НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Радіотехнічний факультет
Радіоприймання та оброблення сигналів

«До захисту допущено»

ВО завідувача кафедри

_____А.В. Мовчанюк

“___”_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

з спеціальності (спеціалізації) 172 Телекомунікації та радіотехніка

на тему: Системи безпеки, які використовують GSM канали

Виконав: студент 4 курсу, групи РА-г61-1

Павленко Богдан Вікторович _____

Керівник старший викладач Бондаренко Г.І. _____

Консультант розділ охорона праці канд. техн. наук, доц. Гусєв А.М. _____

Рецензент старший викладач Новосад А.А. _____

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020 року

Завдання на дипломну роботу

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

Факультет (інститут) радіотехнічний

Кафедра радіоприймання та оброблення сигналів

Рівень вищої освіти – перший (бакалаврський)

Спеціальність (спеціалізація) 172 Телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ
ВО завідувача кафедри

_____ А.В. Мовчанюк

«___»_____2020 р.

ЗАВДАННЯ

на дипломну роботу студенту

Павленко Богдану Вікторовичу

1. Тема роботи: Системи безпеки, які використовують GSM канали
керівник роботи старший викладач Бондаренко Г.І.
затверджені наказом по університету від «___»_____ 2020 р. №_____
2. Строк подання студентом роботи: 10.06.2020 року
3. Вихідні дані до роботи: загальні вимоги до систем централізованого спостереження
4. Зміст (дипломної роботи) розрахунково-пояснювальної записки (перелік завдань, які потрібно розробити): огляд тенденцій розвитку систем безпеки, побудова систем безпеки з використанням GSM каналів зв'язку, аналіз функціонування систем безпеки, які використовують GSM канали, охорона праці та безпека в надзвичайних ситуаціях, загальні висновки.

5. Перелік (ілюстративного) графічного матеріалу (з точним зазначенням обов'язкових креслеників, плакатів тощо) презентація по роботі в обсязі не менше 15 слайдів

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Гусєв А.М.		

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Строк виконання етапів роботи	Примітка
1	Розробка технічного завдання	15.05.2020	
2	Огляд стану систем безпеки	20.05.2020	
3	Побудова систем безпеки	25.05.2020	
4	Аналіз функціонування систем безпеки	01.06.2020	
5	Розділ охорони праці	12.05.2020	
6	Підготовка графічного матеріалу	05.06.2020	

Студент _____ Павленко Б.В.

Керівник роботи _____ Бондаренко Г.І.

* Консультантом не може бути зазначено керівника дипломної роботи

Пояснювальна записка
до дипломної роботи

на тему: **СИСТЕМИ БЕЗПЕКИ, ЯКІ ВИКОРИСТОВУЮТЬ GSM КАНАЛИ**

Анотація

У дипломній роботі проводиться порівняння різних безпровідних технологій, детально розглянутий принцип побудови GSM- каналу в системах охорони, GSM порівнюється з іншими безпровідними технологіями.

Проведений огляд декількох основних безпровідних систем охорони, на їх прикладі був проведений аналіз його використання в різних системах охорони. Проведений аналіз функціонування систем безпеки, які використовують GSM канали, розглянуті принцип шифрування, завадостійкість та завадо-захищеність у GSM-каналі.

Сформульовані декілька основних принципів та рекомендацій по використанню GSM-каналу в системах охорони. Зазначені основні шляхи розвитку мереж GSM.

Представлений один із можливих варіантів розрахунку зони покриття окремо взятої базової станції.

Annotation

A comparison of different off-wire technologies, principle of construction of GSM considered in detail, is made in diploma work - to the channel in the systems of guard, GSM is compared to other off-wire technologies.

Conducted review of a few basic off-wire systems of guard, on their example there was the conducted analysis of his use in the different systems of guard. Conducted, analysis of functioning of the systems of safety that use GSM the channels considered principle of enciphering, noise immunity and noise protection in GSM- channel.

Several basic principles and recommendations for the use of GSM-channel in security systems are formulated. The main ways of development of GSM networks are indicated.

One of the possible options for calculating the coverage area of a single base station is presented.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ПКП – приймально-контрольний пункт

ПЦС – пульт центрального стеження

ПЦО – пункт центральної охорони

РСПС – радіосистем передачі сповіщень

УКХ – ультра короткі хвилі

ПК – персональний комп’ютер

ППКОП – прилад приймально-контрольний охоронно-пожежний

ОПС – охоронно-пожежна сигналізація

ППРЧ – програмна перебудова радіочастот

СЦС – системи централізованого спостереження

БС – базова станція

Wi-Fi – Wireless Fidelity

WLAN – Wireless Local Area Network

SMS – Short Message Service

GSM – Global System for Mobile Communications

DTMF – Dual-Tone Multi-Frequency

CSD – Circuit Switch Data

CLIP – Calling Line Identification Presentation

DSL – Digital Subscriber Line

RLC – Radio Link Control

GPRS – General Packet Radio Service

EDGE – Enhanced Data rates for GSM Evolution

MSC – Mobile Switching Centre

BSS – Base Station System

OMC – Operations and Maintenance Centre

MS – Mobile Stations

TDMA – Time Division Multiple Access

ВСТУП

Нині ринок послуг і устаткування охоронно-пожежної сигналізації нестримно росте. Проте до недавнього часу основним недоліком систем охоронної і пожежної сигналізації (ОПС) було використання дротяних телефонних ліній. До основних недоліків цих систем можна віднести нестійку роботу міських телефонних ліній, низьку фізичну захищеність, відсутність можливості охорони не телефонізованих об'єктів (дачі, котеджі і так далі). Тому в якості надійної альтернативи дротяним охоронним системам з'явився новий напрям або радіо-канальні охоронні системи.

Переваги радіоканальних охоронних систем очевидні:

- відсутність залежності від телефонної лінії і якість роботи мережі;
- простота монтажу;
- можливість охорони будь-якого об'єкту (в межах зони дії радіоканальної мережі);
- універсальність (з простих елементів можна побудувати складну систему);
- висока швидкість монтажу та запуску в експлуатацію;
- можливість оперативної зміни конфігурації;
- мобільність охоронного пульта;
- можливість співіснування декількох пультів;
- немає принципових обмежень для підключення у разі потреби до існуючої системи.

Спочатку безпровідні системи не отримали широкого поширення із-за низької надійності (дротяний зв'язок в цьому плані ще років п'ять назад був надійніший). Але нині з'явився широкий спектр різних додаткових пристроїв, активно використовуються нові покоління безпровідних систем зв’язку.

Повсюдне використання стільникових систем зв’язку позначилося на системах охорони. Можливості, що надаються операторами стільникового зв’язку все активніше використовуються в системах охорони. Також можна

бачити, що GSM канали зв’язку ще не вичерпали ліміт свого розвитку. На сьогодні безпровідні охоронні системи на базі GSM отримали широке поширення завдяки їх відносно невисокій вартості і простоті установки та експлуатації. Стільникова мережа стандарту GSM - 900/1800 забезпечує кращу якість зв’язку і вже розгорнута у більшості міст України та країнах СНГ.

Системи, які використовують GSM зв’язок, дозволяють здійснити охорону будь-яких об’єктів, у тому числі і не телефонізованих. Використання GSM позбавляє від необхідності розгортати свою мережу ретрансляторів тому, що використовуються ретранслятори GSM операторів. Внаслідок цього можна брати під охорону об’єкт скрізь, де упевнено працює мережа GSM оператора.

І, звичайно, дуже перспективним видається використання нових протоколів і мереж 3G, спеціально призначених для корпоративних клієнтів - віртуальні корпоративні мережі передачі даних із захистом інформації.

Проте істотним недоліком подібних систем є низька завадо-захищеність. Не секрет, що GSM канал легко подавити, "GSM глушилки" знаходяться сьогодні у вільному продажі, і робота мережі GSM не завжди відрізняється високою стабільністю і може відмовити в самий відповідний момент. Хоча останні розробки дозволяють повністю контролювати GSM канал, оперативно міняти частоти, що помітно підвищує завадо-захищеність.

Оптимально використати GSM канал в якості дублюючого або додаткового до дротяних або інших радіо-канальних систем. Величезним плюсом GSM систем є можливість самим клієнтом контролювати стан об’єкту і управляти його охороною.

1 ОГЛЯД СУЧАСНОГО СТАНУ СИСТЕМ БЕЗПЕКИ

1.1 Тенденції розвитку систем безпеки з точки зору використання різних каналів зв’язку

Сьогодні у світовій практиці охоронних послуг визначилася стійка тенденція на посилення ролі технічних засобів. Тенденція ця не випадкова: численні дослідження в області особистої і майнової безпеки показали, що широке використання технічних засобів дозволяє виключити або звести до мінімуму негативний вплив самої ненадійної ланки в системі охорони - людини, якій властиві стомлюваність, неуважність, халатність і тому подібне. При цьому, організація охорони за допомогою технічних засобів обходиться споживачеві значно дешевше, а її надійність вище. Найбільш ефективним і економічно вигідним видом охорони є централізована охорона. Суть її в тому, що інформація від технічних засобів, встановлених на територіально розосереджених об’єктах, поступає безпосередньо на центральний пульт, де в автоматизованому режимі робиться її аналіз, узагальнення і видача заявки на реагування технічній службі.

Технічну основу централізованої охорони складають системи централізованого спостереження (СЦС).

Найбільш широке застосування знайшли СЦС, що використовують як канали зв’язку телефонні лінії. Устаткування таких систем порівняно дешеве, а майже повсюдна телефонізація дозволяє підключати до них практично будь-які об’єкти.

В середині 90-х років при створенні СЦС основна увага приділялася таким аспектам, як:

- автоматизація, яка дозволяє до мінімуму спростити процеси здачі/взяття об’єктів під охорону, скоротити черговий персонал пультів централізованої охорони та істотно скоротити кількість хибних тривог;

- контроль каналів зв’язку, що забезпечує високу достовірність передачі;

- розробка широкої гамми об’єктових пристроїв з різними функціональними і сервісними можливостями, що дозволяють задовольнити потреби найбільших шарів населення.

З урахуванням цих вимог були розроблені і впроваджені такі системи, як «Ахтуба», «Юпітер», «Приток-А», «Фобос-А», «Фобос-3» та інші.

З точки зору організації захисту об’єктів від несанкціонованого проникнення (як по устаткуванню технічними засобами охорони, так і по тактиці дій чергових служб) всі перелічені СЦС не мають яких-небудь істотних відмінностей, проте, кожна з них має свої переваги і недоліки, які визначають і обмежують сферу їх застосування.

Проте головним недоліком вказаних систем є різнорідність технічних і конструктивних рішень, а також закрита архітектура побудови, що не дозволяє провести їх об’єднання в єдиний універсальний комплекс технічних засобів централізованої охорони в межах одного ПЦО. В підсумку це призводить до виникнення певних проблем для всіх структур позавідомчої охорони у впровадженні, експлуатації, обслуговуванні та ремонті різнорідних технічних засобів, у проведенні єдиної технічної політики, забезпеченні належного рівня якості та надійності устаткування, а, отже, до додаткових фінансових витрат і збільшення тарифів на охоронні послуги.

Тому найбільш актуальною на сьогодні, залишається проблема впорядкування парку систем централізованого спостереження, його оновлення, заміни застарілого устаткування сучасним, надійнішим.

Тому в цілях подальшого розвитку і вдосконалення централізованої охорони до нових розробок останнім часом висувають додаткові вимоги:

- імітостійкість і крипто-захист системи, що забезпечують стійкість системи до несанкціонованого обходу і обумовлені появою кваліфікованих крадіжок;

- висока інформативність, що забезпечує розділення сигналів про проникнення та пожежу, аварію або зміну параметрів лінії зв’язку і так далі;

- можливість сполучення системи з оптоволоконними каналами зв’язку, обумовлена впровадженням підприємствами зв’язку нових цифрових технологій передачі інформації;

- уніфікація створюваних технічних засобів, тобто можливість об’єднання різних пристроїв в єдиний програмно-апаратний комплекс централізованої охорони.

Пріоритетним завданням технічної політики в області розвитку централізованої охорони є розробка відсутніх на сьогодні єдиних вимог на системи централізованого спостереження, що в умовах різноманіття існуючих та нових підприємств-розробників і виробників засобів охоронно-пожежної сигналізації дозволить уніфікувати стики систем передачі сповіщень, що розробляються, і тих, що вже знаходяться в експлуатації.

