зв'язку по радіоканалу: GSM як відмінний засіб для телефонії, WiFi для домашніх і офісних мереж і Bluetooth для підключення пристроїв і периферії. Однак ці стандарти через набір особливостей недостатній для оптимального вирішення всіх "мережевих завдань". У відповідь на запити потенційних користувачів з'являються численні "альтернативні" специфікації. Одна з них - IEEE 802.15.4 і пов'язаний з нею стандарт ZigBee.

У даній роботі розглядається можливість застосування технології Zigbee стандарту 802.15.4 в системі житлово-комунальному господарстві та проектується система захисту передачі інформації через бездротові пристрої.

# РОЗДІЛ 1. СИСТЕМА МОНІТОРИНГУ ТА ОБЛІКУ ЕНЕРГОРЕСУРСІВ

## 1.1 Загальний опис системи

Система призначена для повної / часткової автоматизації процесу отримання об'єктивних даних про фактичне споживання енергоресурсів на об'єктах житлового та нежитлового фондів з використанням будинкових та / або квартирних приладів обліку, формування бази за попередні періоди, а також для контролю за параметрами енергоносіїв.

Система використовується для інформаційного забезпечення політики енергозбереження та ефективного витрачання енергії, тепла, води при взаємодії органів виконавчої влади, організацій, що надають енергоресурси керуючих організацій житлового фонду та споживачів комунальних ресурсів.

### 1.1.2 Задачі системи

1. Дистанційний моніторинг споживання всіх або частини використовуваних ресурсів, а також надано ие даних з приладів обліку теплоен ергії; гарячого водопостачання; холодного водопостачання; електричної енергії; витрати природного газу;

2. Оперативно - диспетчерське управління, а також контроль параметрами енергоресурсів;

### 1.1.3 Склад системи

Система комерційного обліку споживання енергоресурсів включає наступні компоненти:

- прилади обліку споживання ресурсів ЖКГ;
- імпульсний радиомодем;
- цифровий радиомодем;
- концентратор;
- сервер автоматизованої системи обліку споживання енергоресурсів.

Загалом, система моніторингу енергоресурсів складається з контролерів, реєстраторів, програмних, технічних засобів збору, аналізу, візуалізації та обробки інформації.

До приладів обліку відносяться будинкові і індивідуальні (квартирні) лічильники електрики, холодної і гарячої води, газу, тепла, що володіють інтерфейсами для зчитування показань.

Радіомодем - автономний або вбудовується в корпус лічильника елемент для передачі інформації від приладів обліку в концентратор (безпосередньо або через репітери). Радіомодем має вбудований таймер, зберігає поточні показання лічильників, приймає і відповідає на команди, що надходять з концентратора і тестових приладів. Кожен радиомодем може також виступати в ролі ретранслятора, для ланцюжка пристроїв, і таким чином, шляхом ретрансляції забезпечувати передачу даних від приладу обліку до концентратора.

Концентратор забезпечує збір, зберігання, структуризацію і подальшу передачу даних по мережі зв'язку загального користування в сервер.

1.1.4 Переваги використання системи обліку

- відбувається зниження обсягів енергоспоживання за рахунок оперативного / дистанційного спостереження;

- передача даних в автоматичному / напівавтоматичному режимі з програмованої періодичністю, або ж на вимогу від сервера;

- можливість надання доступу до перегляду споживання обслуговуючим організаціям, кінцевим споживачам, інженерам;

- можливість формування екстрених повідомлень і своєчасна реакція в разі не нормованих показників.

- підвищення енергоефективності об'єктів замовника;

- аналіз приладів обліку енергоресурсів;

- створення ефективної вертикально інтегрованої системи диспетчеризації;

- зниження витрат на експлуатацію будівлі;

- можливість прогнозування споживання енергоресурсів в майбутньому.

- наявності можливості підключення до різноманітних приладів за цифровими інтерфейсами.

### 1.1.5 Загальні технічні вимоги

Для організації збору даних з приладів обліку та забезпечення управляючих впливів в системі передбачена двонаправлена передача даних на ділянках: прилад обліку - радиомодем - концентратор - сервер.

Передача даних з приладів обліку в сервер проводиться автоматично з программир уемой періодичністю (раз в хвилину, раз в півгодини, раз в годину, раз в добу) і / або по команді-замовлення від сервера.

У випадках збоїв в роботі використовуваних каналів зв'язку або в технічних засобах збору даних повинна бути передбачена можливість ініціалізації повторної передачі даних. Число спроб повторної передачі даних необмежено.

Система використовує збережені свідчення для надання інформації зовнішнім автоматизованих систем, обслуговуючим організаціям, постачальникам, споживачам, посадовим особам.

На підставі показань приладів обліку і аналізу даних, що надійшли, система може формувати екстрені повідомлення для інформування відповідного персоналу про позаштатних ситуаціях при використанні енергоресурсів ЖКГ.

Аналітична обробка накопиченої інформації про споживанні енергоресурсів може використовуватися для прогнозування майбутнього споживання.

Система має можливість адаптації програмного забезпечення сервера і п рограмно-апаратних засобів концентраторів і радіомодемів для роботи з різними приладами обліку по цифровими інтерфейсами.

Для створення інформаційної захищеності може бути забезпечено шифрування каналів передачі даних на ділянках радиомодем - концентратор - сервер, а також використання завадостійкого кодування при передачі цих даних.

радіомодеми і концентратор мають в своєму складі загальний модуль - універсальний блок управління і бездротового зв'язку, призначений для бездротової передачі інформації.

Системи можуть будуватися на базі бездротового протоколу ZigBee або з розробленими на його основі комерційними організаціями протоколами для кращої взаємодії з самою організацією.

1.1.6 Досягається економічний ефект за рахунок:

1. виключення «людського фактора» при вимірюванні споживання і показників систем інженерного забезпечення;

2. точності, а також синхронності вимірювань;

3. скорочення транспортних витрат;

4. своєчасного виявлення і усунення втрат в мережах;

5. регулювання споживання енергоресурсів;

6. низькі витрати на побудову бездротових сенсорних систем.

1. 2 Сучасні автоматизовані системи контролю та обліку енергоресурсів (АСКОЕ)

1.2.1 Автоматизована система контролю і обліку енергоресурсів

Сучасні АСКОЕ є масштабними системами, які виконують одночасно вимір і облік кількості енергії і енергоресурсів різного роду по територіально розподіленим точкам обліку і працюють в реальному часі з подальшою передачею інформації по ієрархічним рівнем. Особливу значущість АСКОЕ отримала в електроенергетиці.

Для оптимізації витрат на енергоресурси і автоматичного збору даних про фактичне споживання застосовують системи обліку електроенергії АСКОЕ.

Терміном АСКОЕ називають автоматизовану систему контроля і обліку енергоресурсів. В цілому, дана система є сукупністю як технічних, так і програмних засобів, за допомогою яких реалізується постійний точний облік споживаної електроенергії, а також аналіз, зберігання та передача цієї інформації.

Важливим елементом АСКОЕ є ВОК або вимірювально-обчислювальні комплекси. Ці пристрої встановлюються на точках, де необхідно здійснювати вимірювання.

Будь-яка автоматизована система обліку енергоресурсів проектується в три основні рівні:

Перший рівень становлять різні вимірювальні прилади та датчики.

На другому рівні розташовуються пристрої передачі інформації, кабелі та проводи. Даний рівень є сполучною ланкою між попереднім і наступним.

На останньому рівні знаходите обладнання, яке служить для аналізу, перетворення, зберігання даних. Ці функції виконує обчислювальна техніка, а також спеціалізоване програмне забезпечення.

1.2.1.1 В функції АСКОЕ входить:

1. Ведення єдиного часу на всьому об'єкті;
2. Отримання і перетворення інформації про вимірювання, яка надходить від датчиків, а також прив'язка даних до певного часу;
3. Запис всіх результатів в архів вимірювань;
4. Перетворення даних про вимірювання з метою адаптації інформації під інші системи;
5. Відправка інформації в інші системи, наприклад, для друку на принтер;
6. Складання графіків, діаграм і таблиць для більш наочного уявлення статистики та аналізу інформації;
7. Можливість оперативного доступу до всіх даних.

Впровадження обліку електроенергії АСКОЕ має ряд переваг:

1. Оптимізація витрат на енергоресурси;
2. Зниження споживання електроенергії;
3. Можливість контролювати і аналізувати витрати енергії, а також виставити ліміт;
4. Захист від розкрадання електроенергії;
5. Можливість виявити недоліки всієї електричної системи і усунути їх.
6. Здійснювати оптимальне управління навантаженням споживачів.
7. Збирати і формувати дані на енергооб'єктах.

8. Збирати і передавати на верхній рівень управління інформацію і формувати на цій основі дані для проведення комерційних розрахунків між постачальниками і споживачами електричної енергії.

1.2.2 Види АСКОЕ

- Побутові споживачі;
- Житлові будинки;
- Садові товариства і дачні кооперативи;
- Системи обслуговування до 50 абонентів;
- Системи обслуговування до 1000 абонентів;
- Промислове;
- Комерційне та технічне, однорідне і неоднорідне.

Комерційним (розрахунковим*)* називають облік поставки (споживання) енергії для грошового розрахунку за неї.

Технічний (контрольний*)* облік - облік для контролю процесу постачання або споживання енергії всередині підприємства по його підрозділам.

Цифрова АСКОЕ - цифрова вимірювальна система, яка використовує в якості основного засобу вимірювань в складі кожного свого вимірювального каналу електронний лічильник з вбудованою в нього цифровий базою даних і з зовнішнім доступом до неї по цифровому інтерфейсу.

Нецифрова АСКОЕ має в своєму складі принаймні один нецифровий ІК. Наприклад, ІК з число-імпульсним представленням результату.

1.2.3 Організація та створення АСКОЕ

Сьогодні багато побутові споживачі знімають і оплачують свідчення своїх лічильників з затримкою до двох - трьох тижнів щодо моменту закінчення розрахункового періоду, при цьому часова похибка досягає 40 - 50%.

Ідея технічних засобів автоматизованого дистанційного зчитування давно відома, але практична реалізація почалася в промислово розвинених країнах тільки в 70-80-ті роки XX століття, коли з'явилися інтегральні технології, що дозволили зробити технічні рішення економічно прийнятними для масового застосування.

З розпадом планової економіки закінчилася епоха практично необмежених і дешевих енергоресурсів, коли їх частка в собівартості продукції становила всього лише кілька відсотків. На сьогоднішній день через багаторазове подорожчання енергоресурсів їх частка в собівартості продукції для багатьох промислових підприємств різко зросла і становить 20-30%, а для найбільш енергоємних виробництв досягає 40% і більше. Разом з подорожчанням енергоресурсів як необхідний наслідок настав економічно доцільний межа їх споживання в рамках історично сформованих технологій для кожного окремого підприємства.

Під тиском ринку споживачі приходять до розуміння тієї простої істини, що першим кроком в економії енергоресурсів і зниження фінансових втрат є точний облік.

Сучасна цивілізована торгівля енергоресурсами заснована на використанні автоматизованого приладового енергообліку, що зводить до мінімуму участь людини на етапі вимірювання, збору і обробки даних і забезпечує достовірний, точний, оперативний і гнучкий, адаптований до різних тарифних систем облік як з боку постачальника енергоресурсів, так і з боку споживача. З цією метою як постачальники, так і споживачі створюють на своїх об'єктах автоматизовані системи контролю та обліку енергоресурсів (АСКОЕ) рис. 1.1.