Останніми роками особлива увага приділялася створенню і розвитку радіосистем передачі сповіщень (РСПС). Впровадження охоронних систем, що використовують радіочастотні канали зв’язку, дозволяє:

- розширити сферу діяльності підрозділів позавідомчої охорони шляхом організації охорони об’єктів, що не мають лінії телефонного зв'язку;

- підвищити надійність систем охорони особливо важливих об’єктів за рахунок дублювання телефонних каналів зв’язку;

- забезпечити при необхідності термінову установку обладнання на об’єкті, що потребує охорони.

Діяльність охороних компаній в цій області була спрямована на здешевлення устаткування радіосистем, з метою підвищення його доступності для населення. В той же час якість систем відносно споживчих властивостей і відносно надійності та захищеності інформації повинна постійно підвищуватися.

З цією метою перспективним напрямом є створення радіосистеми ближнього радіусу дії з пониженою вартістю об’єктового устаткування і поліпшеними тактико-технічними, вартісними і експлуатаційними

параметрами, що дозволяє організувати охорону таких об’єктів як гаражні і дачні кооперативи та садівничі товариства.

Переваги радіо-канальних охоронних систем:

- відсутність залежності від телефонної лінії і якості роботи мережі;
- простота монтажу;
- можливість охорони будь-якого об’єкту (в межах зони дії радіо-канальної мережі).

На сьогодні всі безпровідні системи можна розділити на чотири групи:

- GSM системи;
- радіо-канальні системи малого радіусу дії;
- радіо-канальні системи великого радіусу дії;
- супутникові системи.

GSM системи отримали широке поширення на початку XXI століття, після бурхливого розвитку мобільного зв’язку. Спочатку в якості канало-утворюючого обладнання використовувалися мобільні телефони, які підключалися до охоронних панелей через інтерфейс RS-232 та управлялися AT-командами. Це рішення було дуже ненадійним, оскільки телефони могли зависнути або просто відключитися, крім того, умови експлуатації мобільних телефонів не передбачали роботу в сирих і неопалюваних приміщеннях, що істотно обмежувало сферу їх застосування. Сьогодні виробники устаткування мобільного зв’язку випускають спеціалізовані GSM модеми (M2M-рішення) для побудови на їх основі безпровідних систем безпеки. Це рішення істотно підвищило надійність роботи системи, а також надало розробникам систем безпеки додаткові можливості по роботі з сервісами GSM. В якості способу передання інформації в GSM системах використовуються SMS повідомлення, модемне з’єднання (CSD), передача тонових посилок (режим DTMF) і режим пакетної передачі повідомлень GPRS. Поява режиму GPRS дозволила істотно знити витрати на експлуатацію систем радіо-охорони. На сьогодні безпровідні охоронні системи на базі GSM отримали широке поширення завдяки їх відносно невисокій вартості і простоті установки і експлуатації.

Проте істотним недоліком подібних систем є низька завадо-захищеність, а також робота GSM мережі не завжди є стабільною. Вказані недоліки обмежують застосування устаткування подібного класу при побудові систем безпеки. Ці системи більшою мірою застосовуються в якості резервних (додаткових) каналів зв'язку або для побудови систем моніторингу віддалених об'єктів для збору телеметричної інформації. Схема передачі інформації в GSM охоронній системі при використанні функції SMS зображена на рисунку. 1.1.

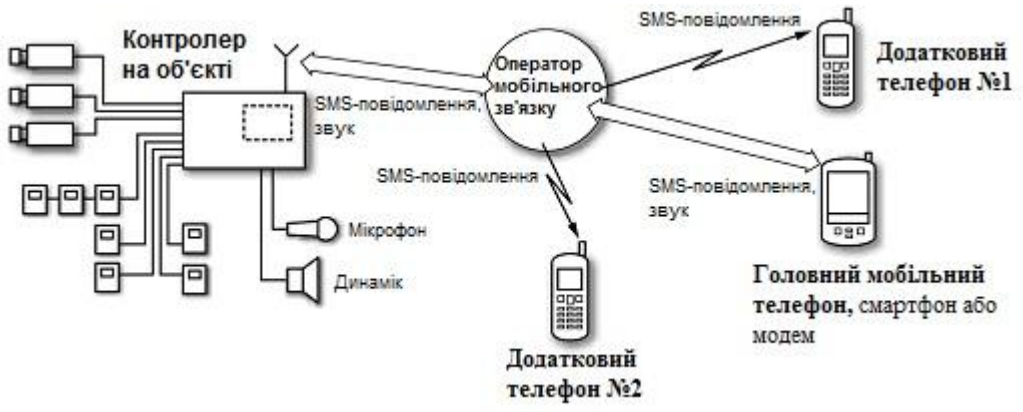

Рисунок 1.1 - Схема передачі інформації в GSM

GSM охоронна система може включати один або декілька GSM контролерів серії TSS-705, а також засоби контролю і управління цими GSM контролерами - стільникові телефони або комп'ютери.

GSM контролери встановлюються на віддалених об'єктах. До кожного з них можна підключати:

- різні дискретні і резистивні датчики (наприклад, контактні датчики, геркони, терморезистори для контролю температури, датчики охоронної і пожежної сигналізації);

- відеокамери (до 3 кольорових або чорно-білих відеокамер PAL або NTSC на один контролер);

- мікрофон і звуковий динамік;

- виконавчі пристрої (контролер має три реле для управління цими пристроями);

- кнопки для установки датчиків на охорону безпосередньо на об’єкті;

- кнопки та зчитувач коду різних ідентифікаторів (карт, брелоків) для зняття датчиків з охорони.

Приклади РСПС: «LONTA-202», «Струна-5».

До радіо-канальних систем малого радіусу дії відносяться безпровідні системи, працюючі в частотному діапазоні (433 МГц і 2,4 ГГц) з малою вихідною потужністю (10 мВт і 100 мВт відповідно).

В основному ці системи застосовуються для організації локального безпровідного зв’язку на території великих об’єктів. Радіус дії таких систем складає зазвичай від декількох сотень метрів до декількох кілометрів, залежно від умов поширення радіосигналу. При цьому пункт централізованого спостереження (ПЦС) зазвичай розташовується на цьому ж об’єкті, або організовується спеціальний виділений канал зв’язку для передачі інформації на віддалений ПЦС. Нині ці системи отримали широке поширення завдяки їх відносно низькій вартості і простоті монтажу. На сьогодні найбільш популярні приймачі стандарту 2,4 ГГц, такі як ZigBee, NanoNet та інші. Ці передавачі випускаються в однокристальному виконанні з підтримкою стека високорівневих протоколів, що спрощує розробку систем безпровідного зв’язку на їх основі і дає розробникам широкі можливості по реалізації алгоритмів обміну даними. Недоліком цих систем є їх низька завадо-захищеність і малий радіус дії.

До радіо-канальних систем великого радіусу дії відносяться системи, що мають виділений радіоканал, які забезпечують радіус 20-100 км в умовах міської забудови. До складу цих систем входять: абонентське устаткування, ретранслятори (базові станції) і пульт централізованого спостереження. У своїй більшості системи цього класу використовують частотний діапазон 146-174 МГц і вихідну потужність 1-10 Вт.

З точки зору організації радіо-інтерфейсу системи можна розбити на дві групи:

- системи, що використовують стандартні УКХ радіо-інтерфейси (такі системи, як правило, використовують частотну маніпуляцію і ширину каналу 12,5 або 25 кГц; недоліком таких систем є низька пропускна спроможність і невисока завадо-захищеність, оскільки сигнал із смугою 12,5 кГц легко подавити);

- системи, що використовують спеціалізовані радіо-інтерфейси (адаптовані під рішення завдань радіо-охорони і забезпечують захист інформації та високу завадо-захищеність каналу зв'язку; прикладом такої системи є радіо-канальна система АРКАН, що використовує для передачі вузько-смугові сигнали і алгоритм «стрибаючих частот», перебудова частоти відбувається за випадковим законом в широкій смузі (300-500 кГц), що забезпечує високу завадо-захищеність і високу місткість системи; до недоліків можна віднести високу вартість інсталяції мережі, проте при великій кількості абонентів ці витрати окупаються; системи широко застосовуються в середніх і великих містах на ПЦС з абонентською базою понад 2000-3000).

Супутникові системи використовують як канали зв'язку супутниковий зв'язок («Globalstar», «Inmarsat», «Thuraya»). Подібні системи використовують для контролю або охорони віддалених об'єктів у місцях, де відсутній мобільний і дротяний зв'язок. Головним недоліком цих систем є висока вартість абонентського устаткування та великі витрати на експлуатацію. З іншого боку, для вирішення завдань охорони віддалених поодиноких об'єктів ці системи не мають іншої альтернативи. З точки зору питань сполучення ОПС і канало-утворюючого устаткування існує три рішення: ОПС зі вбудованим радіо-канальним устаткуванням. Це рішення просте і недороге, в одному корпусі ви отримуєте і охоронну панель з джерелом безперебійного живлення, і радіоканал. Недоліком цього рішення є невелика кількість зон, що охороняються, як що їх не більше 4-8. Але для невеликих об'єктів це цілком добре і дуже вигідне економічне рішення.

ОПС із зовнішнім радіо-канальним устаткуванням, що підключається через спеціалізований інтерфейс. Системи цього типу зазвичай пропонують виробники, що мають широку лінійку систем ОПС і різні типи канало-утворюючого устаткування. Тому користувач може залежно від конкретного завдання визначити для себе склад проектованої системи ОПС і зібрати її з необхідних компонентів. Як правило, ці системи використовують шинні інтерфейси зв'язку між вузлами (наприклад, RS-485). Перевага цього підходу полягає в гнучкості проектування ОПС. Залежно від завдання ви можете вибирати контрольну панель з необхідною кількістю охоронних зон, використати радіоканал або дротяний зв'язок, при цьому все обладнання буде уніфіковано, мати єдину логіку роботи і єдині протоколи обміни. Недоліком цього рішення є те, що ви не зможете використати обладнання різних виробників, а це не завжди зручно, наприклад, у випадку якщо ви збираєтеся використати системи ОПС одного виробника і радіоканал іншого.

ОПС із зовнішнім радіо-канальним устаткуванням, що підключається через стандартний інтерфейс. Цей підхід вирішує проблему, описану вище. Використовуючи стандартний інтерфейс, можна використати устаткування різних виробників. Проте на сьогодні виробники устаткування не прагнуть розробити єдиний стандарт, а навпаки використовують свої закриті протоколи. Єдиним відкритим стандартом сьогодні є інтерфейс Contact ID, розроблений компанією ADEMCO і призначений для передачі повідомлень по телефонним лініям в режимі тонових посилок DTMF. Більшість контрольних панелей мають цей інтерфейс. Тому єдиним рішенням для виробників канало-утворюючого обладнання для охоронних систем було реалізувати всередині своїх пристроїв декодер Contact ID. Ці рішення сьогодні широко застосовуються і в GSM модемах, і радіо-канальних системах. Користувач може вибирати, який канал зв'язку використати: дротяний або безпровідний, при цьому обладнання ОПС перемонтовувати і перенастроювати не треба, просто вихід Contact ID підключається або до телефонної лінії, або на вхід радіопередавача.

Однією з безпровідних технологій, що швидко розвиваються є ZigBee, який спочатку розроблявся як низько-швидкісний канал зв'язку для об'єднання в мережу різних датчиків. Стосовно безпеки це можуть бути датчики охоронної і пожежної сигналізації.

Можливо незабаром ZigBee потіснить багато з існуючих сьогодні радіо-канальних ОПС. Адже майже усі вони розроблені поза якими-небудь стандартами. У кожного виробника свої протоколи обміну, і замінити наявні на об'єкті безпровідні датчики на устаткування іншого виробника неможливо. Якщо стандарт ZigBee отримає поширення, то замовник отримає можливість використати в системах ОПС практично будь-які датчики на вибір. Тим паче, що стандартні профілі (специфікації наборів команд і протоколів обміну) для конкретних додатків у області автоматизації будівель і систем безпеки розроблені та опубліковані, і все це гарантує сумісність устаткування різних виробників.

Цей стандарт хороший для з'єднання центрального вузла з периферією, яка розміщується територіально розподілено, причому за рахунок включення в систему ретрансляторів територія покриття може бути дуже великою. Теоретично можна використати ZigBee і в системах контролю та управління доступом. Але цей канал має невелику швидкість передачі даних і невелику дальність. Погодьтеся, нераціонально будувати довгий ланцюжок ретрансляторів заради з'єднання контролера з комп'ютером. Є багато простіших, а головне, дешевших і надійніших способів.

Можна сказати, що усі перераховані технології на сьогодні активно розвиваються і широко застосовуються для вирішення завдань охорони стаціонарних об'єктів. Вибір тієї або іншої безпровідної системи визначається залежно від типу об'єктів, їх кількості, вимог до надійності доставки повідомлень і віддаленості об'єктів. В деяких випадках для підвищення надійності використовується резервування каналів зв'язку. Можна сказати, що майбутнє за безпровідними технологіями і скоро вони повністю витіснять з ринку дротяні охоронні системи.

1.2 Використання бездротових каналів у системах охорони

Системи відео-нагляду.

Першими в цій області з’явилися електронні пристрої, здатні віддавати лише текстові SMS-повідомлення з об’єкту, який знаходиться під охороною. Такий пристрій складався з електричного блоку, до якого можна було підключити 1-4 зовнішні датчики або шлейф охоронної сигналізації та звичайного мобільного телефону. Пристрій можна було встановити на всякому об’єкті, що має стійкий прийом GSM мережі. Принцип роботи пристрою заснований на сповіщенні користувача за допомогою текстового SMS-повідомлення, яке передавалося на мобільний телефон користувача через GSM-канал, у разі спрацьовування охоронного датчика або порушення цілісності шлейфу охоронної сигналізації. Подібні пристрої швидко завоювали популярність серед хазяїв, невеликих заміських будинків і котеджів невисокою ціною, простотою установки. В якості реакції у відповідь власник подібного пристрою при отриманні SMS-повідомлення, телефонував на мобільний телефон сусіда або місцевого сторожа, той у свою чергу, йшов до будинку та з’ясовував причини спрацьовування. При цьому схожі пристрої мали істотні недоліки: не дозволено було відрізнити хибне спрацьовування від справжнього без участі людини, а при надзвичайній ситуації, нерідко не дозволено було цьому запобігти. При цьому, при сильному завантаженні стільникової мережі SMS-повідомлення могло бути доставлене із запізненням від декількох хвилин до декількох годин, що робило цю систему непотрібною. Сучасні системи відео-спостереження по GSM як правило виконують наступні функції:

- взаємодія користувача з пристроєм для отримання відео-зображення може проводитися в будь-який час;

- передача відео-зображення від 1-4 телекамер в реальному часі;

- автоматичний додзвін до користувача після спрацьовування вбудованого детектора руху або зовнішнього датчика;

- автоматичний запис фото і відеоінформації до вбудованої пам’яті пристрою;

- запис фото і відеоінформації, що приймається на жорсткий диск комп’ютера;

- підключення зовнішнього охоронного датчика або шлейфу до реагуючого входу пристрою;

- підключення виконавчого пристрою до релейного виходу пристрою, і його пряме управління по каналу зв’язку.

Застосування систем віддаленого відео-спостереження по GSM ймовірно на віддалених об’єктах, де відсутні дротяні канали зв’язку: заміські будинки, дачі, склади, автостоянки, гаражі, автозаправні станції, залізничні переїзди. Для віддаленого відео-контролю за комунікаціями: водопроводи, газопроводи, нафтопроводи, електростанції, окремо розташовані підстанції, вишки і тому подібне. Незважаючи на уявну складність облаштувань відео-спостереження по GSM, вони залишаються прості в підключенні і комфортні в експлуатації. Не потрібно використання на передаючій стороні мобільного телефону, GSM-модуль вбудований прямо в центр приладу. Електроживлення здійснюється від джерела постійного струму з широким діапазоном напруги 8-15В або від електромережі 220В.

Альтернативою GSM-каналу є безпровідні мережі WLAN (Wireless Local Area Network). Мережа WLAN - це вид локальної обчислювальної мережі LAN, що використовує для зв’язку і передачі даних між вузлами високочастотні радіохвилі, а не кабельні з’єднання.

Призначені для користувача пристрої можна інтегрувати в мережу, встановивши на них безпровідні мережеві адаптери. Для забезпечення безпровідним користувачам доступу до вже існуючої мережі Ethernet треба встановити безпровідну точку доступу. Найбільш важливим елементом безпровідних мереж є безпровідна точка доступу(англ. Wireless Access Point).

Точки доступу потрібні, щоб виконувати найрізноманітніші функції, такі як для підключення групи комп’ютерів (кожен з безпровідним мережевим

адаптером) в самостійні мережі та для виконання функції моста між безпровідними і кабельними ділянками мережі. Такі поєднані мережі називаються інфраструктурою і використовуються для доступу до центральних баз даних або безпровідного підключення мобільних користувачів. Схема побудови відео-системи за допомогою WI-FI представлена на рисунку 1.2.

Рисунок 1.2 – Схема побудови відео-системи за допомогою WI-FI

Стандарт Wi-Fi (англ. Wireless Fidelity –«безпровідна точність», по аналогії з Hi-Fi - стандарт на устаткування Wireless LAN). При використанні сучасних потокових алгоритмів стиснення швидкості 0,5 Мбіт/с, цього цілком достатньо для передачі одного каналу відео нормальної якості. Також цю відстань можна збільшувати за допомогою спрямованих антен і проміжних точок доступу.

Захист відеоінформації у безпровідних IP- системах відео-спостереження досягається декількома способами. Ключовими серед них є: застосування брандмауерів, використання паролів і шифрування. Брандмауер працює як електронні «ворота», що пропускають зареєстрованих користувачів і забороняють доступ неавторизованим особам. Застосування паролів дозволяє не лише обмежити доступ до системи відео-спостереження, але і розподілити

права доступу персоналу до певних відеокамер. А при шифруванні спроби перехоплення зашифрованих даних в IP- системі охоронного відео-спостереження стають безглуздими, якщо зловмисник не знає унікального коду для розшифровки потоку даних. Цей код встановлюється системним адміністратором.

GPS моніторинг транспорту.

Супутниковий моніторинг транспорту - це система супутникового моніторингу і управління рухливими об’єктами, побудована на основі використання сучасних систем супутникової навігації (GPS/ГЛОНАСС), обладнання і технологій зв’язку (GSM/УКХ), обчислювальної техніки і цифрових карт. GPS моніторинг транспорту - це технологія, яка застосовується в диспетчерських службах, на транспорті, для вирішення завдань транспортної логістики, в системах управління перевезеннями і автоматизованих системах управління автопарком(для контролю фактичних маршрутів транспортних засобів за допомогою системи).

Автотрекер - це прилад, що встановлюється на автомобіль з метою відстеження його подальшого переміщення і контролю його місця розташування. За звичай автотрекер визначає своє місце розташування приймаючи сигнали GPS і відправляючи їх по каналу GPRS на сервер в інтернеті, на якому власник приладу спостерігає його переміщення. Майже усі сучасні прилади, працюючі на цьому принципі, можуть отримати вхідні дзвінки.

Для вирішення завдань моніторингу використовуються наступні компоненти системи :

- супутникові системи навігації (GPS - США, ГЛОНАСС - РФ);

- приймачі GPS та ГЛОНАСС;

- системи зв’язку з центральним пунктом (космічна /GSM / УКХ) та система локального накопичення даних.

Іноді додатково використовуються додаткові датчики, встановлені на самому технічному засобі : поточний запас палива, факт відкривання дверей

або капота, факт наявності пасажира (у таксі), температура в рефрижераторі, факт роботи або простою спеціальних механізмів (поворот стріли крану, робота бетонозмішувача), факт натиснення тривожної кнопки. Отримані дані можуть або накопичуватися в локальному пристрої і потім переноситися в центральну базу після повернення в парк, або передаватися на центральний сервер в режимі реального часу.

Системи GPS моніторингу транспорту вирішують наступні завдання:

- відстеження поточних координат, напряму та швидкості руху транспортного засобу в реальному часі для потреб диспетчерських служб (у деяких системах також можлива установка додаткових датчиків на відкриття дверей, включення або виключення виконавчих механізмів спеціальної техніки, паливних датчиків, датчиків для виміру температури в рефрижераторі; деякі системи допускають підключення до бортового комп'ютера автомобіля (через CAN-шину) і віддалене зчитування параметрів експлуатації транспортного засобу);

- облік пройденого кілометражу і витрат палива потрібний для своєчасного проходу техогляду та контролю витрат паливно-мастильних матеріалів бухгалтерією (у системах TMS за допомогою GPS робиться автоматичний облік доставки вантажів в задані точки);

- контроль відповідності фактичного маршруту автомобіля плановому дозволяє підвищити дисципліну водіїв (у нашій країні, на відміну від розвинених країн, ця функція потрібна для припинення несанкціонованого використання службових транспортних засобів найманими водіями в цілях особистого збагачення, а також для припинення несанкціонованого зливу палива; за оцінками журналу «Логістика», тільки за рахунок підвищення дисципліни водіїв, за допомогою таких засобів, системи GSM моніторингу окупаються за декілька місяців);

- безпека (знання координат дозволяє швидко знайти викрадений транспортний засіб; додатково автомобілі можуть обладнатися прихованою кнопкою, натиснення або не натиснення на яку посилає сигнал тривоги у

диспетчерський центр; окрім цього, деякі термінали GPS моніторингу можуть працювати в режимі GSM-сигналізації, тобто дзвонити на заданий телефонний номер у разі спрацьовування штатної сигналізації).

Типова система GPS моніторингу складається з трьох ланок: терміналів, що встановлюються на автомобілі, сервера і клієнтських робочих місць. Термінали являють собою спеціалізовані GPS-трекери, що містять модуль GPS і модуль стільникового зв'язку (GSM або CDMA). Функції сервера може виконувати звичайний ПК із встановленим серверним ПЗ. На відміну від робочих місць, сервер має бути завжди включений, оскільки саме на ньому накопичуються дані про маршрути. Клієнтське ПЗ в окремих випадках може бути об'єднано в одну програму з серверною частиною, але як правило допускається одночасне підключення декількох робітників місць до одного сервера.

Залежно від технічних рішень, які застосовують, можна виділити п'ять поколінь систем GPS моніторингу транспорту :

- перші системи були оффлайновими, тобто не дозволяли здійснювати моніторинг в реальному часі (GPS-трекер записував усі дані в пам'ять і передавав їх на сервер після прибуття транспортного засобу на базу за допомогою дротяного або безпровідного інтерфейсу, така схема дозволяла контролювати маршрут автомобіля тільки після завершення поїздки і не здатна допомогти при викраденні автомобіля);

- у другому поколінні для організації зв'язку між GPS-терміналами та сервером використовувалися SMS або механізм CSD (на сервер встановлювалися один або декілька модулів стільникового зв'язку, що дозволяють приймати SMS або дзвінки з даними; подібні системи відрізнялися величезними платежами за мобільний зв'язок і дуже великим періодом часу між вимірами координат, з масовим поширенням мобільного інтернету системи другого покоління практично вимерли);

- у третьому поколінні, як транспортна мережа використовуються GPRS або EV-DO, що дозволяє на порядок знизити витрати на мобільний зв'язок і

різко поліпшити точність прокладення маршрутів (сервер в таких системах встановлюється безпосередньо у клієнта і підключається до інтернету і до локальної мережі офісу, на сервер і на робочі місця користувачів встановлюється спеціалізоване програмне забезпечення; у деяких системах допускається оренда портів сервера, що надається постачальником; на даний момент це найпоширеніша схема моніторингу);

- системи четвертого покоління також використовують один з механізмів мобільного інтернету в якості транспортної системи, але відрізняються від третього використанням веб-технологій (у цьому випадку сервер розміщується у компанії постачальника, його потужності діляться між багатьма клієнтами, а захищений доступ до даних здійснюється через веб-сторінку з будь-якого комп'ютера, підключеного до інтернету; оскільки один сервер здатний працювати одночасно з тисячами трекерів, різко знижується вартість впровадження і обслуговування системи, одночасно з цим зростає надійність зберігання даних, оскільки компанії-оператори здатні виконувати багаторазово-резервоване якісне серверне устаткування і штат технічних фахівців для його цілодобового обслуговування; потенційним недоліком систем четвертого покоління є повна централізація, отже вірогідність збою або настання форс-мажорних обставин в таких системах украй низька, зате наслідки збою можуть стати дуже дорогими для компанії-оператора);

- системи моніторингу п'ятого покоління представляють з себе глобальний розвиток і централізацію систем попереднього покоління в єдиний, розподілений центр моніторингу (у такому варіанті дані від пристроїв збираються одним або декількома комунікаційними серверами, стікаються на один основний сервер бази даних і розтікаються між підключеними проміжними серверами, які вже забезпечують взаємодію з користувачем (веб-моніторинг) або виконують фонові завдання; при такій побудові системи користувачі з різних районів, країн і навіть континентів працюють з найближче розташованим регіональним веб-сервером з мінімальною затримкою.