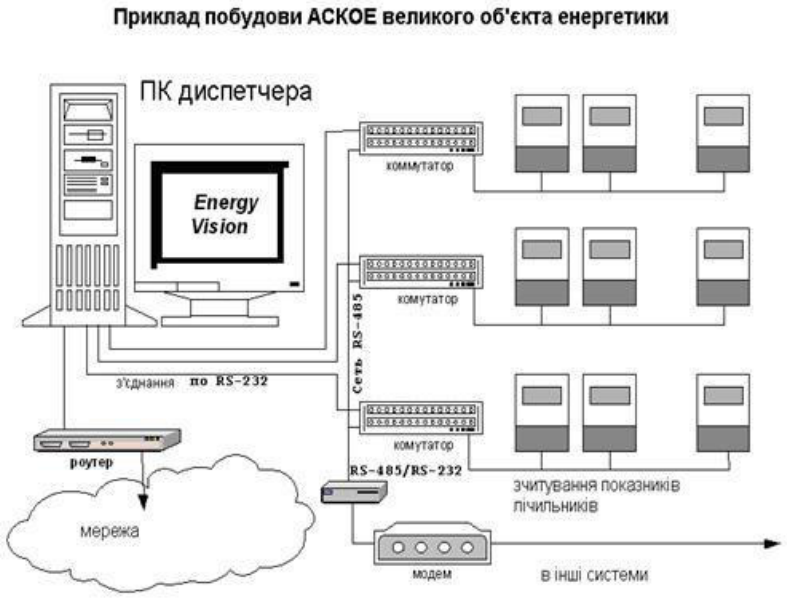


Рисунок 1.1 — Схема побудови і роботи АСКОЕ

При наявності сучасної АСКОЕ промислове підприємство повністю контролює весь свій процес енергоспоживання і має можливість за погодженням з постачальниками енергоресурсів гнучко переходити до різних тарифних систем, мінімізуючи витрати. На розвиток тарифних систем, які гармонізують суперечливі інтереси постачальника і споживача енергоресурсів, відповідає світовому ринку. На рис 1.2 показана схема побудови АСКОЕ регіонального ринку електроенергії

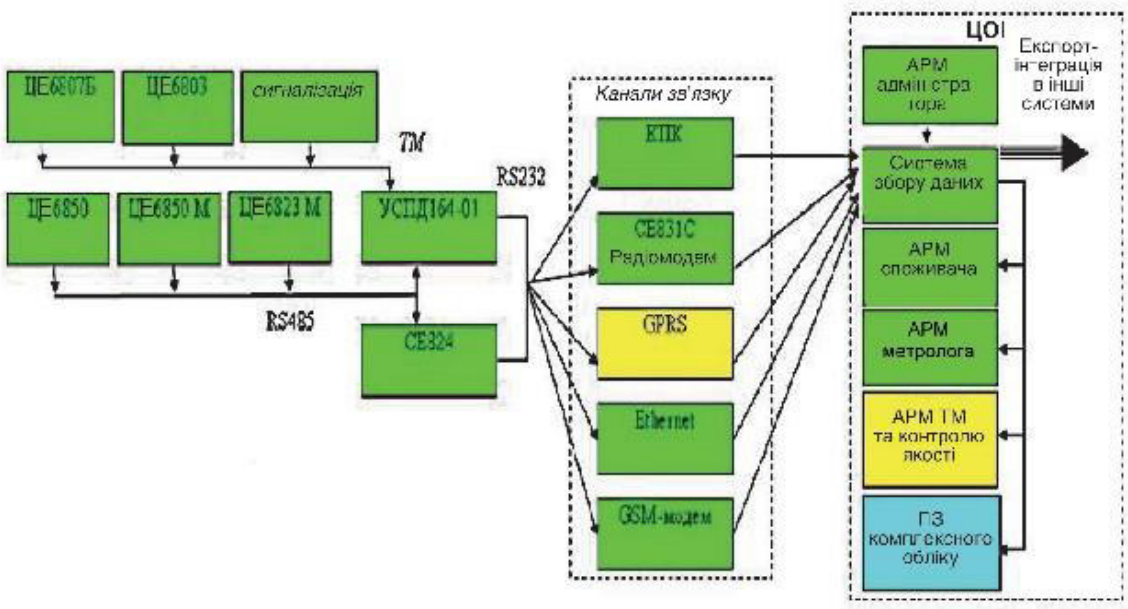


Рисунок 1.2 — Схема побудови АСКОЕ регіонального ринку електроенергії

Рішення проблеми обліку електроенергії вимагає створення автоматизованих систем контролю і обліку, які в загальному випадку утримуючі ат чотири рівні:

- Нижній рівень - первинні вимірювальні перетворювачі (ПІП) з телеметричним виходами, безперервно або з мінімальним інтервалом усереднення изме ряющий параметри електроенергії. Нижній рівень АСКОЕ пов'язаний із середнім рівнем вимірювальними каналами, в які входять всі вимірювальні засоби і лінії зв'язку від точки обліку до контролера;
- Середній рівень - контролери (спеціалізовані вимірювальні системи або багатофункціональні програмовані перетворювачі) з вбудованим програмним забезпеченням обліку, здійснюють в заданому циклі інтервалу

усереднення цілодобовий збір вимірювальних даних з територіально розподілених ПІП, накопичення, обробку та передачу цих даних на верхній рівень. Середній рівень АСКОЕ пов'язаний з верхнім рівнем каналом зв'язку, в якості якого можуть використовуватися фізичні провідні лінії зв'язку.

- Верхній рівень - персональний комп'ютер (ПК) із спеціалізованим програмним забезпеченням АСКОЕ, який здійснює збір інформації з контролера (або групи контролерів) середнього рівня, підсумкову обробку цієї інформації як по точкам обліку, так і за їх групами (підрозділам і об'єктам підприємства), відображення і документування даних обліку у вигляді, зручному для аналізу і прийняття рішень (управління) оперативним персоналом служби головного енергетика та керівництвом підприємства.
- Вищий рівень - Сервер центру збору та обробки даних із спеціалізованим ПО АСКОЕ, які здійснюють збір інформації з ПК або групи серверів центрів збору і обробки даних 3-го рівня, документування та відображення в вигляді, зручному для аналізу і ухвалення рішення персоналом служби гла вного енергетика і керівника.

Всі рівні АСКОЕ пов'язані між собою каналами зв'язку. Для зв'язку 1-го і 2-го рівнів, як правило, використовують пряме з'єднання по стандартних інтерфейсах, 2,3,4й рівень можуть бути з'єднані по виділеним комутованих каналах зв'язку або по локальній мережі.

1.2.4 Лічильники і датчики в системах АСКОЕ

В даний час при стрімкому розвитку мікроелектроніки і зниження цін на електронні компоненти цифрові системи управління поступово витісняють своїх аналогових конкурентів. Одні з головних переваг цифрових систем управління на базі мікроконтролерів - гнучкість і багатофункціональність, досягається не апаратно, а програмно без додаткових матеріальних витрат, а також підвищення точності і надійності обліку. Цифровий лічильник електроенергії на базі найпростішого мікроконтролера має очевидні переваги: надійність за рахунок повної відсутності тертьових елементів, компактність, можливість виготовлення корпусу з урахуванням інтер'єру сучасних житлових будинків;

збільшення періоду повірок в кілька разів; ремонтопридатність і простота в обслуговуванні і експлуатації. При невеликих додаткових апаратних і програмних витратах навіть найпростіший цифровий лічильник може мати ряд сервісних функцій, відсутніх у всіх механічних, з таких прикладів можливість реалізації багатотарифний оплати за споживану енергію, автоматизованого обліку та контролю споживаної електроенергії.

Залежно від вимог сучасні цифрові лічильники повинні в будь-який момент часу оперативно передавати необхідні дані по різних каналах зв'язку на диспетчерські пункти енергопостачальних підприємств для оперативного контролю та економічних розрахунків споживання електроенергії.

Не менш важливу роль відіграють всілякі сервісні функції, такі як дистанційний доступ до лічильника, до інформації про спожитої енергії і багато інших. Наявність цифрового дисплея, керованого від мікроконтролера, дозволяє програмно встановлювати різні режими виведення інформації, наприклад, виводити на дисплей інформацію про спожитої енергії за кожен місяць, за різними тарифами і так далі.

Промисловістю в Україні і за кордоном випускаються для потреб АСКОЕ лічильники - датчики на мікропроцесорній основі різного типу і призначення - одне – і трифазні, одне – і багатотарифні, комбіновані інтелектуальні багатофун кціональні. На рис. 1.3 показано загальний вигляд лічильників-датчиків, що використовуються в АСКОЕ.

Рисунок 1.3 — Загальний вигляд лічильників-датчиків

Завдяки застосуванню передових технологій проведення вимірювань та використанню мікрокомп'ютерних технологій сучасні високоточні електронні лічильники призначені для проведення вимірювань в широкому діапазоні і виконання тарифних функцій. Будучи комбінованими і включаються через трансформатори струму, і напруги, лічильники реєструють активну і реактивну енергію в обох напрямках з класом точності 0,2 і 0,5 - при вимірюванні активної енергії і 1,0 - реактивної енергії. За допомогою сервісної програми, якою оснащується ПК, всі робочі параметри встановлюються індивідуально.

Впровадження автоматизованих систем контролю й обліку енергоресурсів (АСКОЕ) є стратегічним напрямком підвищення ефективності енергетичного потенціалу країни.

1.3 Технології передачі даних в системах моніторингу та обліку енергоресурсів.

В області розрізняють наступні модулі зв'язку: RS-485, PLC, ZigBee , CAN, GSM.

1.3.1 Основна інформація про модулі

Інтерфейси RS-485 і CAN зарекомендували себе як надійні способи обміну даними в різних системах віддаленого контролю і управління. Однак для побудови мереж на основі цих інтерфейсів необхідно прокладати додаткові лінії зв'язку, оскільки середовищем передачі даних в даному випадку є кручена пара. Використання GSM-каналу для інформаційного обміну не вимагає прокладки комунікацій, але послуги операторів стільникового зв'язку становлять додаткову статтю витрат по оплаті трафіку. В результаті розгортання АСКОЕ на базі каналів обміну даними RS-485, CAN або GSM зажадає додаткових фінансово-часових затрат, що в міру розширення парку приладів обліку електроенергії може поставити під сумнів економічну доцільність даного заходу. Організація обміну даними за допомогою PLC і ZigBee при побудові мереж АСКОЕ вигідно відрізняється від описаних вище способів тим, що не потрібно додаткових витрат як на прокладку ліній зв'язку, так і на утримання мережі. Зупинимося докладніше на кожному з варіантів.

### 1.3.2 Технологія PLC

Лінії електропередачі - природне середовище передачі даних в системах обліку спожитої електроенергії. Загальна назва технологій, що реалізують такий спосіб комунікації між пристроями, - PLC (Power Line Communication).

Розрізняють вузькосмугову та широкосмугову передачу даних за допомогою технології PLC. Вузькосмугова PLC-технологія, що забезпечує швидкість обміну на рівні сотень кілобіт в секунду, використовується для передачі даних між пристроями. Широкосмугова PLC-технологія, призначена для організації офісних, промислових або внутрішньобудинкових мереж, підходить як для обміну даними, так і для передачі мультимедійного контенту на швидкості від десятків до сотень мегабіт в секунду. Одна з переваг PLC-технології в тому, що при розгортанні мережі не потрібно прокладати додаткові комунікації: дроти електромережі служать одночасно фізичним середовищем передачі інформаційного сигналу. Але це ж накладає певні обмеження на вибір частотного діапазону і рівень переданого PLC-пристроями сигналу - повинні забезпечуватися вимоги електромагнітної сумісності з іншими пристроями, підключеними до електромережі.

При передачі даних по PLC-технології, як і будь-який інший технології зв'язку, передані дані попередньо модулюються. У прийомнику здійснюється демоду-ляція сигналу. Пристрої, що забезпечують передачу даних по електричних мережах за допомогою PLC-технології, називають PLC-модемами. Основними типами модуляції, які застосовуються в PLC-модеми, є частотна маніпуляція (FSK - Frequency Shift Keying), частотна маніпуляція з рознесеними частотами (S-FSK - Spread Frequency Shift Keying), різні види фазової маніпуляції двійкова (BPSK- Binary Phase Shift Keying), квадратурна (QPSK - Quadrature Phase Shift Keying), восьмерична (8 PSK - 8 PhaseShift Keying) і ортогональне мультиплексування з частотним поділом каналів (OFDM - Orthogonal Frequency Division Multiplexing). При організації каналу зв'язку з використанням PLC-технології необхідно враховувати, що електромережі являють собою найгірший вариант середовища передачі сигналів з численними

джерелами перешкод від підключених до електромережі пристроїв споживачів. До цього можна додати і неекрановані проводи великої довжини, і низька якість електричної розводки, найчастіше на основі алюмінієвого проводу, в якому загасання сигналу відбувається швидше через більш високого електричного опору в порівнянні з мідним. В результаті від вибору типу модуляції нерідко залежать показники швидкості і надійності зв'язку по електричних мережах. Слід зауважити, що високі швидкості передачі даних і хороша перешкодозахищеність тягнуть за собою збільшення складності апаратно-програмної частини PLC-модему, так як потрібні додаткові обчислювальні ресурси для виконання необхідних алгоритмів і дотримання підвищених вимог до блоку живлення пристрою. Тому вибір PLC-модему - це компроміс між характеристиками каналу зв'язку і ціною кінцевого обладнання. Якщо з цих позицій оцінювати застосовувані в узкополосной PLC-технології основні типи модуляцій сигналу, то до переваг FSK, S-FSK і BPSK відносяться легкість реалізації і прийнятний рівень завадостійкості при нестабільності каналу зв'язку, а до недоліків - невисока швидкість передачі даних. Більш складні в реалізації - модуляції QPSK і 8-PSK, але використання останньої забезпечує більш високий рівень завадостійкості і в три рази більшу, в порівнянні з варіантом FSK, швидкість передачі. [1]

Від модуля зв'язку, що використовує дротову PLC-технологію передачі даних, перейдемо до розгляду іншого варіанту модуля на базі бездротової технології ZigBee.