На даний момент на ринку представлені багато різних систем GPS моніторингу, як імпортних, так і вітчизняних. Імпортні рішення, як правило, відрізняються розширеною функціональністю, зате у вітчизняних краще реалізовані функції контролю за несанкціонованим використанням автомобіля, краще вирішено питання карт. Важливим у наших умовах чинником є також захист терміналів від протидії водіїв: наявність резервного акумулятора, пломбування пристроїв та інше.

В якості основного каналу зв'язку в професійних системах контролю і управління доступом можуть використовуватися тільки ті безпровідні технології, які еквівалентні по функціоналу, призначенню і вартості стандартній дротяній комп'ютерній мережі підприємства (Wi-Fi, Wi-Max і аналогічні безпровідні мережі).

Технології сенсорних мереж типу ZigBee, Z-Wawe і більшості аналогічних повинні використовуватися за своїм прямим призначенням: для отримання інформації від різних датчиків без прокладення дротів на обмеженій території. Така мережа як GSM, може використовуватися або в домашніх системах, або як додатковий канал віддаленого доступу до серверів системи контролю і управління доступом для отримання звітів і аналогічних дій.

1.3 Огляд існуючих систем безпеки, які використовують GSM канали

Існує багато систем безпеки, які використовують GSM канали, як вітчизняних, так і імпортних. Розглянемо декілька найпоширеніших з них.

1.3.1 Орлан GSM 900/1800 («Охорона і безпека», Україна)

«Орлан» - це комплекс технічних засобів і програмного забезпечення для створення пульту центрального стеження за станом пристроїв пожежної і охоронної сигналізації GSM з використанням стільникової мережі
GSM 900/1800 в голосовому режимі та режимі GPRS. Призначений для прийому кодованих повідомлень, що передаються радіокомунікаторами серії «Лунь», і трансляції їх на ПК для реєстрації і обробки за допомогою програмного забезпечення «Фенікс 2». Програмне забезпечення підтримує

підключення до ПК цифрових приймачів ПАКТ2 і DSC-SurGard, для прийому кодованих повідомлень по телефонній лінії від більшості охоронно-пожежних панелей (Napco, Ademco, DSC і подібних). Пульт центрального стеження «Орлан» забезпечує прийом повідомлень від зовнішніх пристроїв із звуковим і візуальним супроводом, розшифровкою і обробкою, стеження і миттєва зміна стану об'єкту на ньому при прийомі чергового повідомлення. Передбачені до п'яти функцій віддаленого управління об'єктовими приладами операторами пульта, а також зберігання і відображення інформації в текстовому і графічному виді.

Пульт центрального стеження веде архіви прийнятих повідомлень, пошук в архіві за різними критеріями, друк і експорт бази даних, архіву подій. Є можливість розбиття об'єкту на групи і відстеження інформації окремо по кожній групі, можливість задавати розклад роботи для кожної з груп. Резервне копіювання та архівація бази даних відбувається автоматично. Всі події з об'єкту дублюються на мобільний телефон господаря у вигляді SMS (до 3 телефонів), на видалений пульт «Фенікс-міні» у вигляді SMS (до 3 пультів), а також по каналу GPRS. Є можливість переключення об'єкту, групи або окремого шлейфу в режим постійного або тимчасового стенду. Проводиться аналіз та побудова графіків і звітів про роботу пульта за місяць. Інформативність (види сповіщень) - 256. Розмір буфера пам'яті прийнятих подій - 32. Час готовності пульта центрального стеження до роботи - не більше 40 секунд. Час одного сеансу зв'язку в голосовому режимі - не більше 4 секунд. Час одного сеансу зв'язку у в режимі GPRS - не більше 1 секунди. Централізована база даних у форматі Microsoft SQL Server 2000 з клієнт-серверною архітектурою ПЗ, розподілений доступ до БД з різних ПК в мережі. Протоколювання часу прибуття групи реагування на об'єкт. Індивідуальний інтервал тестування для кожного охоронного приладу від 15 хв.

1.3.2 Станція моніторингу STAM-2 (Satel, Польща)

Станція моніторингу STAM-2 польської компанії Satel складається з: програмного забезпечення, основної плати для прийому повідомлень від командного пункту та захисного апаратного USB-ключа. При цьому основну плату можна встановити у будь-який вільний PCI-слот ПК, а з автономним джерелом живлення можлива робота станції без комп'ютера. Програма моніторингу істотно полегшує роботу оператора системи ОПС, автоматично вибираючи події, що вимагають його втручання, надаючи список інструкцій у кожній конкретній ситуації і нагадуючи про невиконані завдання. STAM-2 може обслуговувати більше 50 000 абонентів, виводити на друк звіти про дії операторів системи ОПС, звіти про системні події і автоматично відстежувати несанкціоновану зміну системних файлів.

Пульт центрального стеження STAM-2 підтримує наступні способи обміну даними з командним пунктом: прийом сигналів по телефонній лінії, по IP-каналу, по мережі GSM у вигляді SMS-повідомлень та по радіоканалу за наявності радіостанції стандарту VISONIC. При цьому підбір плат, що встановлюються на ПК, залежить від вибраних способів передачі даних.
У рамках однієї станції моніторингу STAM-2 може працювати до 16 сполучених між собою плат, що дозволяє регулювати кількість доступних телефонних ліній і IP-адрес.

Система має модульний принцип побудови. Один модуль «АРМ оператора пульта центрального стеження» дозволяє підключити до 540 об'єктів. Можна організувати роботу декількох модулів «АРМ операторів пульта центрального стеження». Як комунікатор використовуються універсальний GSM ГТС та IP- модем. По каналу GSM інформація передається в цифровому форматі DATA.

SMS-повідомлення власника об'єкту про доставку сповіщення на пульт центрального стеження і на стільниковий телефон власника відбувається альтернативним каналом передачі сповіщень (розмиканням контактів реле пульта). Цей пульт є автоматизованим робочим місцем на основі

персонального комп’ютера з підключеними до нього концентраторами і встановленим програмним забезпеченням інтегрованої системи безпеки «Лавина». Він дозволяє вирішувати комплекс завдань по моніторингу системи, підготовці і веденню бази даних по об’єктах, програмуванні ключів перенесення даних для об’єктових приладів. Також можливе виконання адаптивної конфігурації та налаштування системи, програмування об’єктових приладів, отримання довідкової та звітної інформації.

Програмне забезпечення складається з декількох модулів, які забезпечують прийом і декодування інформації, відображення стану усіх об’єктів, підключених до системи, видачу сповіщень про тривогу, фіксацію дій операторів при вступі повідомлень, детальне представлення кожного об’єкту, відображення журналу подій, контроль працездатності модулів для зв’язку з концентратором.

1.3.3 Програмована безпровідна сигналізація ABAX

Система ABAX включає безпровідні контролери, охоронні датчики, оповісники і інші облаштування ОПС фірми Satel, на базі яких будується система безпровідної сигналізації офісу, магазину або квартири. Ця система дозволяє розширити безпровідними пристроями будь-яку дротяну ОПС. Важливою особливістю ABAX є наявність двостороннього радіозв’язку між контролером і пристроєм з шифруванням даних, що забезпечує високу міру захисту системи ОПС від злому і саботажу.

ABAX швидко реагує на тривогу та передає сигнал на командний пункт системи. При цьому вона забезпечує роботу системи сигналізації в енергозберігаючому режимі та дозволяє дистанційно конфігурувати безпровідні пристрої за допомогою ПО. Працює ABAX в смузі частот 868,0.868,6 Гц з модуляцією FSK.

В якості базового пристрою сигналізації ABAX використовується контролер ACU-100 фірми Satel, який може обслуговувати одночасно до 48 охоронних пристроїв, і працює спільно з будь-якими приймально-контрольними приладами (ПКП). ABAX організовує двосторонній зв’язок

між безпровідними пристроями, тому прийом повідомлень від датчиків сигналізації завжди підтверджується. В той же час ACU-100 проводить в режимі онлайн, опитування безпровідних датчиків сигналізації, визначаючи присутність в системі кожного пристрою.

1.3.4 Радіосистема передачі сповіщень Дельта

РСПС «Дельта» призначена для забезпечення передачі, збору, обробки інформації з віддалених об’єктів, що охороняються та її зберігання на пультах централізованого спостереження в масштабах підприємств, районів, міст, областей. Забезпечується: пожежна та охоронна сигналізація, контроль доступу на об’єкти, що охороняються, автоматичний контроль стану обладнання, контроль стану та витоку хімічно небезпечних речовин, витоку води, газу і так далі. Сповіщення, що посилаються об’єктовими передавачами, поступають на пульти централізованого спостереження. Кожне прийняте сповіщення декодується і обробляється, після чого оператор може вжити необхідні заходи по залученню сил швидкого реагування. Передбачено дублювання по телефонних лініях і автоматичну відправку SMS-повідомлень.

Принцип роботи радіо-канальної системи передачі сповіщень «Дельта» побудований на використанні виділеного для цих цілей радіочастотного ресурсу для передачі сполучень з об’єктами, обладнаними радіопередавачами, на пульт централізованого спостереження, де відбувається прийом повідомлень, їх обробка та відображення на моніторі диспетчера, який передає отриману інформацію у відповідні служби реагування по спеціальному каналу зв’язку.

Використання виділеного каналу виключає залежність системи від інших операторів зв’язку, а його експлуатаційна готовність забезпечується державною радіочастотною службою. До об’єктового радіопередавача може бути підключена будь-яка периферія (охоронна, тривожна, пожежна сигналізація, датчики витоку води, газу і так далі). Конфігурація мережі дозволяє використати інформацію, необхідну для відповідного реагування

таким структурам, як підрозділу позавідомчої охорони МВС, відомча охорона, служба порятунку, пожежна охорона, приватні охоронні підприємства, міські комунальні служби, підприємства водопостачання, електромережі, тепломережі.

Основні характеристики:

- частотний діапазон 136-174 або 400-500 МГц;
- потужність передавачів до 15Вт;
- дальність без ретрансляції 15 км;
- до 30 ретрансляторів в системі;
- місткість системи 12000 об’єктів з використанням однієї частот.

Склад системи :

- пульти централізованого спостереження, що складаються з: антенно-фідерних пристроїв, базових станцій, ПК зі встановленим програмним забезпеченням автоматизованого робочого місця операторів, обладнання енергонезалежного живлення; для автоматичної відправки SMS-повідомлень використовуються спеціалізовані GSM радіо-модеми «Дельта – GSM»; дублювання по телефонній лінії забезпечує «Дельта-Т».
- об’єктове обладнання, що складається з передавачів з антенами, підключених безпосередньо до оповіщувачів або до будь-яких приймально-контрольних пунктів з обладнанням енергонезалежного живлення;
- для розширення зони радіо-охорони можуть використовуватися ретранслятори.

Основні відмінні особливості:

- велика дальність забезпечена високою потужністю передавачів - до 15 Вт і високою чутливістю приймального тракту - 0.25мкВ;
- велика місткість, забезпечена малою тривалістю відправки - 0.125 секунд;
- передавачі виконують функції об’єктових ПКП;
- застосування високошвидкісного формату FSK передачі даних з перевіркою контрольних сум повідомлень і алгоритм дублювання переданих

сполучень з рознесеними за часом посилками у випадковий часовий інтервал (5-8 секунд) надають системі високу надійність при високій місткості і інформативності (до 256 параметрів);

- інтервал тестових сигналів може бути встановлений від 1 хвилини до 256 годин, що дозволяє тестувати об’єкти з необхідним періодом залежно від місткості системи або залежно від категорії об’єкту;

- одночасний моніторинг стаціонарних і мобільних об’єктів;

- комплексне використання прямого радіоканалу, телефонних каналів і GSM;

- невисока вартість;

- можливість побудови системи від невеликого пульта з декількома об’єктами до мережі, що включає велику кількість центральних станцій і ретрансляторів, в масштабах великого міста або області.

«Дельта» використовують протоколи, подібні до системи "PIMA" (Ізраїль) і «Informer 12000» (США), що дозволило перейняти багаторічний досвід світових лідерів і при цьому мати усі переваги вітчизняного виробника.

Підсумовуючи вище сказане, можна зробити висновок по системам:

- у всіх системах використовується шифрування даних;

- всі системи підтримують передачу даних за допомогою SMS-повідомлень за допомогою мережі GSM;

- системи Орлан GSM 900/1800 та STAM-2 обидві можуть виводити звіт про дії операторів системи та звіти про системні події, але STAM-2 є надійнішим в плані охорони даних системи, бо автоматично відстежує несанкціоновану зміну системних файлів; в обох системах є можливість створення архіву бази даних, його ведення та моніторингу, також можливе отримання звіту за певний період часу;

- найбільшу кількість об’єктів може підключити система Дельта (12000), після неї STAM-2 (до 540), Орлан GSM 900/1800 (до 256) та ABAX (48);

- у Дельта системі передача повідомлень дублюється по телефонній лінії, а в STAM 2 – по IP лінії;

- система ABAX працює в смузі частот 868,0…868,6 Гц з модуляцією FSK, система Дельта має частотний діапазон 136-174 або 400-500 МГц;

- перевагою ABAX є двосторонній зв'язок, між безпровідними пристроями, тому прийом повідомлень від датчиків сигналізації завжди підтверджується;

- перевагою РСПС Дельта є використання виділеного каналу, що виключає залежність системи від інших операторів зв'язку, а його експлуатаційна готовність забезпечується державною радіочастотною службою.

1.4 Функції GSM каналів, які використовуються системами безпеки

SMS канал. Досить сильно поширений на ринку систем безпеки в нашій країні тип сигналізації, що використовує функцію SMS повідомлень. Така популярність обумовлюється низькою вартістю (як самої сигналізації так і абонентської плати) та простотою використання цих GSM-сигналізації. У професійних охоронних системах цей тип передачі сповіщень використовується в основному як сервісний канал. Сповіщення про надзвичайну ситуацію або про проникнення на об'єкт є обов'язковим атрибутом систем охорони та з точки зору технічної реалізації може бути виконане в такій формі як попередження голосом (дзвінком на телефон), DTMF (Dual Tone Multi Frequency) кодом, у будь-якому цифровому виді, а також передачею SMS повідомлення власнику.

Для передачі сповіщень засобом SMS повідомлень використовується найпопулярніший GSM сервіс мобільних операторів. І одночасно найпростіший у реалізації метод. GSM модеми з SMS-передавачем мають доступну ціну, у той же час прості в налаштуванні, а пультовим приймальним пристроєм може бути будь-який стільниковий телефон.

SMS (англ. Short Message Service – служба коротких повідомлень) – система, що дозволяє посилати і приймати повідомлення у вигляді тексту за допомогою мобільного телефону. Текст може складатися з алфавітно-

цифрових символів. Максимальний розмір повідомлення в стандарті GSM - 140 байт. Таким чином, при використанні 7-бітового кодування (латинський алфавіт і цифри) можна відправляти повідомлення завдовжки до 160 символів. При використанні 8-бітового кодування (німецька, французька мова) можна відправляти повідомлення завдовжки до 140 символів. Для підтримки інших національних алфавітів (китайського, арабського та ін.) використовується 2-бітове кодування UTF - 16 (Unicode). Таким чином, SMS-повідомлення, написане кирилицею, не може перевищувати 70 знаків. Що дуже обмежує використання цього сервісу в охоронному обладнанні.

У стандарті також передбачена можливість відправляти сегментовані повідомлення. У таких повідомленнях у заголовку, який призначений для користувача даних (UDH) поміщається інформація про номер сегменту повідомлення та загальну кількість сегментів. Цю можливість підтримують не усі GSM-модеми, а ті, які підтримують, частенько накладають обмеження на кількість сегментів в повідомленні (3 або 5). Модем, який не підтримує сегментацію, відображає кожен сегмент як окреме повідомлення. Як правило, кожен сегмент тарифікується як окреме повідомлення. Технологія SMS підтримується основними стільниковими мережами (GSM, NMT, D - AMPS, CDMA). Також SMS повідомлення на телефони можна відправляти за допомогою інтернету і інших мереж, використовуючи спеціальні програми, а також безпосередньо шлюзи мобільних операторів.

У своїй роботі GSM-сигналізації, які використовують SMS повідомлення для передачі повідомлень про тривогу, повністю ідентичні своїм аналогам, які використовують інші канали передачі даних. У цих сигналізаціях використовуються все ті ж GSM-модеми. На об’єкті встановлюється контрольна панель з GSM-модулем. Залежно від типу зв’язку з датчиками (дротяні і безпровідні охоронні датчики) підключаються охоронно-пожежні датчики. У разі спрацьовування одного з датчиків, на панель поступає сигнал. У свою чергу у разі замикання однієї із зон контролер дає команду

GSM-модему відправити SMS повідомлення на один або декілька телефонних номерів з пам’яті.

Широке поширення отримали так звані дачні охоронні сигналізації. Цей тип GSM-сигналізацій майже завжди поєднує в собі охоронні функції і функції дистанційного керування виконавчими пристроями. У професійній охороні цей тип зв’язку застосовується обмежено, в основному як сервісний канал, наприклад для підтвердження взяття об’єкту під охорону або контроль напруги мережі на об’єкті. Так само цей канал використовується як останній резервний канал в професійних охоронних системах.

Слабке місце цих охоронних систем усім добре відоме: SMS повідомлення можуть затримуватися в SMS-сервері на невизначений час, а іноді просто втрачаються. Так як цей канал зв’язку не є пріоритетним. У разі завантаженості GSM каналу SMS повідомлення відправляють в останню чергу (чого не скажеш про голосові виклики). Невизначеність часу доставки SMS повідомлень роблять цей метод неприпустимим для професійної охорони.

Таблиця 1. Підтримка способів передання сповіщень на ПЦС.

Методи передачі сповіщень на ПЦС	**Орлан**	**IPCOM**	**TELE monitor**	**Контакт**	**Андромеда**
Передача сповіщень на ПЦС					
CLIP	-	-	-	Система «Барс»	-
SMS	-	У розробці	V	V	-
Contact ID/GSM Voice/CDMA	GSM	-	-	GSM	GSM
GSM Data/CSD	-	-	-	V	-
TCP/IP GPRS	V	V	V	V	V
Радіоканал далекої дії	-	-	-	-	V
Передача рівня сигналу GSM на ПЦС		-*	V	-*	-*
Контроль балансу абонента		-	-	-	-
Дистанційне програмування	V	У розробці	V*****	CSD	V
FIRMWARE		V			
Підтримка двох SIM	У розробці		V**	V	-
Шифрування каналу TCP/IP GPRS	-	SSL128bit	SSL128bit	-	128/192/256bit AES

* - рівень на приладі; ** - визначає модель терміналу; ***** - у межах, які задаються при першочерговому програмуванні.

Voice (мовний) канал. Умовно ділитися на DTMF сигнал і мовне сповіщення. Цей канал дуже популярний серед пультових охоронних систем. У цього каналу GSM мережі є свої плюси і мінуси. З плюсів можна виділити простоту переходу з дротяної охоронно-пожежної сигналізації на GSM-

сигналізацію. Мінуси це забивання каналу у разі несправності або поганого сигналу. Мовний канал є найпоширенішим каналом передачі даних в охоронних системах,які використовують GSM технології передачі даних. Voice канал - це голосовий тракт, що використовує мовне сповіщення (зазвичай в приватних охоронних системах) і DTMF- код (обладнання для пультів централізованого спостереження). При мовному сповіщенні у разі тривоги GSM-сигналізація дзвонить на телефон і промовляє заздалегідь записане повідомлення. З DTMF трохи складніше, при натисненні на клавішу телефону лунає звук, який є комбінацією двох тонів, високочастотного та низькочастотного. Система сигналів DTMF включає вісім тонів, які були спеціально підібрані так, щоб передаватися через телефонну мережу без загасання і з мінімальною дією один на одного. Оскільки ці звукові сигнали потрапляють в частотний діапазон людського голосу, були додатково введені заходи для того, щоб голос не сприймався як набір. Один з таких заходів - ділення тонів на дві групи, високочастотну та низькочастотну.

Зазвичай в GSM-сигналізаціях для пультів централізованого спостереження (ПЦС) використовуються стандартні формати, наприклад протокол Contact ID. На даний момент DTMF є найпоширенішим каналом передачі даних, оскільки формати даних, принцип передачі, приймальне обладнання - повністю за позичено у дротяного моніторингу. Наприклад, якщо охоронне підприємство вже має станцію централізованого моніторингу, то застосування GSM-сигналізацій не викликає зайвих витрат, тому не вимагається замінювати устаткування на станції моніторингу.

Таблиця 2. Можливості, які представляються різними системами охорони.

Повідомлення /керування користувачем	**Орлан**	**IPCOM**	**TELE monitor**	**Контакт**	**Андромеда**
Передаючий модуль	-	IPCOM	Siemens TC65/75	GSM5	Hunter+GSM 200
SMS-повідомлення	з ПЦС	-	з ПЦС	V	AI-47 (з ПЦС)
Вид повідомлення	Трансліт	-	Трансліт	Кирилиця	Латиниця /Кирилиця
Деталізація	-	-	Contact ID	Contact ID	10парам.(4*)
Мовні повідомлення	-	-	-	V	V(9*)
Деталізація/ тривалість	-	-	-	Contact ID	20 с(9*)
Прослуховування	-	-	-	-	V
Керування:	V	-	V	V	V
приладом SMS/GSM Voice/ Internet	з ПЦС	У розробці	GPRS***	Voice/ DTMF	Voice/ DTMF
виходами SMS/GSM Voice/ Internet	DTMF	-	GPRS***	Voice/ DTMF	DTMF
(4*) – можна налаштувати час приходу події, назву, номер та адресу об’єкта (9*) – при наявності мовного модуля *** - з ПК через інтернет або за допомогою мобільного телефону JAVA 2ME					

Використання DTMF форматів пред’являє додаткові вимоги до опрацювання звукового тракту GSM-модему. Аналого-цифрові перетворення спричиняють спотворення при передачі сигналу. Через це можуть відбуватися збої при прийомі звітів від об’єктового обладнання. Ця проблема досить часто зустрічається у вітчизняного обладнання. І хоча сигнал не

загубиться в мережі (більшість систем контролюють передачу даних, запрошуючи підтвердження прийому), але значно збільшиться час проходження сигналу. Причому збільшення часу проходження сигналу може бути фатальним. Уявіть собі ситуацію, коли на об’єкт встановлено устаткування, що використовує передачу даних у форматі DTMF кодів. Через несправність устаткування або погану якість сигналу об’єктовий прилад не зможе передати повідомлення на пульт. І, як наслідок, не отримає підтвердження про прийом. Не отримавши повідомлення про прийом прилад почне повторний набір із спробою передати повідомлення. Але у результаті, не отримавши нічого, починається цикл додзвону. Цей цикл повністю займає весь канал, що не дозволяє передати повідомлення інших об’єктових приладів, тобто буде втрачений зв’язок з об’єктами. Не буде повідомлень про тривогу, не буде сполучень про постановку та зняття з охорони і так далі. І як наслідок неробочий ПЦС.

GSM DATA/CSD (Circuit Switch Data). Цифровий канал передачі даних на швидкості 9,6 кбіт/с. Цей метод характеризується практично сто відсотковою вірогідністю доставки повідомлення. Час встановлення з’єднання близько 20 с. Тарифікація CSD щохвилинна, як і для голосового каналу GSM. На відміну від передачі повідомлення в стандартному форматі Contact ID, в голосовому каналі протокол передачі в CSD не стандартизований (хоча може бути максимально наближений до CID). Це не дозволяє використати передавачі одного виробника у системі іншого виробника (звичайно, якщо вони не домовилися і не зробили спеціальних заходів по сполученню своїх систем).

Можлива установка в «прозорому» (transparent) та «непрозорому» (non - transperent) режимах. Відмітною особливістю передачі даних з використанням «непрозорого» режиму є велика завадо-захищеність, що досягається за рахунок введення алгоритму корекції помилок, а також наявності підтвердження успішної (без спотворень) доставки передаючої інформації. Таким чином, використання «непрозорого» CSD- з’єднання представляється переважно при низькому співвідношенні сигнал/шум. Проте

тривалість часу встановлення з’єднання в «непрозорому» режимі більша, ніж в «прозорому». У режимі CSD також реалізована процедура підтвердження прийнятих сповіщень на ПЦС.

CLIP (Calling Line Identification Presentation). Цей метод заснований за допомогою сервісу оператора мобільного зв’язку, за поданням інформації про номер абонента, що здійснює дзвінок. Принцип систем, які використовують CLIP, дуже простий. Об’єктовий ППКОП у разі системної події здійснює дзвінок по мережі стільникового зв’язку на приймальний пристрій, у якості якого може виступати GSM-модем або звичайний мобільний телефон. Приймальний пристрій прочитує номер викликаючого абонента і відхиляє виклик. Сам факт дзвінка від відомого в системі абонента є основою для реєстрації тривожної події. Перевагою методу є те, що відсутня плата за вихідний виклик, адже ніякого з’єднання не відбувається. Проте інформативність такого повідомлення дуже мала.