### 1.3.3 Технологія ZigBee

ZigBee є програмною надбудовою стандарту IEEE 802.15.4. Спочатку стандарт IEEE 802.15.4 розроблений для управління побудови фізичного і канального рівнів малопотужних пристроїв низкоскоростной передачі даних на невеликі відстані. Специфікація ZigBee розроблена однойменною альянсом, що складається з більш ста компаній, серед яких - виробники систем автоматизації, вентиляції і кондиціонування. Основні області застосування ZigBee- передача інформації від рухомих механізмів (наприклад, роботів), систем управління в

промисловості, збір свідчень з інтелектуальних датчиків і різноманітних приладів обліку, системи охорони, тобто забезпечення зв'язку між пристроями в автоматизованих системах. Найбільш відомими прикладами таких систем являють ся "Розумний будинок" і "Інтелектуальна будівля". Для мереж ZigBee х арактерні досить скромні показники швидкості передачі і расстоя ня між вузлами, при цьому устаткування може довго працювати від автономних джерел живлення. Крім того, технологія ZigBee дозволяє створювати самоорганізовані і самовідтворювані мережі. Стійкість мережі пояснюється можливістю ретрансляції даних, що передаються через безліч вузлів в мережі. У разі виходу з ладу або виключення одного з вузлів мережі пристроєм знаходить новий маршрут передачі даних. При включенні живлення пристрою мережа знову включає його до свого складу. Завдяки цьому мережа просто і швидко розгортається і легко масштабує ся шляхом простого приєднання додаткових пристроїв. [12]

1.3.3.1 Основні переваги ZigBee :

- надійність і здатність до самоорганізації;
- велика кількість підтримуваних вузлів;
- простота установки;
- тривалий (рік і більше) термін автономної роботи;
- безпека;
- низька вартість;
- широка область використання;
- забезпечення взаємозамінності мереж і вузлів
- незалежність від виробника обладнання.

Пристрої ZigBee використовують переважно частотний діапазон 2,4 ГГц, так як в цьому випадку досягається максимальна швидкість передачі і висока стійкість. Стандартом преду розглядати також використання частот 868 МГц і 915 МГц. Діапазон 868 МГц застосовується в Європі, а 915 МГц - в США. Смуга пропускання 2,4 ГГц розділений на 16 каналів, по 5 МГц кожен. При обміні даними вибирається канал з мінімальним рівнем перешкод. Швидкість

передачі даних разом зі службовою інформацією, необхідною для роботи протоколу, становить 250 кбіт / с. При цьому середня пропускна здатність, яка припадає на корисні дані, залежить від завантаженості мережі і кількості ретрансляцій і знаходиться в діапазоні від 5 до 40 кбіт / с. Максимальна відстань між вузлами, при якому можливий обмін даними, залежить як від потужності передавача, так і від умов поширення радіохвиль в зоні вузла. Найбільш широкого поширення набули передавачі потужністю 1 мВт, що забезпечують зв'язок на відстані до 10 м в приміщенні і до 100 м - на відкритому повітрі. Специфікацією ZigBee існують три типи пристроїв: координатор, маршрутизатор і кінцевий пристрій.

Координатор виконує функції ініціалізації і управління вузлами мережі, обробки і зберігання інформації про налаштування кожного вузла, задає номер частотного каналу, по якому слід передавати дані.

Координатор в процесі роботи може служити джерелом, приймачем і ретранслятором повідомлень. Маршрутизатор, відповідає за вибір шляху доставки повідомлення, що передається від одного вузла до іншого, в процесі роботи також може бути джерелом, приймачем і ретранслятором повідомлень.

Кінцевий пристрій не бере участі в управлінні мережею, ретрансляції повідомлень, це лише джерело і приймач повідомлень.

Стандарт IEEE 802.15.4 складається з набору шарів і рівнів, з'єднаних між собою логічними зв'язками. Кожен шар відповідає за виконання певного набору функцій, а також надає послуги для вищих рівнів.

Структура шарів стандарту відповідає загальноприйнятій семиуровневой моделі взаємодії відкритих систем (OSI- Open Systems Interconnection).
Стандарт описує тільки два нижніх рівні, а саме фізичний (PHY - Physical Layer) і рівень доступу до середовища передачі (MAC - Media Access Control).

Фізичний рівень передачі даних описує низькорівневий механізм управління радіочастотним приймачем. Використовувана на фізичному рівні зв'язка QPSK і DSSS (Direct Sequence Spread-Spectrum - пряме розподіл в

спектрі) дозволяє досягати високу стійкість перед перешкодами і дуже малі втрати даних в пакетах. [6]

MAC рівень управляє доступом до бездротового середовищі, відповідає за доступ до фізичних каналах всіх типів звернень вищих рівнів. На цьому рівні є спеціальна схема запобігання колізій CDMA / CA (Carrier Sense Multiple Access With Collision Avoidance - множинний доступ з кодовим поділом і униканням колізій), яка проводить перевірку зайнятості каналу перед першим виходом вузла мережі на передачу. Ця перевірка здійснюється за допомогою індикатора рівня сигналу (RSSI - Received Signal Strength Indication). Тільки за умови, що канал вільний, вузол мережі ініціює передачу. У всіх інших випадках передавач робитиме нові спроби зв'язку через випадкові інтервали часу. На додаток до RSSI функціонує індикатор якості з'єднання LQI (Link Quality Indicator), який може використовуватися для визначення факту наростання помилок в прийнятих пакетах даних в результаті погіршення якості зв’язку. [11]

Пристрої всередині мережі поділяються за призначенням на три види: координатор, маршрутизатор і кінцевий пристрій. Кінцеве пристрій - пристрій з обмеженою функціональністю, що забезпечує мінімальний набір функцій, за рахунок чого дозволяє економити на енергоспоживанні і комплектуючих.

Низький рівень споживання енергії забезпечується сплячим режимом вузлів. Важливою особливістю є те, що перехід вузла в сплячий режим не позначається на збереженні підключення. Маршрутизатор - пристрій з повною функціональністю, забезпечує функцію моста для пересилання даних від одного пристрою до іншого. Координатор - той же маршрутизатор, що організує мережу і містить всю інформацію про мережеві з'єднаннях.

Вище MAC рівня розташовується протокол ZigBee, який також використовує кілька стратегій зниження взаємного впливу пристроїв один на одного. Координатор при запуску проводить сканування всіх каналів і встановлює той канал, на якому була виявлена найменша сумарна активність.

Подальше функціонування протоколу ґрунтується на доказах передачі пакетних даних, повторних передачах і системі адаптивної маршрутизації.

Система адаптивної маршрутизації може забезпечувати альтернативні шляхи проходження пакетів даних при наявності в мережі тимчасово або постійно перебувають поза зоною видимості (відключених, несправних і т.д) вузлів. Для пошуку альтернативних шляхів проходження пакета через мережу протокол застосовує алгоритм пошуку маршруту, відомий як вектор визначення дистанції на вимогу (AODV - On-DemandDistance Vector). Наявність AODV робить мережу гнучкою, забезпечуючи зв'язок в разі пошкодження вузла або різкого погіршення якості связікакого-небудь ділянки. При виявленні декількох альтернативних шляхів зв'язку з потрібним вузлом мережі маршрутизатор використовує дані кількох індикаторів, включаючи таблицю оновлень LQI для вибору оптимального шляху проходження пакету з найменшою вірогідністю втрати даних. Структуру стеку можна побачити на рис. 1.4.

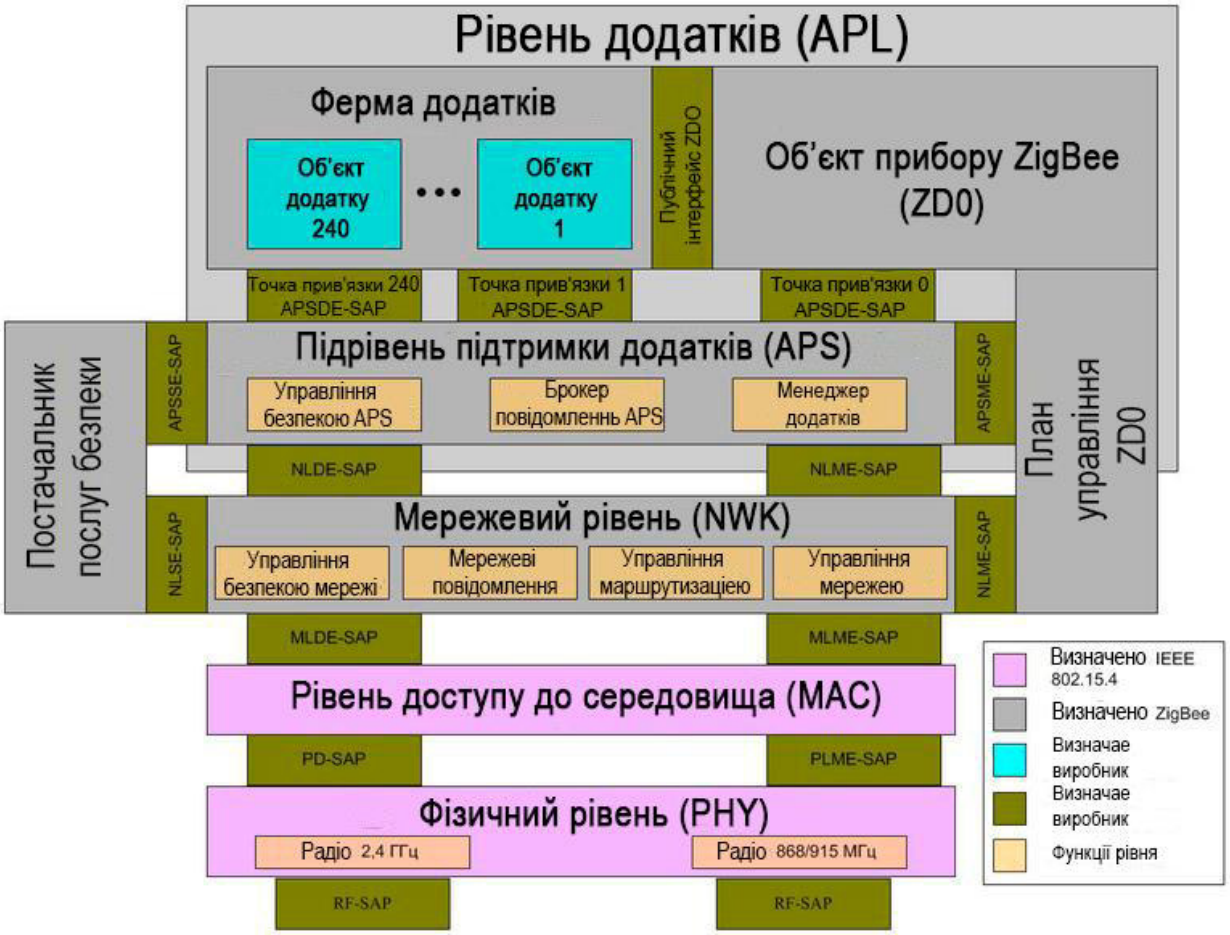


Рисунок 1.4 — Структура ZigBee стеку

Можливість адаптивної маршрутизації служить також і для іншої важливої мети - збільшення зони покриття мережі. Досяжна дальність зв'язку істотно

залежить від рівня вихідної потужності передавача, наявності перешкод в середовищі передачі та інформаційних перешкод від інших пристроїв. Адаптивна маршрутизація дозволяє мережевій архітектурі постійно змінюватися: здійснювати перепризначення вузлів мережі в режимі реального часу і швидко підключати нове устаткування. Вдається встановити більше оптимальних шляхів між вузлами мережі, що покращує умови передачі даних, зменшує кількість ретрансляції і забезпечує зниження споживаної потужності. В результаті роботи протоколу ZigBee формується змішана полносвязанная са-моорганізована топологія мережі, що отримала назву Mesh –топологія і показана на рис 1.5.

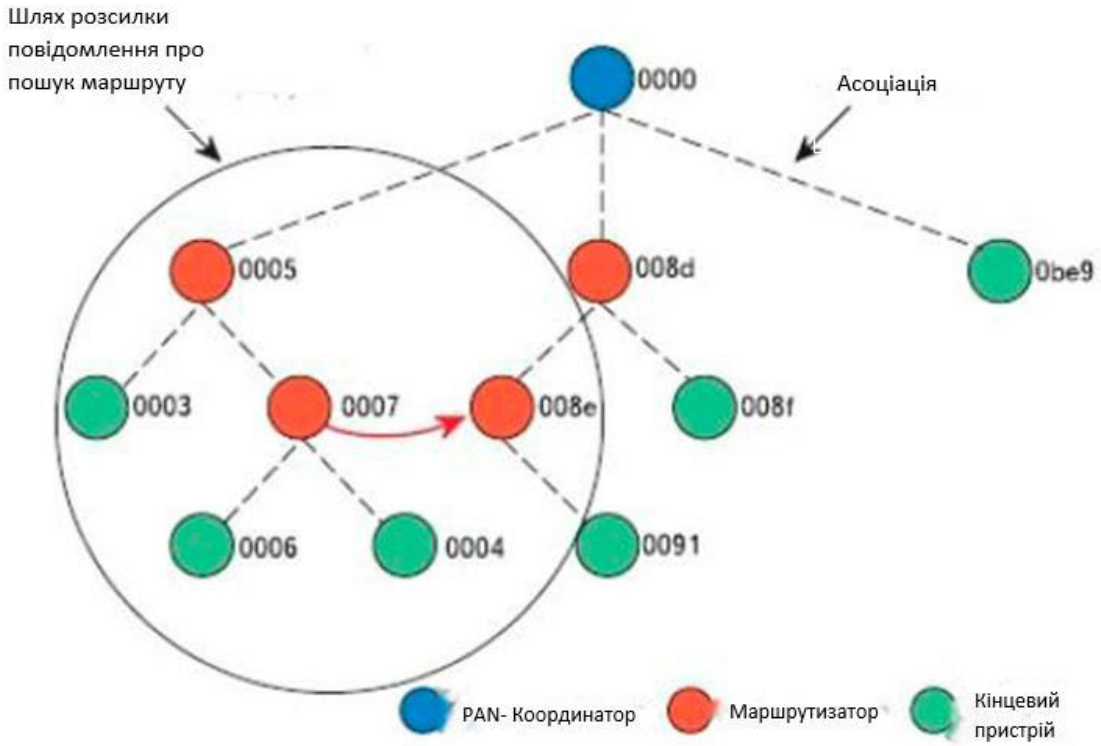


Рисунок 1.5 — Мережа Mash –топології

Використання адаптивної маршрутизації в мережах з Mesh-топологією всі маршрутизатори повинні постійно "слухати", завжди "відповідати"; іншими словами постійно " віщати " і бути готовими до "Зигзагу" маршруту. Звідси пояснення терміну ZigBee: зигзаг (англ. Zig) і бджоли (англ. Bee). Завдяки працьовитості кожної з бджіл вулика інформація про всіх

зигзаги маршруту її польоту до квіткової галявини стає доступною всьому улею. [1]

Висновки до першого розділу

Проаналізувавши види систем моніторингу мереж бездротової передачі данних та принцип їх роботи, можна провести аналіз можливих вразливостей, загроз, способів атаки та запропонувати рішення для захисту мереж моніторингу в ЖКХ.

# РАЗДІЛ 2. АНАЛІЗ АТАК І ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ МЕРЕЖ МОНІТОРИНГУ ТА СПОСОБИ ЇХ ЗАХИСТУ

## 2.1 Види загроз для бездротових мереж

В даний час існує все більша кількість можливих атак на БММ, більшість з яких спрямовані на виведення з ладу безпородних вузлів мережі, на дезорієнтацію протоколів маршрутизації, а також збій роботи мережі в цілому.

Актуальною проблемою використання бездротових мереж є їх захист та способи захисту даних в них, оскільки комунікаційні сигнали при їх розповсюдженні через радіоефір доступні для перехоплення. Існує кілька форм загрози безпеці в бездротових мережах. Так, хакери можуть викрасти дані, отримавши неавторизований доступ до мережі, і навіть порушити роботу мережі.

### 2.1.1 Моніторинг трафіку

Досвідчений хакер або навіть випадковий снупер (snooper – відстежувач, перехоплювач) може відстежити пакети даних в незахищеній бездротовій мережі, використовуючи відповідні програмні засоби за допомогою яких можна повністю розшифрувати вміст пакетів даних із бездротової мережі.

### 2.1.2 Неавторизований доступ

Також можна здійснити моніторинг виконуваних в мережі програм і без особливих зусиль, якщо не прийнято належних запобіжних заходів, отримати доступ до бездротової мережі, знаходячись поза приміщенням, де вона функцонує. За допомогою сучасних операційних систем можна легко встановлювати під’єднання до бездротових мереж, особливо до загальнодоступних. Коли комп’ютер (ноутбук) під’єднаний до бездротової локальної мережі, його власник отримує доступ до будь-якого іншого комп’ютера (ноутбука), що під’єднаний до тієї самої бездротової локальної мережі. Якщо на комп’ютері не встановлений персональний брандмауер, то хто завгодно може отримати доступ до даних такого комп’ютера (ноутбука). Навіть якщо в бездротовій мережі задіяні механізми захисту, істотною загрозою є під’єднання до підставної точки доступу (rogue access point).

2.1.3 Повторне відтворення даних

Атака повторного відтворення - це форма мережевої атаки, при якій передача валідних даних навмисне або шляхом обману повторюються. Так як зловмисник може прослухати будь-яке повідомлення, передане за допомогою мережі, він може вставити «нові» повідомлення або маніпулювати будь-яке повідомлення, відправлене уповноваженим відправником мережі. У представленій утиліті всі прослухані повідомлення зберігаються в базу даних описів пакетів, так що користувач має можливість змінити їх і пізніше перенадіслати.

2.1.4 Атака воронки

Атака воронки яка перешкоджає базової станції отримувати повні та коректні дані з сенсорів, таким чином створюючи серйозну загрозу додатків високого рівня. Зазвичай атаки воронки проводяться зі створенням шкідливого вузла, спеціально спрямованого для найближчих вузлів згідно з алгоритмом маршрутизації.

2.1.5 Вибіркова пересилання

При атаці вибіркової пересилання зловмисник може перенаправляти певних повідомлень і просто залишати їх, перебуваючи в упевненості, що вони не будуть далі поширюватися.

2.1.6 Флудинг

В атаці флуда HELLO-пакетів зловмисник має на меті порушення основного дерева маршрутизації.

2.1.7 Ін'єкція шкідливого коду

Використовуючи переваги вразливостей щодо пам'яті на сенсорних вузлах, такі як переповнення буфера, зловмисник може відправити спеціально створені пакети, щоб здійснити переповнення стека і запустити на виконання довільний код на цільовій системі.

2.1.8 Операція пінгування і поширення програмного образу.

Ці операції можливі при використанні бездротового протоколу програмування Deluge. При дії пінгування відправляється повідомлення на

особливий сенсорний вузол для здійснення запиту про його стан, способу програми, яка в даний момент працює і які інші образи зберігаються на цьому вузлі. Поширення програмного способу - це базисний сервіс в сенсорних мережах, за допомогою якого здійснюється передача оновлень образів. Однак це призводить до погроз, так як зловмисник може легко зруйнувати його за допомогою модифікації або заміни справжнього образу коду, який поширюється на сенсорні вузли.

Наведені вище уразливості вимагають особливого підходу до проектування бездротової мережі, що є базовим складовим елементом «інтернету речей». Цей підхід полягає в тому, щоб польовий вузол системи підтримував процедури аутентифікації, кодування і не підтримував можливість здійснення флудинг і пінінгованія зовнішніми пристроями.

2.1.9 Атака типу «людина всередині»

Завдяки використанню механізмів шифрування і аутентифікації підвищується безпека бездротової мережі, проте, досвідчені хакери відшукують слабкі місця, знаючи, як працюють протоколи мережі. Певну небезпеку представляють атаки типу «людина всередині» (man-in-the-middleattacks): хакер розміщує фіктивний пристрій між легальними користувачами і бездротовою мережею. Наприклад, при здійсненні стандартної атаки типу «людина всередині» використовується протокол перетворення адрес (address resolution protocol (ARP)), який використовується у всіх мережах Ethernet. Хакер, маючи необхідне програмне забезпечення, може, скориставшись ARP, отримати контроль над бездротовою мережею. За допомогою ARP відправляються запити (як в провідниковій, так і в бездротовій мережі) через мережеву плату з метою виявлення іншої фізичної або MAC адреси, куди має прийти даний запит. Проблема, яка виникає при використанні протоколу ARP, полягає в тому, що є небезпека для системи захисту даних за допомогою спуфинга (spoofing (спуфінг) – імітація з’єднання, отримання доступу обманним шляхом). Можна імітувати з’єднання між комп’ютерами, посилаючи на один з комп’ютерів через підставний мережевий пристрій фіктивний ARP запит, що містить IP-

адресудійсного мережевого пристрою іMAC-адресупідставного. Це приведе до того, що на всіх комп’ютерах мережі автоматично відновляютьсяARP-таблиці, які будуть містити помилкові дані. В результаті за допомогою комп’ютерів передаватимуться пакети до підставного пристрою, а не до дійсної точки доступу або маршрутизатора. Це і є класична атака типу «людина всередині», в результаті якої можна отримати доступ до управління сеансами зв'язку користувача, отримати паролі, важливі дані і навіть можна отримати доступ до корпоративних серверів. Для запобігання такого роду атак з використанням спуфінга ARP розробники пропонують захищені ARP (secure ARP, SARP). Цей ARP забезпечує спеціальний захищений канал зв’язку («тунель») між кожним клієнтом і бездротовою точкою доступу або маршрутизатором, за допомогою якого ігноруються всі ARP-відповіді, не пов'язані з клієнтом, що знаходиться на другому кінці цього каналу зв’язку. Але можна встановити SARP на клієнтських пристроях (комп’ютерах, ноутбуках), забезпечивши захист мережі від атак типу «людина всередині».

2.1.10 Атака типу «Відмова в обслуговуванні»

Атака типу «відмова в обслуговуванні» (denial of service, DoS) – це атака, в результаті якої бездротова мережа стає недоступною або її робота блокується. Можливість такої атаки потрібно враховувати при створенні і використанні бездротових мереж. Серйозність DoS-атакизалежить від того, до яких наслідків може привести вихід з ладу бездротової мережі. Одним з різновидів DoS-атакє метод «грубої сили» (bruteforce attack). Масове розсилання пакетів в мережі, при якому використовуються всі ресурси мережі, в результаті чого мережа переповнюється і блокується – це і є варіант DoS-атаки, виконаний за методом «грубої сили». Альтернативним методом припинення роботи більшості бездротових мереж, особливо тих, в яких використовується метод виявлення мережі, є використання сильного радіосигналу, що «глушить» всі інші. Проте спроба проведення атаки на мережу з використанням сильного радіосигналу може виявитися вельми ризикованою, оскільки для проведення такої атаки потрібний потужний передавач, який повинен розташовуватися в безпосередній

близькості від приміщення, в якому розгорнута бездротова мережа. Власник мережі може виявити цей передавач, використовуючи засоби виявлення, що входять до складу мережевих аналізаторів. Іноді «відмова в обслуговуванні» бездротової мережі виникає внаслідок ненавмисних дій.

Найбільш дієвим захистом від DoS-атак є розробка і дотримання таких правил безпеки:

– встановлення та оновлення брандмауерів;

– постійне оновлення антивірусних програмних засобів;

– встановлення останніх оновлень, за допомогою яких ліквідовують недоліки в системі безпеки операційної системи;

– використання довгих паролів;

– від'єднання мережевих пристроїв, які не використовуються.