Цей спосіб можна видозмінити для підвищення інформативності. Наприклад, встановити на ПЦС декілька GSM-модемів. Передавальний пристрій програмують так, щоб по одній групі подій модем робив виклик на перший модем (тривоги), по іншій групі - на другий і так далі. Слід зазначити, що цей спосіб не знайшов істотного поширення з-за малої інформативності.

TCP/IP GPRS (General Packet Radio Service). Як відомо, технологія пакетної передачі GPRS використовує як механізм доставки пакетів даних протоколи TCP/IP, у разі застосування яких кожному з приладів мережі привласнюється унікальна IP-адреса. Існує два види IP-адрес: статичні та динамічні. Статичні IP-адреси можуть надаватися інтернет провайдерами або операторами стільникових мереж. Динамічні IP-адреси видає оператор при під’єднанні до мережі GPRS тільки на час сеансу зв’язку. Якщо з яких-небудь причин сеанс перервався, то при повторному з’єднанні пристрій, що не має статичної IP-адреси, отримує новий динамічний, відмінний від попереднього. Необхідно згадати той факт, що якщо пристрій, у тому числі

модем GSM/GPRS, авторизувався у мережі і отримав динамічну IP-адресу, то для підтримки віртуального GPRS-каналу в активному стані треба через певні часові інтервали передавати сигнальні пакети на будь-яку відому IP-адресу, інакше оператор перерве з'єднання з мережею.

Можливі різні варіанти виділення IP-адрес ЦПО і концентраторами мереж лічильників. Варіант, що найчастіше зустрічається - наявність у ЦПО статичної IP-адреси, а у абонентів - динамічних. Причому статичну IP-адресу для ЦПО виділяє не стільниковий оператор, а інтернет провайдер при підключенні ЦПО до інтернету по виділеному каналу доступу (утвореному за допомогою технології ADSL або інших. При такій організації системи можливі два сценарії встановлення з'єднання між пристроями у цілях передачі даних. Якщо пристроєм, що ініціює з'єднання, є концентратор, він організовує GPRS-сеанс з інфраструктурою стільникового оператора, отримує від нього динамічну IP-адресу та встановлює TCP/IP-з'єднання з ЦПО (якщо знає його статичну IP-адресу). Останній (ЦПО) має бути налаштований на прийом та обробку запитів на з'єднання по виділеному каналу доступу в інтернет. При надходженні запиту на з'єднання від концентратора його динамічна IP-адреса стане відома ЦПО (в IP-заголовку пакету міститься інформація про адресу відправника, що робить можливим двосторонній обмін інформацією).

Якщо ж ініціатором зв'язку є ЦПО, то він додзвонюється до віддаленого модему по голосовому каналу GSM або посилає SMS-повідомлення на його номер. Концентратор сприймає вхідний дзвінок (чи SMS-повідомлення, що поступило) з відомого номера як команду на встановлення з'єднання з ЦПО і далі діє так, як було описано раніше. Мінімальною вимогою при організації з'єднання з ЦПО є знання концентратором статичної IP-адреси ЦПО. Якщо ж концентратор не знає цю адресу, то її можна повідомити концентратору по голосовому каналу GSM або за допомогою служби SMS. При необхідності організувати зв'язок з концентратором, що має статичну IP-адресу, ЦПО звертається до нього за цією адресою, встановлюючи GPRS-з'єднання. Для

цього модем GSM/GPRS концентратора має бути налаштований на прийом та обробку запитів на з’єднання по каналу TCP/IP. Такий спосіб організації каналу передачі даних можливий, проте на практиці майже не зустрічається з-за складності отримання статичних IP-адрес у стільникових операторів для всіх віддалених пристроїв системи.

Актуальний і такий варіант: концентратори і ЦПО мають динамічні IP-адреси. Це можливо, коли ЦПО не забезпечений віддаленим каналом доступу в інтернет, але розташований у зоні дії одного з операторів стільникового зв’язку. У цьому випадку вже не важливо хто є ініціатором зв’язку - концентратор або ЦПО, дії з реалізації каналу передачі даних завжди будуть одні і ті ж. Пристрій, який ініціює зв’язок, організовує GPRS-сеанс з інфраструктурою стільникового оператора та отримує від нього динамічну IP-адресу. Потім він повідомляє (наприклад, за допомогою служби SMS) отриману адресу іншому пристрою (концентратору) та надає йому команду з’єднатися за цією адресою. Пристрій, що викликається, організувавши GPRS-сеанс та отримавши динамічну IP-адресу, встановлює TCP/IP-з’єднання з тим, хто його викликає.

2 ПОБУДОВА СИСТЕМ БЕЗПЕКИ, ЯКІ ВИКОРИСТОВУЮТЬ GSM КАНАЛ

2.1 Побудова GSM каналу

Стандарт GSM був розроблений Європейським інститутом телекомунікаційних стандартів (ETSI) і визнаний найбільш надійним і масовим по використанню в засобах телекомунікації і зв'язку.

За приблизними підрахунками, число абонентів цього виду зв'язку в Євразії складає 100 млн.

Функціональна побудова і інтерфейси, прийняті в стандарті GSM, ілюструються структурною схемою (рисунок 2.1), на якій MSC (Mobile Switching Centre) - центр комутації рухливого зв'язку; BSS (Base Station System) – обладнання базової станції (БС); OMC (Operations and Maintenance Centre) - центр управління і обслуговування; MS (Mobile Stations) - рухливі станції (РС).

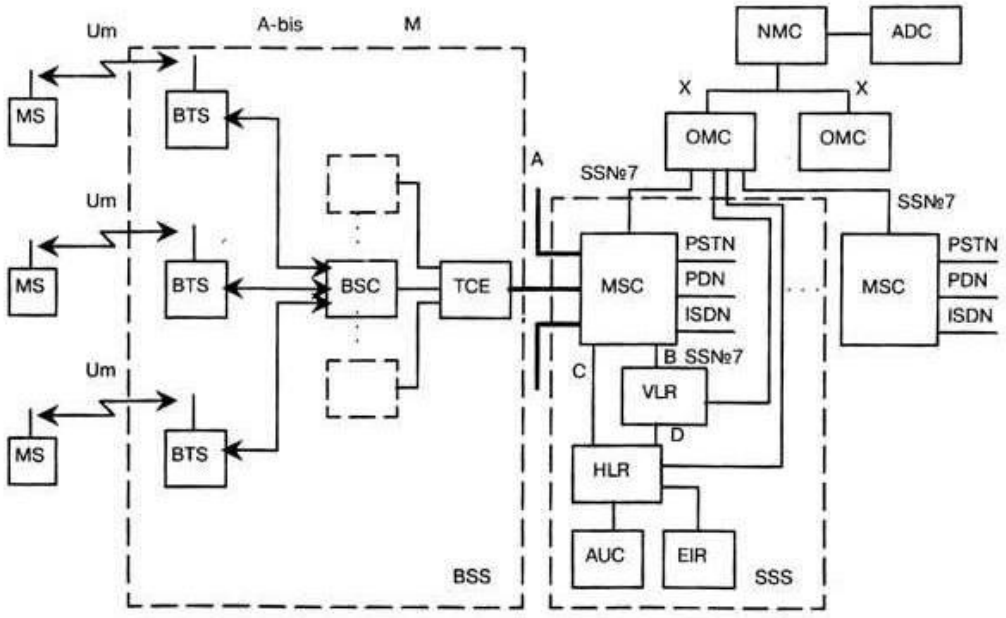

Рисунок 2.1 – Структурна схема

Функціональне сполучення елементів системи здійснюється рядом інтерфейсів. Всі мережеві функціональні компоненти в стандарті GSM

взаємодіють відповідно до системи сигналізації МСЕ-Т SS N7(CCITT SS. N7).

Центр комутації рухомого зв’язку обслуговує групу стільників і забезпечує всі види з’єднань, яких потребує в процесі роботи МС. MSC аналогічно комутаційній станції ISDN є інтерфейсом між фіксованими мережами (PSTN, PDN, ISDN) і мережею рухливого зв’язку. Він забезпечує маршрутизацію викликів та функцію управління викликами. Окрім виконання функцій звичайної комутаційної станції ISDN, на MSC покладаються функції комутації радіоканалів. До них відносяться «естафетна передача», в процесі якої досягається безперервність зв’язку при переміщенні рухливої станції із стільника в стільник, і перемикання робочих каналів в соті при появі поломок або перешкод.

Кожен MSC забезпечує обслуговування рухливих абонентів, розташованих в межах певної географічної зони (наприклад, Київ та область). MSC управляє процедурами встановлення виклику і маршрутизації. Для телефонної мережі загального користування (PSTN) MSC забезпечує функції сигналізації по протоколу SS N7, передачу виклику або інші види інтерфейсів відповідно до вимог конкретного проекту. MSC формує дані, необхідні для виписки рахунків за надані мережею послуги зв’язку, накопичує дані розмов, що відбулися, і передає їх в центр розрахунків (білінг-центр). Також MSC складає статистичні дані, необхідні для контролю роботи і оптимізації мережі та підтримує процедури безпеки, які вживають для управління доступами до радіоканалів.

Практично HLR є довідковою базою даних про постійно прописаних у мережі абонентів. У ній містяться розпізнавальні номери і адреси, а також параметри достовірності абонентів, склад послуг зв’язку, спеціальна інформація про маршрутизацію. Ведеться реєстрація даних про роумінг абонента, включаючи дані про тимчасовий ідентифікаційний номер рухливого абонента (TMSI) і відповідно VLR. До даних, що містяться в HLR, мають дистанційний доступ усі MSC і VLR мережі і, якщо в мережі є

декілька HLR, у базі даних міститься тільки один запис про абонента, тому кожен HLR є певною частиною загальної бази даних мережі про абонентів. Доступ до бази даних про абонентів здійснюється по номеру IMSI або MSISDN (номеру рухливого абонента в мережі ISDN). До бази даних можуть отримати доступ MSC або VLR, що відносяться до інших мереж, у рамках забезпечення між мережевого роумінгу абонентів.

VLR містить такі ж дані, як і HLR, проте ці дані містяться в VLR тільки до тих пір, поки абонент знаходиться в зоні, яка контролюється VLR. У мережі рухливого зв'язку GSM стільники групуються в географічні зони (LA), яким привласнюється свій ідентифікаційний номер (LAC). Кожен VLR містить дані про абонентів декількох LA. Коли рухливий абонент переміщається з однієї LA в іншу, дані про його місце розташування автоматично оновлюються в VLR. Якщо стара і нова LA знаходяться під управлінням різних VLR, то дані на старому VLR стираються після їх копіювання в новий VLR. Поточна адреса VLR абонента, що міститься в HLR, також оновлюється.

EIR є регістром ідентифікації обладнання, містить централізовану базу даних для підтвердження достовірності міжнародного ідентифікаційного номера обладнання рухливої станції (IMEI). Ця база даних відноситься виключно до устаткування рухливої станції. База даних EIR складається зі списків номерів IMEI, організованих таким чином : білий список містить номери IMEI, про які є відомості, що вони закріплені за санкціонованими рухливими станціями; чорний список містить номери IMEI рухливих станцій, які вкрадені або яким відмовлено в обслуговуванні з іншої причини; сірий список містить номери IMEI рухливих станцій, у яких існують проблеми, виявлені за даними програмного забезпечення, що не є основою для внесення в чорний список. До бази даних EIR мають дистанційний доступ MSC цієї мережі, а також MSC інших рухливих мереж.

OMC – центр експлуатації і технічного обслуговування, є центральним елементом мережі GSM, він забезпечує контроль і управління іншими

компонентами мережі та контроль якості її роботи. OMC з'єднується з іншими компонентами мережі GSM по каналах пакетної передачі протоколу X.25. OMC забезпечує функції обробки аварійних сигналів, призначених для сповіщення обслуговуючого персоналу та реєструє відомості про аварійні ситуації в інших компонентах мережі. Залежно від характеру несправності OMC дозволяє забезпечити її усунення автоматично або при активному втручанні персоналу. OMC може забезпечити перевірку стану устаткування мережі і проходження виклику рухливої станції. OMC дозволяє робити управління навантаженням в мережі. Функція ефективного управління включає збір статистичних даних про навантаження від компонентів мережі GSM, запис їх в дискові файли і виведення на дисплей для візуального аналізу. OMC забезпечує управління змінами програмного забезпечення і базами даних про конфігурацію елементів мережі. Завантаження програмного забезпечення в пам'ять може виконуватися з OMC в інші елементи мережі або з них в OMC.