Універсального способу протидії DoS-атакам всіх типів не існує. Тому, якщо в результаті атаки бездротова мережа все ж таки вийшла з ладу, слід забезпечити перехід до пакетного опрацювання даних за допомогою дротової мережі (якщо це можливо).

2.1.11 Засоби захисту інформації мереж Wi-Fi

Для захисту бездротової мережіWi-Fівикористовуються наступні засоби:

– протокол шифрування WEP — цеп ротокол шифрування, що використовує досить нестійкий алгоритм RC4 на статичному ключі. Існує 64-,128-,256 - і512-бітовешифрування. Чим більше біт використовується для зберігання ключа, тим більше можливих комбінацій ключів, а відповідно більш висока стійкість мережі до злому. ЧастинаWEP-ключає статичною (40 біт у випадку64-бітногошифрування), а інша частина (24 біта) - динамічною (вектор ініціалізації), вона змінюється в процесі роботи мережі. Основною вразливістю протоколу WEP є те, що вектори ініціалізації повторюються через деякий проміжок часу, і зламнику буде потрібно лише обробити ці повтори і обчислити по них статичну частину ключа. Для підвищення рівня безпеки також додатково доWEP-шифруваннявикористовується стандарт 802.1x або VPN;

–протокол шифрування WPA — це більш стійкий протокол шифрування, ніж WEP, хоча використовується той самий алгоритм RC4. Більш високий рівень безпеки досягається за рахунок використання протоколів TKIP і MIC. TKIP (Temporal Key Integrity Protocol) - протокол динамічних ключів мережі, які змінюються досить часто. При цьому, кожному пристрою також привласнюється ключ, що теж змінюється. MIC (Message Integrity Check) - протокол перевірки цілісності пакетів, захищає від перехоплення пакетів і їх перенаправлення.

Також існує можливість використання 802.1x та VPN, як і у випадку з протоколом WEP. Існує 2 види WPA:

1.WPA-PSK(Pre-SharedKey) - для генерації ключів мережі і для входу в мережу використовується ключова фраза. Оптимальний варіант для домашньої або невеликої офісної мережі.

2. WPA-802.1x- вхід у мережу здійснюється через сервер аутентифікації. Оптимально для мережі великої компанії;

–протокол WPA2 - удосконалення протоколу WPA. На відміну від WPA, використовується більш стійкий алгоритм шифрування AES. За аналогією з WPA, WPA2 також ділиться на два типи: WPA2-PSKiWPA2-802.1x;

Слід звернути увагу на протоколи стандарту безпеки 802.1x. До них відносяться:

–EAP (Extensible Authentication Protocol) - протокол розширеної аутентифікації. Використовується спільно з RADIUS - сервером у великих мережах;

–TLS (Transport Layer Security) - протокол, який забезпечує цілісність і шифрування переданих даних між сервером і клієнтом, їх взаємну аутентифікацію, запобігаючи перехопленню і підміну повідомлень;

–RADIUS (Remote Authentication Dial-InUser Server) - сервер аутентифікації користувачів за логіном і паролем;

–VPN (Virtual Private Network) - віртуальна приватна мережа. Цей протокол спочатку був створений для безпечного підключення клієнтів до мережі через загальнодоступні Інтернет-канали. Принцип роботи VPN - створення так званих

безпечних «тунелів» від користувача до вузла доступу або сервера. Хоча VPN спочатку був створений не дляWi-Fi, його можна використовувати в будьякому типі мереж. Для шифрування трафіку в VPN найчастіше використовується протокол IPSec. [3]

Також існує де-кільказасобів додаткового захисту мереж Wi-Fi.Серед них слід відмітити наступні:

– фільтрація за MAC адресою. MAC адреса - це унікальний ідентифікатор пристрою (мережного адаптера), «зашитий» в нього виробником. На деякому обладнанні, можливо, задіяти цю функцію і дозволити доступ в мережу необхідним адресам. Це створить додаткову перешкоду зламнику;

– приховування SSID. SSID - це ідентифікатор бездротової мережі. Більшість обладнання дозволяє його приховати, таким чином, при скануванні мережі видно не буде. Але це не дуже серйозна перепона, якщо хакер використовує більш просунутий сканер мереж, ніж стандартна утиліта в Windows;

– заборона доступу до налаштувань точки доступу або роутера через бездротову мережу. Активувавши цю функцію можна заборонити доступ до налаштувань точки доступу черезWi-Fiмережу, однак, це не захистить мережу від перехоплення трафіку або від проникнення да неї.

Засоби захисту інформації мереж WiMAX. Для здійснення захисту інформації в мережах WiMAX та у відповідності зі стандартом здійснюється шифрування всього переданого по мережі трафіку. Базова станція (БС) WiMAX являє собою модульний конструктив, в який при необхідності можна встановити кілька модулів зі своїми типами інтерфейсів, але, при цьому, має підтримуватися адміністративне програмне забезпечення для управління мережею. Це програмне забезпечення забезпечує централізоване управління всією мережею. Логічне додавання в існуючу мережу абонентських комплектів здійснюється також через цю адміністративну функцію.

Абонентська станція (АС) являє собою пристрій, що має унікальний серійний номер, MAC-адреса, а також цифровий підпис X. 509, на підставі якої

відбувається аутентифікація абонентської станції на базовій станції. При цьому, відповідно до стандарта, термін дійсності цифрового підпису абонентської станції становить 10 років. Після установки абонентської станції у клієнта і подачі живлення вона авторизується на базовій станції, використовуючи певну частоту радіосигналу, після чого базова станція, ґрунтуючись на перерахованих вище ідентифікаційних даних, передає абоненту конфігураційний файл TFTP протоколу. У цьому конфігураційному файлі знаходиться інформація про піддіапазоні передачі (прийому) даних, типи трафіку і доступній смузі, розклад розсилки ключів для шифрування трафіку і інша необхідна для роботи абонентської станції інформація. Необхідний файл з конфігураційними даними створюється автоматично, після занесення адміністратором системи АС в базу абонентів. Після процедури конфігурування аутентифікація абонентської станції на базовій станції відбувається наступним чином: абонентська станція надсилає запит на авторизацію, в якому міститься сертифікат X.509, що підтримується методами шифрування і додаткова інформація, базова станція, у відповідь на запит на авторизацію (у разі достовірності запиту), надсилає відповідь, в якій міститься ключ на аутентифікацію, зашифрований відкритим ключем абонента, 4-бітнийключ для визначення послідовності, необхідний для визначення наступного ключа на авторизацію, а також час життя ключа. У процесі роботи абонентської станції, через проміжок часу, який визначається адміністратором системи, відбувається повторна авторизація та аутентифікація, і в разі успішного проходження аутентифікації і авторизації потік даних не переривається. [4]

Для забезпечення надійності роботи мережі у стандарті технології WiMAX використовується протокол PKM (Privacy Key Management), відповідно до якого визначено декілька видів ключів для шифрування переданої інформації:

– Authorization Key (АК) - ключ, використовуваний для авторизації на базовій станції;

– Traffi c Encryption Key (ТЕК) - ключ, використовуваний для криптозахисту трафіку;

–Key Encryption Key (KEK) - ключ, використовуваний для криптозахисту переданих в ефірі ключів.

В кожен момент часу використовуються два ключі одночасно, які перекриваються часом життя. Дана міра необхідна в середовищі з втратами пакетів (а в ефірі вони неминучі) і забезпечує безперебійність роботи мережі. Є велика кількість динамічно змінних ключів, досить довгих, при цьому встановлення безпечних з'єднань відбувається за допомогою цифрового підпису. Відповідно до стандарта, криптозахист виконується відповідно до алгоритма 3-DES. [5] Опціонально передбачено шифрування за надійнішого алгоритмом AES.

Заходи для вирішення питань безпеки бездротових мереж. Способи захисту даних в бездротових мережах:

– фізичний захист бездротових точок доступу. Деякі точки доступу мають спеціальну кнопку «Reset», за допомогою якої можна повернути налаштуванням пристроїв за замовчуванням. В такому випадку пристрій не буде забезпечувати навіть мінімального захисту бездротової мережі. Це зробить таку точку доступу уразливою. Тому слід забезпечити адекватну фізичну захищеність апаратного забезпечення точок доступу;

– відключення точок доступу, які тимчасово не потрібні користувачам. Можна вимикати електроживлення кожної точки доступу, або якщо є можливість використовувати обладнання, управління електроживленням якого здійснюється через мережу, такі точки доступу можна вмикати і вимикати дистанційно;

– використання систем шифрування та аутентифікації. Також слід звернути увагу на захист даних в бездротових мережах. Для цього слід використовувати, як мінімум, шифрування цих даних. В процесі шифрування біти даних змінюються за допомогою секретного ключа. Оскільки ключ секретний, зловмиснику (хакеру) буде важко дешифрувати отримані дані.

Отже, системи захисту бездротових мереж – це один з найважливіших і складніших елементів налаштування бездротових мереж. Використовуючи

ефективні механізми аутентифікації і шифрування, можна істотно понизити небезпеку.

2.2 Види вразливостей БСМ.

2.2.1. Апаратна вразливість.

В останні роки в багатьох країнах світу в житлових будинках впроваджують так звані інтелектуальні лічильники (Smart Meter). Вони відрізняються від традиційних лічильників розширеними можливостями, дозволяють вести облік часу споживання ресурсів, а також оснащуються комунікаційними засобами для автоматичної передачі показників. Як і будь-які бездротові електронні пристрої, інтелектуальні лічильники електроенергії, а разом з ними і самі "розумні" електромережі уразливі для хакерів.

Зловмисники можуть встановити голкові контакти з кожного боку чіпа інтелектуального лічильника, щоб перехоплювати і аналізувати електричні сигнали для розуміння програмної начинки пристрою. Аналогічним чином можуть бути перехоплені і радіосигнали. Після того, як зловмисник отримав доступ до кодів, він може підключатися до лічильника і віддавати йому команди, причому цим командам будуть підкорятися всі лічильники певної марки в межах мережі. Дослідниками з Університету Південної Кароліни, Університету Рутжерса (Rutgers University), а також компанії Applied Communication Sciences було встановлено, що в поширених інтелектуальних лічильниках досить легко провести реверс-інжиніринг комунікаційних протоколів, використовуваних в AMR, а також атаки типу «маскарад» (spoofing). Це дозволяє втручатися в роботу лічильника, спотворювати показання і керувати ним. Ніяких алгоритмів шифрування в лічильниках не використовується, що дозволяє будь-якому охочому «прослуховувати» дані. Зловмисники можуть віддалено контролювати, чи є хто в квартирі, шляхом знімання інформації про рівень енергоспоживання лічильника. Також можлива атака, яка веде до розряду акумулятора лічильника.

При отриманні сигналу активації він відразу ж передає пакет, тому при безперервному подаванні безлічі таких сигналів лічильник може швидко розрядитися. Атаки типу «маскарад» призводять до втрати цілісності даних і їх

спотворення. Як виявилося, в системах інтелектуального обліку не передбачена аутентифікація. Крім того, перевірка на вході також відсутня. При отриманні кількох пакетів з однаковим ID і різними показниками лічильника, зчитувач приймає пакет з найсильнішим сигналом. При використанні більш сучасної моделі зчитувача, який виробляє таку перевірку, існує можливість простий блокування пакетів з легітимного лічильника і перенаправлення зчитувача на прийом пакетів з підставного пристрою. [8]

2.2.2. Мережева вразливість.

Одним з можливих рішень захисту інтелектуальних лічильників є Smartsynch Universal Communications Model, - модель інтелектуального лічильника в збірці, що дозволяє замінювати застарілі контролери, на нові підтримують аутентифікацію і шифрування, без необхідності видалення з мережі лічильника. Для бездротових мереж основні цілі безпеки залишаються такими ж, як і для провідних мереж: збереження конфіденційності, гарантія недоторканності і забезпечення доступності інформації. Таким чином, визначення ризиків для конфіденційності сенсорних мереж являє собою ступінь доступності даних, що передаються, які представляють найвищу цінність. За ступенем важливості способи, за допомогою яких зловмисник може скомпрометувати конфіденційність даних, виділяються атаки за допомогою яких визначається несуча частота, розмір повідомлення, рівень сигналу і відомості про маршрутизації інформації. Ці дані виходять за допомогою мережевого сніффер, який здійснює прослуховування інформації про маршрутизації даних.

При вивченні схеми проходження трафіку сенсорної мережі можна простежити розташування базової станції або іншого стратегічно розташованого вузла. Більш того, протоколи маршрутизації многоскачковой зв'язку надають можливість зловмиснику простежити весь потік повідомлень і визначити джерело інформації. Будь-який аналіз мережевого трафіку або декодування пакетів може бути здійснений в реальному часі, або в режимі офлайн (при відсутності підключення) за допомогою наявної бази даних описів пакетів.

Більшість які підтримуються в даний час бездротових атак підпадають під одну з наступних категорій:

1. Атаки на конфіденційність: Ці атаки намагаються перехопити секретну інформацію, що надсилається засобами бездротової передачі.

2. Атаки на недоторканність: Дані атаки посилають фрейми (структурні одиниці інформації) помилкового контролю, управління або містять дані для виникнення збою на одержувача, або використовуються для полегшення проведення іншого типу атак.

3. Атаки на доступність: Ці атаки перешкоджають доставці бездротових повідомлень для легалізації користувачів за допомогою виводу з ладу мережевих ресурсів.

2.3 Безпечна передача даних в мережі ZigBee на прикладі радіомодулів XBee

Для реалізації завдань, поставлених в дипломній роботі можна обрати радіомодуль XBee або XBee Pro американської компанії Digi International. Детальні характеристики обладнання приведені в таблиці 2.1.

Таблиця 2.1 - Технічні характеристики модулів Xbee, XBee PRO

| Параметри | XBee | XBee Pro |
|---|---|---|
| Радіус дії в приміщенні, м | 30-100 | 100-1000 |
| Радіус дії у просторі, м | 100 | >1000 |
| Вихідна потужність, мВт | 1 | 100 |
| Швидкість передачі передачі, кбит/сек | 250 | |
| Чутливість приймача, дБм | -92 | -100 |
| Струм споживання в режимі прийому, мА | 45 | 270 |
| Діапазон частот, ГГц | 2,4 | |
| Рабоча температура | -40ºС …+85 ºС | |
| Кількість каналів | 16 | 13 |
| Ціна за одиницю | ≈799 | ≈1299 |

2.3.1 Безпека даних в ZigBee

У мережах ZigBee передбачено кілька механізмів криптографічного захисту даних (Security), всі або деякі з яких можуть бути задіяні розробником:

- шифрування AES 128-біт;

- 2 типу ключів шифрування;

- підтримка центру довіри (Trust Center);

- механізми перевірки цілісності повідомлення (Integrity) і перевірки його справжності (Authentication).

Специфікація ZigBee включає три режими безпеки (Security modes) - локальний (residential), стандартний і підвищений. Локальна безпека була вперше введена в стандарті ZigBee 2006. Вона вимагає, щоб ключ шифрування був встановлений на всіх пристроях, що підключаються до мережі. Стандартний режим безпеки додає деякі опціональні можливості, а також вводить шифрування на рівні додатку (APS layer link key). Підвищена безпека передбачає перевірку справжності і деякі інші удосконалення, які в даний час не підтримуються виробниками ZigBee-стеків в достатній мірі.[7]

Модулі XBee ZB, в основному, підтримують стандартний режим безпеки. У той же час, кінцеві пристрої, що підтримують локальний режим безпеки, можуть підключатися і взаємодіяти з вузлами мережі, що працюють зі стандартним режимом безпеки. Далі розглядаються різні аспекти шифрування даних саме для режиму стандартної безпеки.

Безпека в ZigBee використовується як на мережевому рівні, так і на рівні додатку. Передана по ефіру інформація шифрується за допомогою алгоритму AES з довжиною ключа 128 біт. Як ключів шифрування застосовується мережевий ключ (Network Key) і опціональний зв'язковий ключ (Link Key). Ключі шифрування є деякою 128-бітну послідовність (16 байт), яка вручну завантажується в модуль або формується їм самостійно. Витягти ключ з модуля неможливо. Тільки ті два ZigBee-вузла, які містять однакові ключі шифрування, можуть взаємодіяти між собою. Роутери та кінцеві пристрої, які працюють в мережі з включеною безпекою, повинні отримати правильні ключі шифрування.

Центр довіри в мережі ZigBee з безпекою авторизує підключаються до мережі вузли і виконує розсилку ключів шифрування. Зазвичай в якості центру довіри виступає координатор.[9]

2.3.2 Безпека на мережевому рівні

Ключ мережі застосовується для шифрування даних користувача (Application Data) і додаткової інформації верхнього рівня (APS Layer). APS Layer - це надбудова над корисними даними, пов'язана з поняттям «профілів» в ZigBee (включає інформацію про профілі, кластері і кінцевих точках). Крім захисту власне корисного навантаження (Payload), безпеку на мережевому рівні забезпечується шифруванням даних, пов'язаних зі службовими мережевим операціями, такими як прокладка маршрутів і команди рівнів APS і ZDO. Мережева безпека не поширюється на MAC-рівень. Така інформація як PAN ID або адреси MAC-рівня не шифруються. Це означає, що будь-який пристрій 802.15.4 може коректно прийняти пакет, який передається в ZigBee-мережі з включеною безпекою, проте отримати доступ до даних, розташованим за MAC-заголовком, йому не вдасться - там воно виявить незрозумілий набір бітів. Якщо в ZigBee-мережі включений режим безпеки, то всі пакети з даними передаються тільки в зашифрованому вигляді за допомогою 128-біт алгоритму AES (рис. 2.1).


Рисунок 2.1 — Шифрування на мережевому рівні

Мережевий заголовок зашифрованого пакета включає 32-біт лічильник фреймів. Кожен вузол в мережі підтримує власний 32-біт лічильник фреймів, який збільшується на 1 при відправці будь-якого пакета. Додатково, кожен вузол відстежує лічильники фреймів всіх сусідніх вузлів. Якщо отримується пакет від сусіднього вузла має номер фрейма менший, ніж був до цього, такий пакет

відкидається. Лічильники фреймів використовуються для протистояння т.зв. злому захисту шляхом заміщення оригіналу (Replay attacks). Лічильник фреймів послідовно збільшується до свого максимального значення 0xFFFFFFFF і далі не змінюється. При досягненні його максимального значення вузол не зможе більше відправляти пакети. У зв'язку з великою розрядністю переповнення лічильника фреймів малоймовірно - при відправці повідомлень щосекунди насичення лічильника станеться через 136 років. Для підтримки високого ступеня захисту обнулення лічильника фреймів можливо тільки при зміні мережевого ключа шифрування.[2][6]

Мережевий заголовок, APS-заголовок і корисні дані доповнюються сертифікатом справжності. Над вмістом цих полів виконується хешування, і до пакету додається код цілісності мережевого повідомлення (4-байт Network Message Integrity Code, nMIC). nMIC-код дозволяє одержувачеві бути впевненим в тому, що повідомлення не було змінено. nMIC-код забезпечує цілісність повідомлень в мережі ZigBee (message integrity). Якщо вузол отримує пакет з nMIC-кодом, що не відповідає прийнятим повідомленням, такий пакет відкидається.

В безпечної ZigBee-мережі пакет дешифрується і шифрується за будь-якої ретрансляції на всьому маршруті проходження. Проміжний вузол дешифрує пакет і перевіряє його цілісність. Якщо пакет призначений не із сайтом, то дані знову зашифровуються і автентифіковані на основі лічильника фреймів і мережевого адреси (входять в мережевий заголовок) проміжного вузла. Додаткові операції в мережі з безпекою збільшують затримки при доставці повідомлень. Крім того, максимальний обсяг корисних даних в пакеті зменшується на 18 байт за рахунок додавання лічильника фреймів, адреси джерела, MIC-коду і деяких інших службових байтів.

2.3.3 Безпека на рівні додатку

Безпека на рівні додатку (APS layer security) дозволяє зашифрувати корисні дані за допомогою ключа шифрування, відомому тільки відправнику і одержувачу пакета. У той час як мережеве шифрування на базі мережевого

ключа застосовується до всіх повідомлень всередині мережі, шифрування на рівні додатку є необов'язковим і може використовуватися тільки при надсиланні конкретного пакета. Шифрування на рівні програми не може застосовуватися до широкомовною розсилок. Шифрування корисних даних і формування коду цілісності повідомлення виробляється на основі 128-біт алгоритму AES (див. рис. 2.2).

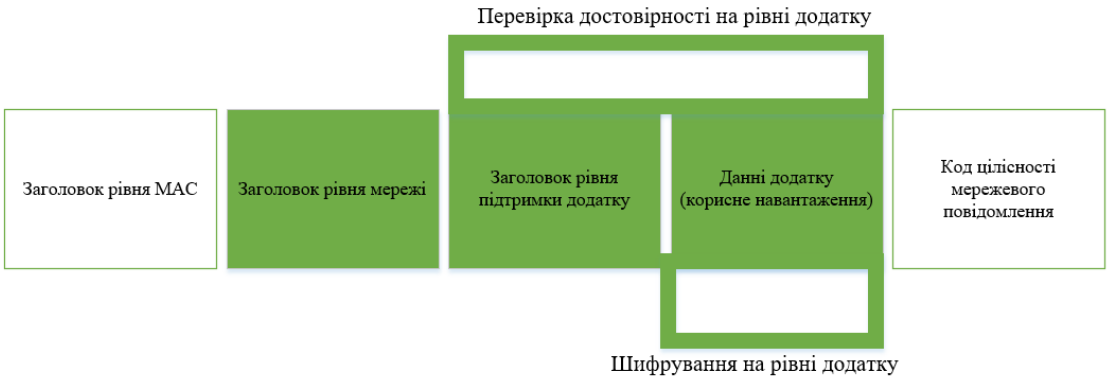


Рисунок 2.2 — Шифрування на рівні додатку

Код цілісності повідомлення (APS Message Integrity Code, aMIC-код) в даному випадку відрізняється від nMIC-коду, одержуваного при шифруванні на рівні мережі (Network Message Integrity Code). Одержувач повідомлення не буде використовувати прийнятий пакет, якщо обчислюється їм хеш-функція над корисними даними дасть результат, відмінний від aMIC-коду в самому пакеті. При шифруванні на рівні програми використовуються два типи ключів - зв'язковий ключ для обміну даними з центром довіри і ключ шифрування даних програми. Проміжні вузли мережі не можуть отримати доступ до цих даних, тому що ключ шифрування даних додатка відомий тільки відправнику і одержувачу. Використання безпеки на рівні додатку зменшує максимальну величину корисних даних на 9 байт. На рис. 2.3 наведена діаграма пакета для випадку одночасного використання безпеки на рівні мережі і на рівні додатку.