NMC – центр управління мережею, дозволяє забезпечувати раціональне ієрархічне управління мережею GSM. Він забезпечує експлуатацію і технічне обслуговування на рівні всієї мережі, підтримуваної центрами OMC, які відповідають за управління регіональними мережами. NMC забезпечує управління графіком в усій мережі і забезпечує диспетчерське управління мережею при складних аварійних ситуаціях, як наприклад, вихід з ладу або перевантаження вузлів. Крім того, він контролює стан облаштувань автоматичного управління, задіяних в устаткуванні мережі, і відображує на дисплеї стан мережі для операторів NMC. Це дозволяє операторам контролювати регіональні проблеми та при необхідності надавати допомогу OMC, відповідальному за конкретний регіон. Таким чином, персонал NMC знає стан усієї мережі і може дати вказівку персоналу OMC змінити стратегію рішення регіональної проблеми.

BSS – це обладнання базової станції, складається з контролера базової станції (BSC) і приймально-передавальних базових станцій (BTS). Контролер

базової станції може управляти декількома приймально-передаючими блоками. BSS управляє розподілом радіоканалів, контролює з'єднання, регулює їх черговість, забезпечує режим роботи із стрибаючою частотою, модуляцію і демодуляцію сигналів, кодування та декодування повідомлень, кодування мови, адаптацію швидкості передачі для мови, даних і виклику, визначає черговість передачі повідомлень персонального виклику.

2.2 Принцип шифрування GSM каналу

Використання пароля (чи коду PIN - персонального ідентифікаційного цифрового коду) – один з простих методів аутентифікації. Він дає дуже низький рівень захисту в умовах використання радіозв'язку. Досить почути цей персональний код усього лише один раз, щоб обійти засоби захисту. Насправді GSM використовує PIN-код у поєднанні з SIM (Subscriber Identify Module), який перевіряється на місці самим SIM без передачі до ефіру. Обчислення аутентифікації зображено на рисунку 2.2.

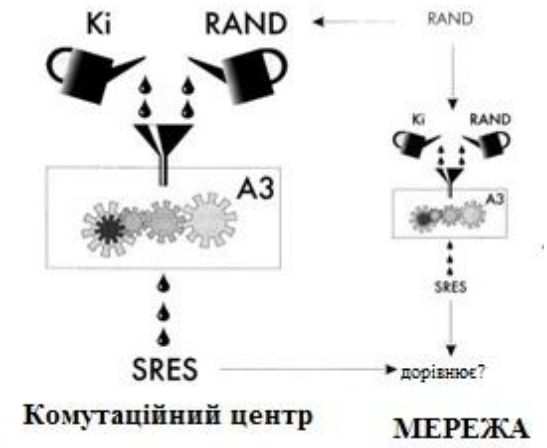

Рисунок 2.2 – Обчислення аутентифікації

Окрім нього, GSM використовує складніший метод, який полягає у використанні випадкового числа, на яке може відповісти тільки відповідне абонентське устаткування (в даному випадку - SIM). Суть цього методу полягає в тому, що існує величезна безліч подібних чисел, тому мало вірогідно, що воно буде використано двічі.

Аутентифікація робиться шляхом вимоги дати правильну відповідь на наступну головоломку: яку відповідь SRES абонент може вивести з RAND, що поступив, застосовуючи алгоритм A3 з особистим (секретним) ключем Ki? Відповідь, яка називається SRES (Signed Result - підписаний результат), отримують у формі підсумку обчислення, що включає секретний параметр, що належить цьому користувачеві, який називається Ki. Секретність Ki є основою всіх механізмів безпеки, свій власний Ki не може знати навіть абонент. Алгоритм, що описує порядок обчислення, називається алгоритмом A3. Як правило, такий алгоритм зберігається в секреті.

Для того, щоб досягти необхідного рівня безпеки, алгоритм A3 має бути однонапрямленою функцією, як її називають експерти криптографи. Це означає, що обчислення SRES при відомих Ki і RAND має бути простим, а зворотна дія – обчислення Ki при відомих RAND і SRES повинно бути максимально ускладнено. Безумовно, саме це і визначає зрештою рівень безпеки. Значення, що обчислюється по алгоритму A3, повинне мати довжину 32 біта. Ki може мати будь-який формат і довжину. Криптографічні методи дають можливість за допомогою відносно простих засобів добитися високого рівня безпеки. У GSM використовуються єдині методи для захисту всіх даних, будь то призначена для користувача інформація, передача сигналів, пов’язаних з користувачем (наприклад, повідомлень, у яких містяться номери телефонів, що викликаються), або навіть передача системних сигналів (наприклад, повідомлень, що містять результати радіо-вимірів для підготовки до передачі). Необхідно проводити відмінність тільки між двома випадками: або зв’язок виявляється захищеним (тоді всю інформацію можна відправляти в зашифрованому виді), або зв’язок є незахищеним (тоді вся інформація відправляється у вигляді незашифрованої цифрової послідовності).

Алгоритм A5 (рисунок 2.3) виводить послідовність шифрування з 114 біт для кожного пакету окремо, з урахуванням номера кадру і шифрувального ключа Kc.

Як шифрування, так і розшифровка робляться за допомогою операції «виключне або» до 114 кодованих біт радіо-пакету та 114-бітової послідовності шифрування, генерованої спеціальним алгоритмом, який називається A5. Для того, щоб отримати послідовність шифрування для кожного пакету, алгоритм A5 робить обчислення, використовуючи два введення: одним з них є номер кадру, а іншим є ключ (який називається Кс), відомий тільки мобільній станції і мережі.

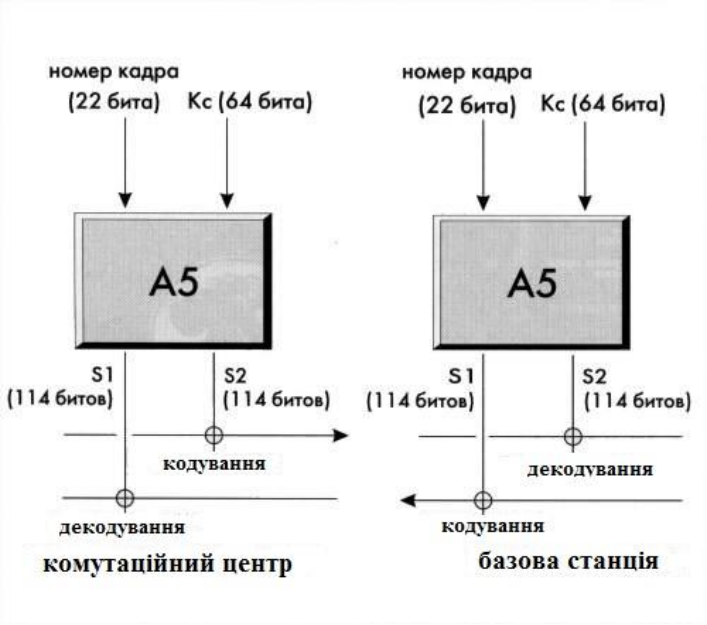

Рисунок 2.3 – Алгоритм A5

В обох напрямках з’єднання використовуються дві різні послідовності: у кожному пакеті одна послідовність використовується для шифрування в мобільний станції та для розшифровки на BTS, тоді як інша послідовність використовується для шифрування в BTS та розшифровки на мобільний станції.

Номер кадру змінюється від пакету до пакету для всіх типів радіоканалів. Ключ Кс контролюється засобами передачі сигналів та змінюється, як правило, при кожному повідомленні. Цей ключ не вдається до гласності, але оскільки він часто міняється, то не потребує таких сильних засобів захисту, як ключ Ki (наприклад, Кс можна вільно прочитати в SIM).

Алгоритм A5 необхідно встановлювати на міжнародному рівні, оскільки для забезпечення MS-роумінгу він має бути реалізований у рамках кожної

базової станції (так само як і у будь-якому мобільному обладнанні). На даний момент один єдиний алгоритм А5 встановлений для використання в усіх країнах. Базові станції можуть підтримувати три основні варіанти алгоритму А5: А5/1 – найбільш стійкий алгоритм, вживаний у більшості країн; А5/2 – менш стійкий алгоритм, що впроваджується в країнах, в яких використання сильної криптографії небажане; А5/3 – шифрування відсутнє. В Україні застосовується алгоритм А5/1. З міркувань безпеки його опис не публікується. Цей алгоритм є власністю організації GSM MOU. Проте, його зовнішні специфікації обнародувані, і його можна представити як чорний ящик, що приймає параметр завдовжки 22 біта та параметр завдовжки 64 біта для того, щоб створювати послідовності завдовжки 114 біти. Як і у випадку з алгоритмом аутентифікації А3, рівень захисту, запропонований алгоритмом А5, визначається складністю зворотного обчислення, тобто обчислення Кс при відомих двох 114-бітових послідовностях шифрування і номера кадру.

Ключ Кс до початку шифрування має бути узгоджений мобільною станцією і мережею. Особливість стандарту GSM полягає в тому, що ключ Кс обчислюється до початку шифрування під час процесу аутентифікації. Потім Кс вводиться в енергонезалежну пам’ять всередині SIM з тим, щоб він зберігався там навіть після закінчення сеансу зв’язку. Цей ключ також зберігається в мережі та використовується для шифрування. Кожного разу, коли яка-небудь мобільна станція проходить процес аутентифікації, ця мобільна станція та мережа також обчислюють ключ шифрування Кс, використовуючи алгоритм А8 з тими ж самими вхідними даними RAND і Ki, які використовуються для обчислення SRES за допомогою алгоритму А3.

Алгоритм А8 використовується для обчислення Кс з RAND і Ki.

Фактично, алгоритми А3 і А8 можна було б реалізувати у формі одного-єдиного обчислення. Наприклад, у вигляді єдиного алгоритму, вихідні дані якого складаються з 96 біт: 32 біта для утворення SRES і 64 біта для утворення Кс. Слід також відмітити, що довжина значимої частини ключа Кс, видана алгоритмом А8, встановлюється групою підписів GSM MOU і може

бути менше 64 бітів. В цьому випадку значимі біти доповнюються нулями для того, щоб в цьому форматі завжди були використані всі 64 біти.

Шифрування виявляється дуже ефективним для захисту конфіденційності, але для захисту кожного окремо взятого обміну інформацією по радіоканалу використовуватися не може. Шифрування за допомогою Кс застосовується тільки в тих випадках, коли мережі відома особа абонента, з яким йде розмова. Зрозуміло, що шифрування не може застосовуватися для загальних каналів, таких як ВССН, який приймається одночасно усіма мобільними станціями у цій стільниковій комірці та в сусідніх стільникових комірках (інакше кажучи, воно може застосовуватися з використанням ключа, відомого всім мобільним станціям, що абсолютно позбавляє його використання, як механізму безпеки). При переміщенні мобільної станції на який-небудь спеціальний канал деякий час відбувається початкове завантаження, впродовж якого мережа ще не знає особу абонента, тому шифрування його повідомлення неможливе. Тому весь обмін сигнальними повідомленнями, що несе відомості про особу невизначеного абонента, повинен відбуватися в незашифрованому виді. Яка-небудь третя сторона на цій стадії може підслуховувати інформацію про цю особу. Вважається, що це обмежує право абонента на секретність, тому в GSM введена спеціальна функція, що дозволяє забезпечити такого роду конфіденційність.

Захист також забезпечується шляхом використання ідентифікаційного псевдоніма, або TMSI (тимчасового ідентифікатору мобільного абонента), який використовується замість ідентифікатора абонента IMSI (міжнародного ідентифікатору мобільного абонента) у тих випадках, коли це можливо. Цей псевдонім має бути погоджений заздалегідь між мобільною станцією і мережею. Особливо варто відмітити, що в наземному каналі передачі дані передаються по дротах в незашифрованому виді, і перехоплення інформації йде саме з них.

3 ФУНКЦІОНУВАННЯ СИСТЕМ БЕЗПЕКИ, ЯКІ ВИКОРИСТОВУЮТЬ GSM КАНАЛИ

3.1 Завадостійкість та завадо-захищеність GSM каналу

Перешкоди в радіоканалі створюються як за рахунок спотворень сигналу при його поширенні, так і в результаті дії зовнішніх джерел. Перший тип спотворень порівняно легко усунути, а з перешкодами від зовнішніх джерел борються за допомогою розширення спектру сигналу, який передають. Теоретично, збільшення бази сигналу (добуток ефективного значення тривалості сигналу та ефективного значення ширини його спектру) дозволяє зменшити перешкоду до скільки завгодно малого рівня.