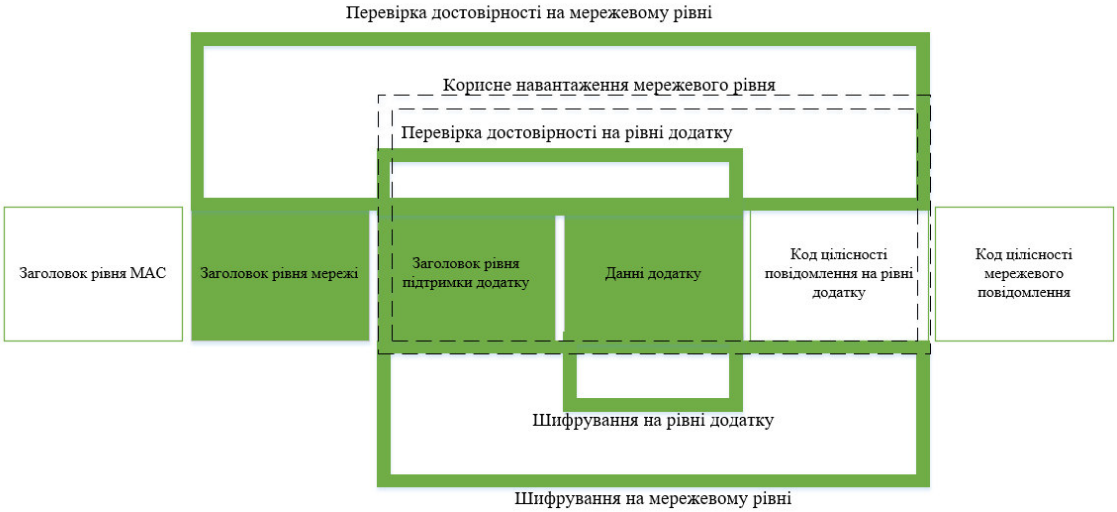


Рисунок 2.3 — Шифрування на рівні мережі і додатки

### 2.3.4 Формування ZigBee-мережі з безпекою

Координатор відповідає за вибір мережевого ключа шифрування. Ключ мережі (Network key) може бути визначено з самого початку (примусово записаний в координатор) або обраний координаторам самостійно випадковим чином. Зазвичай координатор виступає в ролі центру довіри, тому він керує формуванням і роздачею зв'язкового ключа (Link key). Зв'язковий ключ може бути обраний випадковим чином або попередньо записаний в модуль. Кожне що підключається до мережі новий пристрій має отримати мережевий ключ в процесі приєднання до мережі. Якщо підключається пристрій має зв'язковою ключ (встановлений примусово), то тоді передача мережевого ключа відбувається в зашифрованому вигляді - для шифрування використовується встановлений зв'язковий ключ. В іншому випадку передача мережевого ключа виконується у відкритому вигляді, проте центр довіри повинен вирішити, відправляти чи ні ключ в незашифрованому вигляді. Не рекомендується використовувати відкриту відсилання мережевого ключа шифрування, тому що це створює дірку в безпеці. Для забезпечення максимальної закритості системи все вузли повинні вводитися в мережу з передвстановленим коректним зв'язковим ключем.[2]

2.3.5 Шифрування даних в модулях XBee

Радіомодулі XBee (див. рис. 2.4) містять вбудований стек ZigBee Pro і підтримують безпечну передачу даних. У прошивці ZB режим безпеки за замовчуванням відключений (EE = 0). Якщо безпеку ввімкнено (EE = 1), то новий вузол отримує мережевий ключ в момент приєднання до мережі. Опціонально можна використовувати шифрування на рівні додатку. Для включення режиму безпеки параметр EE повинен бути встановлений в 1. Після установки параметра EE необхідно подати команду AC (застосувати настройки). При включенні режиму безпеки модуль виходить з існуючої мережі і намагається сформувати (координатор) або підключитися (роутер, кінцеве пристрій) до нової мережі. При EE = 1 всі дані шифруються на основі мережевого ключа. Шифрування даних призводить до зменшення максимального розміру корисного повідомлення. Команда NP дозволяє дізнатися максимальний розмір пакету, який можливий при поточних настройках параметрів безпеки. Параметр EE повинен бути встановлений однаково на всіх модулях, які працюють в одній мережі. Це значення слід зберегти в незалежній пам'яті за допомогою команди WR.


Рисунок 2.4 — Радіомодулі XBee

Координатор призначає мережевий ключ для всієї мережі. Команда NK використовується для завдання мережевого ключа на координатора. За допомогою команди NK можна записати мережевий ключ, проте вважати його не можна. Якщо NK = 0 (за замовчуванням), то мережевий ключ вибирається випадковим чином. Це цілком підходящий варіант для більшості завдань. В іншому випадку, якщо NK ≠ 0, то мережевий ключ визначається значенням NK.

Параметр NK встановлюється тільки на координатора. Роутери та кінцеві пристрої з включеним режимом безпеки (ATEE = 1) отримують мережевий ключ в момент приєднання до мережі. Ключ мережі передається від координатора в закритому вигляді, якщо в приєднується вузол був попередньо записаний правильний зв'язковий ключ.

Зв'язковий ключ також задається координатором за допомогою параметра KY. За замовчуванням KY = 0, тобто координатор вибирає зв'язковий ключ випадковим чином (нерекомендовані режим). Ключ мережі можна встановити примусово, задавши будь-яке значення KY, відмінне від 0. Параметр KY можна прочитати (тільки запис). Якщо зв'язковий ключ обраний координатором випадковим чином, то цей ключ невідомий підключається вузлу, тому не може використовуватися для шифрування. У цьому випадку передача мережевого ключа проводиться у відкритому вигляді, що знижує безпеку системи в цілому. Можна заборонити координатору розсилку мережевого ключа у відкритому вигляді за допомогою команди EO (біт 1). Якщо KY встановлений примусово (будь-яке значення, крім 0), то мережевий ключ передається в зашифрованому вигляді. Для його отримання те ж значення зв'язкового ключа (KY) має бути задане для підключається до мережі вузла. Таким чином, якщо на координатора KY НЕ дорівнює 0, то до мережі можуть підключитися тільки попередньо сконфігуровані модулі, в які було примусово прописано те ж значення KY.

Команда EO використовується для призначення координатора центром довіри. Якщо координатор виступає в якості центру довіри, йому повідомляється про кожному новому модулі, який намагається підключитися до мережі. У прошивці ZB безпечна передача даних може працювати як в режимі з центром довіри, так і без нього. Якщо мережа працює з використанням центру довіри (EO = 2), то зміна параметра NK на координатора призведе до зміни мережевих ключів шифрування на всіх вузлах мережі. При цьому зміна NK не форсує відключення і повторне підключення вузлів. Мережа продовжить роботу на тому ж каналі з тим же значенням PAN ID, але все вузли оновлять свій мережевий ключ (з обнуленням лічильника фреймів). Якщо координатор не виступає в ролі

центру довіри, то для мережевого скидання може використовуватися широкомовна команда NR1 (з будь-якого вузла мережі). За цією командою всі пристрої залишають поточну мережу і намагаються підключитися знову. Коли втрачено мережу, лічильник фреймів обнуляється. Дана команда виконується відносно довго (~ 10 с), тому що спочатку координатор виконує стандартний процес запуску мережі (вибір частотного каналу, PAN ID і т.д.), потім підключаються всі модулі, які покинули попередню мережу.

Опціональне шифрування даних на рівні програми не підтримується в поточній версії програмно-апаратних засобів.

2.3.6 Приклади налаштувань XBee

У наведених прикладах використовуються конкретні значення параметрів модуля XBee для роботи з різними режимами безпеки. Використовуваный запис виду EE = 1 не відповідає формату відправлених AT-команд. Для реального задання значення за допомогою AT-команд необхідно надіслати через UART модуль рядок виду ATEE1. При роботі з API-фреймами параметр AT-команди вказується в бінарному вигляді у відповідному полі відправляється структури.

Приклад 1. Формування мережі з включеною безпекою (зв'язковий ключ задається вручну)

Запускаемо координатор з наступними настройками:

- ID = 3345 встановити мережевий ідентифікатор PAN ID (значення вибрано довільно);

- EE = 1 включити режим безпечної передачі даних;

- NK = 0 згенерувати мережевий ключ випадковим чином;

- KY = 9ABC задати значення для зв'язкового ключа (вибрано довільно);

- WR зберегти настройки в незалежній пам'яті.

Далі чекаємо, коли у відповідь на команду AI прийде значення 0 ( «Успішний старт мережі»). Потім підключаємо до мережі роутер (и) з тими ж самими настройками. Після приєднання до мережі передача даних між вузлами буде виконуватися в зашифрованому вигляді на основі випадково обраного мережевого ключа. Ключ мережі надаватиметься координатором кожному

новому вузлу мережі. Передача мережевого ключа буде відбуватися в зашифрованому вигляді - для шифрування використовується зв'язковий ключ KY = 9ABC. В даному прикладі мережевий ключ шифрування неможливо прочитати ні з одного вузла мережі.

Приклад 2. Формування мережі з включеною безпекою зі значеннями ключів за замовчуванням:

Стартуємо координатор з наступними настройками:

- ID = 6678 встановити мережевий ідентифікатор PAN ID (значення вибрано довільно);

- EE = 1 включити режим безпечної передачі даних;

- NK = 0 згенерувати мережевий ключ випадковим чином;

- KY = 0 згенерувати зв'язковий ключ випадковим чином;

- WR зберегти настройки в незалежній пам'яті.

Після формування координатором мережі (коли у відповідь на команду AI прийде значення 0) підключаємо до мережі роутер(и) з тими ж самими настройками (крім параметра NK). Після приєднання до мережі передача даних між вузлами виконується в зашифрованому вигляді на основі випадково обраного мережевого ключа. У цьому прикладі мережевий ключ відсилається координатором в незашифрованому вигляді. Це вразливе місце в безпеці, тому використання налаштувань за замовчуванням не рекомендується.

2.3.7 Влив параметрів на доступність мережі

Принцип роботи XBee при вимкненому шифруванні, які параметри впливають на «доступність» мережі для сторонніх підключень в тих випадках, коли шифрування в мережі не включено (EE = 0). В цьому випадку можна налаштувати мережу таким чином, що до неї не зможуть підключитися небажані пристрої. Мова йде про випадкових або цілеспрямованих спробах втрутитися в роботу мережі за допомогою стандартних модулів (тобто працюють відповідно до специфікації ZigBee).

На підключення до мережі впливають мережеві параметри ID і NJ. Якщо залишити на координатора і роутерах значення PAN ID за замовчуванням (ID =

0), це призведе до того, що реальне значення PAN ID буде вибрано координатором випадковим чином, а роутер буде готовий підключитися до будь-якої мережі. При такому варіанті налаштувань до мережі зможе підключитися будь-який «модуль з коробки». Установка конкретного значення для PAN ID стане своєрідним фільтром, відтинає підключення сторонніх модулів.

Підключення до такої мережі неможливо без знання реального PAN ID. Ще одним параметром, що обмежує «відкритість» мереж без шифрування, є дозволений час підключення (NJ). За замовчуванням NJ = FF, і підключення нових пристроїв до мережі не обмежена за часом. Установка NJ в будь-яке значення менше 0xFF задає граничний час в секундах, протягом якого підключення до мережі дозволено (через конкретний роутер або координатор).

Рекомендується обмежувати час доступу в мережу і надавати його тільки на період розгортання мережі. Якщо в процесі роботи виникне необхідність підключення додаткового пристрою, для цього можна перезаписати значення NJ на якомусь мережевому вузлі для створення нового тимчасового вікна доступності мережі.

Висновок другого розділу

Вбудовані в модулі XBee можливості шифрування дозволяють будувати бездротові мережі з гарантованим рівнем криптостійкості. Захист і аутентифікація даних забезпечується за допомогою алгоритму шифрування AES-128. Залежно від розв'язуваних завдань розробник має можливість гнучко налаштовувати рівень безпеки розгортаємої ZigBee-мережі.

# РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою розділу є технічно-економічне обґрунтування доцільності впровадження технічних засобів та програмного забезпечення в цілях захисту бездротових мереж в системі ЖКГ.

Для проведення обчислень було вибрано ЖКГ «Департамент Житлового Господарства ДМР», Шевченківського району, вул. Воскресінська,16, м. Дніпро, який в середньому обслуговує 1600 квартир, для проведення захисту можна використати існуючі ПК в самій організації та закупити модулі XBee в розмірі 1600 для кожного помешкання в районі. Необхідні апаратні ресурси приведені у таблиці 3.1.

| Найменування | Характеристика | Вартість в гривнях |
|---|---|---|
| Комплект Maxstream XBee Series 2 (AMP-X124) | 1600 модулей XBee Series 2 и 1600 переходных плат с интерфейсами RS-232 для встановлення в лічильник. ПЗ включено (API) | 128000 |
| ZigBee Operator | Програмне забезпечення для роботы з модулями Xbee | 2000 |

Таблиця 3.1 – Устаткування моніторингу мережі

Для економічного обґрунтування запропонованих рішень необхідно здійснити наступні розрахунки:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект;

– показники економічної ефективності застосування моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації.

3.1 Розрахунок (фіксованих) капітальних витрат

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

3.1.1. Визначення витрат на придбання обладнання та опрацювання ПЗ для захисту БММ.

3.1.1.1. Визначення трудомісткості використання та опрацювання програмного продукту для захисту БММ.

Трудомісткість створення захисту визначається тривалістю кожної робочої операції:

$$t = t_{mз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин,} \quad (2.1)$$

де $t_{mз}$ – тривалість складання технічного завдання на експлуатацію ПЗ, $t_{mз} = 10$

$t_{в}$ – тривалість вивчення ТЗ, $t_{в} = 4,47$;

$t_{а}$ – тривалість розробки алгоритму для впровадження технології, $t_{а} = 9,54$;

$t_{пр}$ – тривалість встановлення обладнання за розробленим алгоритмом, $t_{пр} = 11,93$;

$t_{опр}$ – тривалість опрацювання програми на ПК, $t_{обр} = 89,43$;

$t_{д}$ – тривалість підготовки технічної документації на ПЗ, $t_{д} = 21,34$.

t = 10 + 4,47 + 9,54 + 11,93 + 89,43 + 21,34 = 146,7 годин,

3.1.1.2 Розрахунок витрат на встановлення ПЗ

Витрати на встановлення програмного продукту Кпз складаються з витрат на заробітну плату виконавця програмного забезпечення Ззп і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК Змч:

$К_{пз} = З_{зп} + З_{мч}$ = 11000 + 332,61 = 11332,61 грн.

$З_{зп} = t*З_{пр}$ = 146,7 *75 = 11000 грн.

де $t$ – загальна тривалість створення ПЗ, годин;

*Зпр* – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину. *Зпр* = 75 грн/год.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{д}\ ,\ \text{грн}, \qquad (2.2)$$

$$З_{мч} = 332{,}60\ \text{грн},$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P\ \cdot t_{нал} \cdot Се + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}\ ,\ \text{грн} \qquad (2.3)$$

де $P$ – встановлена потужність ПК, кВт, Р = 0,25;

$С_е$ – тариф на електричну енергію, грн/кВт · година ,$С_е$ = 1,68;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн. $Ф_{зал}$ = 4500;

$Н_а$ – річна норма амортизації на ПК, частки одиниці , $Н_а$ = 0,5 ;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці, $Н_{апз}$ = 0,2;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн. $К_{лпз}$ = 2000;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня

$F_р$ = 1920.

$С_{мч}$ = 3,48 , грн

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пз} + К_{аз} + К_{навч} + К_{н} = 157200 \text{ грн.} \quad (2.4)$$

де $К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, $К_{навч}$ = 3000 грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad \text{тис. грн.} \quad (2.5)$$

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{єв} + С_{ел} + С_{о} + С_{тос}, \text{ грн.} \quad (2.6)$$

С = 20000 + 52530 + 648000 + 142600 + 2580 + 3152 = 868862, грн.

$С_{н}$ – витрати на навчання адміністративного персоналу й кінцевих користувачів, $С_{н}$ = 20000;

$С_{а}$ – річний фонд амортизаційних відрахувань, $С_{а}$ = 52530;

$С_{а}$ = К/3 = 157200/ 3 = 52530

$С_з$ – Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}\text{ , грн.} \quad (2.7)$$

$$С_з = 648000\text{, грн}$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

$З_{осн}$ = 600000, грн

$З_{дод}$ = 48000, грн

Вартість електроенергії, що споживається апаратурою, системою інформаційної безпеки протягом року (грн)

$$С_{ел} = Р \cdot F_р \cdot Ц_е\text{ , грн.,} \quad (2.8)$$

$$С_{ел} = 0{,}8*1920*1{,}68 = 2580{,}48\text{ грн.}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р = 0,2 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) визначаються за даними організації.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%).

$С_{тос}$ = К * 0.02;

$С_{тос}$ = 157200 *0.02 = 3152;

$С_{єв} = С_з * 0.22$ = 648000 * 0.22 = 142600;

## 3.3 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Слід розрахувати величину відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \quad (3.1)$$

$$U = 1250 + 63950 + 565 = 65765 \text{ грн}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \quad (3.2)$$

$$П_п = \frac{12000 + 10000}{176} \cdot 10 = 1250 \text{ грн}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.3)$$

$$П_в = 341 + 682 + 63000 = 64023 \text{ грн}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента

корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} \quad (3.4)$$

$$П_{ви} = \frac{20000}{176} \cdot 5 = 341 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \quad (3.5)$$

$$П_{пв} = \frac{24000}{176} \cdot 5 = 682 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{Fг} \cdot (t_п + t_в + t_{ви}) \quad (3.6)$$

$$V = \frac{9677000}{2080} \cdot (10 + 3 + 5) = 81280$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum_i \sum_n U . \quad (3.7)$$

$$B = 3 \cdot 15 \cdot 65765 = 2959425$$

Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \quad (3.8)$$

$$E = 2959425 \cdot 0.7 - 999100 = 1072498$$

де $B$ – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

$R$ – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

$C$ – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

а) сукупна вартість володіння (TCO);

б) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

в) термін окупності капітальних інвестицій $T_o$.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K} \qquad (4.1)$$

$$ROSI = \frac{1072498}{157600} = 6,8$$

де Е – загальний ефект від впровадження системи інформаційної безпеки грн;

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

Оскільки організація здійснює фінансування капітальних інвестицій систему інформаційної безпеки за рахунок позикових коштів, тобто за рахунок банківського кредиту, то в якості бажаного значення $E_н$ варто приймати величину плати за кредит (кредитної ставки) $N_{кр}$.

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

$$ROSI > (N_{кр} + N_{інф})/100 , \qquad (4.2)$$

$$6,8 > (0,12 + 0,089)/100$$

$$6,8 > 0,2$$

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

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

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} \tag{4.3}$$

$$T_O = \frac{1}{6,8} = 0.15 \text{ років}$$

Висновок до третього розділу

Оцінивши коефіцієнт повернення інвестицій та термін окупності капітальних інвестицій можна вважати що розробка та введення в експлуатацію системи моніторингу енергоресурсів з використанням бездротової мережі є економічно доцільною, оскільки при введенні в експлуатацію системи захисту можна спостерігати позитивний економічний ефект. Про це свідчать такі показники як ROSSI, значення якого 6,8 що значно більше ніж величина банківської кредитної ставки з урахуванням інфляції 0,2, враховуючи це та термін окупності інвестицій, проект є економічно доцільним.

# ВИСНОВКИ

У дипломній роботі розв’язано завдання щодо підвищення рівня інформаційної безпеки та дослідження захищеності бездротових мереж передачі інформації.

В ході розв’язання поставлених задач були отримані наступні результати:

1. Проаналізовані види бездротової передачі інформації та АСКОЕ.
2. Проаналізовано ймовірні ризики та атаки в мережі моніторингу енергоносіїв.
3. Запропоновано використання додаткової аппаратури для підвищення рівня захищення бездротової мережі.
4. Розраховано витрати на впровадження технології захисту бездротової мережі моніторингу та обліку, передачі інформації в цілому.

Практична значимість дипломної роботи полягає у впровадженні рекомендацій для підвищення рівня інформаційної безпеки для підприємств, що надають комунальні послуги та захисту енергоносіїв в секторі енергозбереження.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Шахнович А. Беспроводные сети (Электронный ресурс) / Способ доступа: URL: http://www.flylik.ru/info/articles.

2. Соколов М. Программно-аппаратное обеспечение беспроводных сетей на основе техологии Zigbee/802.15.4 // Электронные компоненты. - №12. – 2004.

3. В.С. Коваленко. Методи захисту бездротових мереж (Електронний ресурс) / Спосіб доступу:URL: http://elartu.tntu.edu.ua.

4. Маркелов К.С., Нейман А.Б. Безопасность беспроводных сетей // Молодой ученый. – 2012. – № 4. – С. 63–66.

5. Франчук В.М. Захист даних в безпровідних комп'ютерних мережах. // Науковий часопис НПУ імені М.П. Драгоманова. Серія№2. Комп'ютерноорієнтовані системи навчання: Збірник наукових праць. /Редрада. – К.: НПУ імені М.П. Драгоманова, 2011. – №10 (17).

6. Олег Пушкарев. Программируемые модули XBee серии S2B//Беспроводные технологии. 2010. № 3.

7. Лекнин В. Спецификация ZigBee. Безопасность (Электронный ресурс) / Способ доступа: URL: https://habr.com/post/158355/.

8. Ковальова Ю.В., дисертаційні дослідження на тему: "Інформаційні технології оцінювання часу життя автономних бездротових мереж моніторингу енергоспоживання об'єктів критичної інфраструктури", 2018.

9. Е. Баранова. IEEE 802.15.4 и его программная надстройка ZigBee. Интернет-журнал по широкополосным сетям и мультимедийным технологиям(Электронный ресурс)/Способ доступа: URL: http://www.telemultimedia.ru/art.php?id=292.

10. Comparing the Digi XBee API with EmberZNet EM260 API URL: http://www.compel.ru/images/news/2009080501/wp_xbeeapivsember.pdf.

11. Описание XBee/XBee-PRO ZB RF Modules (Электронный ресурс) /Способ доступа: URL: www.digi.com.

12. ZigBee Specification, Document 053474r17 / URL: www.zigbee.org.

13. Е.С.Семенистая, Н.С. Линник, А.А.Горбунов Обзор существующих схем деления систем учета расхода энергоресурсов и воды и разработка схемы деления нового типа // Инженерный вестник Дона, 2016, №4 URL: ivdon.ru/ru/magazine/archive/n4y2016/3860

14. Дмитриев В. Технология Zigbee// Компоненты и технологии. – №1. – 2004

15. HABR Сети ZigBee. Зачем и почему? (Електронний ресурс) / Спосіб доступу: URL: https://habr.com/post/155037/

16. Прошин И.А., Егоров С.В., Шепелев М.В. АВТОМАТИЗАЦИЯ УЧЁТА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ КАК СРЕДСТВО ПОВЫШЕНИЯ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ // Технические науки - от теории к практике: сб. ст. по матер. XXXIII междунар. науч.-практ. конф. № 4(29). – Новосибирск: СибАК, 2014 (Електронний ресурс) / Спосіб доступу: URL: https://sibac.info/conf/tech/xxxiii/38004

17. Зуб М. А. Исследование алгоритмов маршрутизации в динамических сетях на базе технологии ZigBee (Електронний ресурс) / Спосіб доступу: URL: http://masters.donntu.org/2010/fknt/zub/diss/index.htm

18. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

19. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. М.: 2000г

20. Галицкий А.В. и др. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2005. - 616 с.

21. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / Упоряд.: О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв,О.В. Кручінін. – Дніпро: НГУ, 2018. – 50 с.

ДОДАТОК А. Відомість матеріалів дипломного проекту

| № | Формат | Найменування | Кількість листів | Примітка |
|---|---|---|---|---|
| 1 | А4 | Реферат | 3 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 3 | |
| 4 | А4 | Вступ | 2 | |
| 5 | А4 | 1 Розділ | 20 | |
| 6 | А4 | 2 Розділ | 24 | |
| 7 | А4 | 3 Розділ | 11 | |
| 8 | А4 | Висновки | 1 | |
| 9 | А4 | Перелік посилань | 2 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 1 | |
| 12 | А4 | Додаток В | 1 | |
| 13 | А4 | Додаток Г | 1 | |

# ДОДАТОК Б. Перелік файлів на електронному носії

1. ПояснювальнаЗаписка.docx
2. Реферат.docx
3. УмовніСкорочення.docx
4. Зміст.docx
5. Вступ.docx
6. Розділ1.docx
7. Розділ2.docx
8. Розділ3.docx
9. Висновки.docx
10. СписокЛітератури.docx
11. ДодатокА.docx
12. ДодатокБ.docx
13. ДодатокВ.docx
14. ДодатокГ .docx
15. Диплоний проект.pdf
16. Презентація_Диплом.pttx

# ДОДАТОК В. Відгук керівника економічного розділу

Керівник: _____ к.е.н, доц. Пілова Д.П.
(підпис)

# ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Кібербезпека систем обліку та моніторингу енергоносіїв в житлово-комунальному господарстві.
студента групи 125м-17-1
Жука Єгора Владиславовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 70 сторінках та містить 9 рисунків, 2 таблиць, 21 джерел та 4 додатка.

Розробка інтелектуальних систем обліку та управління споживанням енергетичних ресурсів в сфері житлово-комунального господарства є перспективною задачою, від вирішення якої залежить стратегія розвитку енергоринку держави. Актуальною проблемою використання бездротових мереж є захист даних, які передаються безпосередньо в мережі, оскільки комунікаційні сигнали при їх розповсюдженні через радіоефір доступні для перехоплення. Аналіз атак і вразливостей бездротових мереж моніторингу актуалізує питання проведення заходів щодо підвищення захищенності об’єктів комунального господарства.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав добрий рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. В дипломному проекті відображені форми загроз безпеці в бездротових мережах, що порушують роботу мережі.

Робота оформлена та написана відповідно до вимог щодо написання дипломних проектів. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а її автор Жук Єгор Владиславович заслуговує на оцінку «_____».

Керівник дипломної роботи,
к.ф.-м.н., доцент Гусев О.Ю.

Керівник спеціального розділу
ас. кафедри БІТ Ю.В. Ковальова