Основна складність при побудові GSM каналу пов’язана з неможливістю забезпечити безперервність GSM/GPRS-зв’язку з оператором із-за перебоїв у мережі, які призводять до переривання передачі даних і до зависання модему. Практика показує, що жоден GSM-оператор на сьогодні не забезпечує надання гарантованого GPRS-каналу зв’язку. У спробах реалізації безперервності підключення розробники вимушені додатково оснащувати традиційні GSM-модеми додатковими пристроями - зовнішніми контролерами, сторожовими таймерами, що здійснюють перезавантаження модему при зависанні. На жаль, подібні рішення хоч і є зазвичай економічними, але як і раніше не гарантують безперервного і безперебійного процесу передачі даних, а також ведуть до ускладнення системи в цілому і, як наслідок, до зниження її надійності.

Додатково до перерахованих методів, для підвищення завадостійкої РЕС, що використовують вузько-смугові сигнали, застосовують багатократне дублювання фрагментів повідомлень, що передаються у частотній або часовій області. Наприклад, модеми для передачі даних в короткохвильовому діапазоні частот використовують для одночасної передачі інформації до 50 носійних частот, використовуються повільні скачки по частоті SFH (Slow

Frequency Hopping) чи інакше - повільна псевдовипадкова або програмна перебудова радіочастот (ППРЧ). Використання ППРЧ спільно із завадостійким кодуванням і перемеженням дозволяє в умовах вузько-смугових перешкод у каналах із завмираннями підвищити завадостійкість на прийомі на 9-11дБ, в той час, як без ППРЧ ця цифра коливається в межах 4-6 дБ.

Завадостійкість, на думку цілого ряду фахівців в області радіо-канальних пожежних і охоронних систем, визначається наступним:

- кількістю частотних діапазонів, у яких може працювати радіосистема;
- кількістю частотних каналів у кожному діапазоні;
- можливістю автоматичного вибору резервних каналів;
- наявністю автоматичного регулювання потужності випромінювання.

Відповідно до європейської класифікації існує три класи пожежних і охоронних дротяних і радіо-канальних систем, що відрізняються між собою, передусім, по мірі ризику (ЕМ 50131-1) :

- клас А: низька міра ризику – об’єкти приватного користування (заміські будинки, квартири);
- клас В: середня міра ризику – об’єкти громадського користування (магазини, учбові заклади);
- клас С: висока міра ризику – об’єкти державної важливості (музеї, історичні пам'ятники).

Типова ситуація на об’єкті, що знаходиться під охороною радіосистеми. Час від часу пропадає зв’язок з тим або іншим радіопристроєм. Швидше за все, причиною є не умисний саботаж роботи системи, а робота інших приладів та систем за допомогою обраного каналу зв’язку, який використали при установці системи. Діапазон частот 433 і 868 МГц є таким, що не ліцензується, і його використовують не лише пожежні і охоронні радіосистеми, але і побутові пристрої: переносні радіостанції, іграшки, шлагбауми і так далі. Залежно від класу, радіосистеми повинні реагувати по-різному:

- клас А: індикація про тимчасову втрату зв’язку з радіо-облаштуванням системи відсутня;

- класи В і С: радіосистема зобов’язана максимально використати всі можливі способи доставки сигналу і тільки після цього передати сигнал "Тривога".

Наприклад, сповіщувач, не отримавши квитанцію від приймально-контрольного приладу після передачі тестового сигналу (що можливо тільки у системі з двостороннім протоколом), негайно міняє частотний канал, потужність випромінювання, періодичність виходу до ефіру і так далі. Якщо зв’язок не може бути відновлений навіть після всіх згаданих дій, то в даному випадку має місце умисний саботаж роботи системи.

Здатність радіолінії працювати в умовах дії організованих перешкод називається завадо-захищеністю. Завадо-захищеність розділяється на два класи:

- просторова завадо-захищеність (за рахунок низького рівня бічних пелюсток приймальної антени, по яких діє перешкода, формування нулів діаграми спрямованості приймальної антени у напрямі на джерело перешкод);

- сигнальна завадо-захищеність (за рахунок широкосмугових методів модуляції).

Принцип пригнічення заснований на постановці вузько-смугової перешкоди приймальному каналу GSM-пристрою. На сьогодні пригнічувачів GSM-пристроїв дуже багато, їх основне використання заглушати мобільні телефони на нарадах, конференціях, у бібліотеках, театрах і тому подібне. Проте це не заважає застосовувати їх і для негативних цілей. Їх застосування не залишиться не поміченим для операторів мобільного зв’язку.

Відомі декілька типів пристроїв, вживаних для глушення супутникових і GSM охоронних систем:

- широкосмугова глушилка (постійно випромінює потужний шум на всіх робочих частотах GSM, тим самим GSM-модуль перестає бачити як

супутники GPS, які передають поточні координати автомобіля, так і БС оператора GSM);

- глушилка, що перебирає частоти (цей тип глушилок працює також як і перший тип, відмінність лише у тому, що шумоподібна перешкода ставиться послідовно по всіх частотах каналу GSM, не дозволяючи GSM-модулю передавати сигнал; розміром вона досить компактна та живиться від звичайних батарей, діє в радіусі 5-15 метрів);

- «розумна» (це глушилка, яка видає себе за базову станцію оператора GSM; при її включенні, GSM-модуль працюватиме без збоїв та вважати, що все добре, глушилка вимагає потужного джерела живлення).

На сьогодні існує два способи боротьби з глушенням:

- визначення факту глушення на стороні GSM-модуля (якщо модуль бачить, що в ефірі на робочих частотах з'явився сигнал або шум, він намагається встигнути зробити сповіщення; але це мало вірогідно, адже відправити SMS або голосове повідомлення навряд чи вийде тому, що передавач вже заглушений);

- визначення факту глушення ззовні (для цього організовується постійна перевірка зв'язку між GSM-модулем та спеціально виділеним сервером – контроль каналу, таким чином, на стороні сервера можна гарантовано визначити пропажу зв'язку з автомобілем; у разі пропажі GSM-сигналу, сервер оповіщає власника SMS-повідомленням, по e -mail, або дзвінком).

Для зниження глушення сигналу треба:

- мати дублюючий канал для обміну важливою інформацією;

- використовувати періодичний тест з об'єкту;

- застосувати виносні антен.

3.2 Дослідження швидкості передачі даних та пропускної спроможності GSM каналу

Максимальна швидкість передачі даних по одному голосовому каналу GSM (режим CSD) складає 9,6 Кбіт/с, а багатоканальний режим HSCSD забезпечує передачу даних на швидкості 19,2 Кбіт/с і вище. У таблиці 3 наведено перелік послуг та якість роботи додатків на різних швидкостях передачі.

Таблиця 3. Перелік послуг і якість роботи додатків на різних швидкостях передачі

	9,6	14,4	32	64	128	384	2 М
Голос, SMS	+	+	+	+	+	+	+
E-mail	-	±	+	+	+	+	+
Відео-зображення, фото	-	±	+	+	+	+	+
Робота з БД	-	-	±	+	+	+	+
ПД	-	-	±	+	+	+	+
Відео(повільне)	-	-	±	+	+	+	+
Інтернет	-	-	±	±	+	+	+
Повне відео	-	-	-	±	±	+	+

До недоліків використання голосового каналу GSM можна віднести значну вартість пересилки кілобайта інформації та істотний негативний вплив (на економічні показники системи) часу організації сеансу зв’язку між модемами, при передачі малих об’ємів даних. У таблиці 4 наведені характеристики поколінь GSM.

Таблиця 4. Характеристики поколінь GSM

Технології	2G	2,5G	3G
Базові послуги	Мова	Мова, данні	Мова, данні, відео данні
Швидкість передачі, кбіт/с	9,6-14,4	115(фаза 1), 384(фаза 2)	2048(фаза 1), 10^4 (фаза 2)
Тип комутації	Комутація каналів	Змішана (переважно каналів)	Змішана (переважно пакетів)
Базові технології радіо доступу	GSM, TDMA, PDC,CDMA One	GPRS, EDGE,IS-136+, IS-95B/C, CDMA 2000 1X	Стандарти серії IMT-2000

Наприклад, час передачі 20 Кбіт інформації дорівнює приблизно 2 с, а час організації сеансу може варіюватися від 2 до 16 с, залежно від режиму роботи модемів. Максимально можлива швидкість обміну даними за допомогою технології GPRS теоретично може досягати 170 кбіт/с.

У технології GPRS була запропонована нова структура пакету розміром 456 біт (чотири інформаційні блоки по 114 біт), яка забезпечує загальну швидкість передачі по каналу 22,8 кбіт/с. В цілях підвищення гнучкості передачі і пропускної спроможності в системі GPRS можуть використовуватися чотири схеми кодування даних: від CS1 до CS4(табл.5). Для управління роботою радіолінії у режимі пакетної передачі розроблений спеціальний протокол RLC (Radio Link Control), який забезпечує її адаптивне налаштування, програмну перебудову частоти та управління потужністю. Адаптація радіолінії включає вибір тієї або іншої схеми кодування (CS1-CS4) залежно від виду інформації, що передається характеристик радіоканалу і рівня перешкод.

Таблиця 5. Основні характеристики схем кодування в GPRS

Схема кодування	CS1	CS2	CS3	CS4
Кількість інформаційних бітів	181	268	312	428
Швидкість кодування	½	½	½	1
Загальна кількість бітів у кадрі	456	456	456	456
Швидкість передавання інформації, кбіт/с	9,05	13,4	15,6	21,4

Таким чином, в режимі GPRS кожному абонентові надається від 1 до 8 канальних інтервалів. Під час пакетної передачі ресурси ліній зв’язку вгору та вниз можуть виділятися незалежно один від одного, тобто в системі допускається реалізація асиметричного режиму передачі. При використанні схеми кодування CS2 швидкість передачі даних в GPRS-системі складає 115,2 (8x14, 4) Кбіт/с, проте теоретично вона може бути збільшена до 171,2 (8x21, 4) Кбіт/с - якщо застосувати схему кодування CS4.

Принципи оптимізації якості зв’язку при використанні чотирьох варіантів кодування даних залежно від відношення сигнал/шум (C/I) наведено на рисунку 3.1.

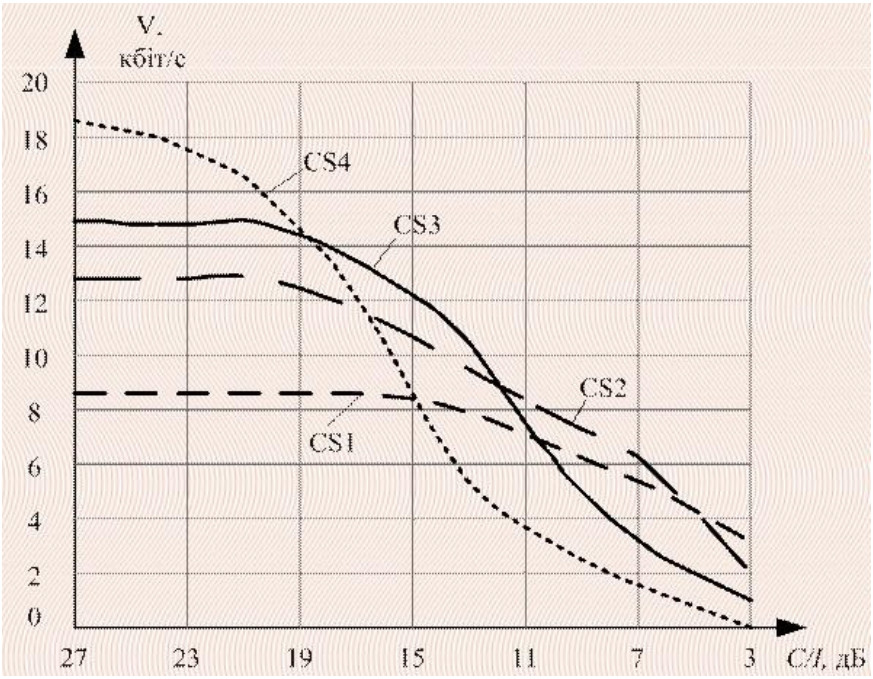

Рисунок 3.1 – Відношення сигнал/шум

Перша схема CS1 гарантує з'єднання в будь-яких умовах і є найбільш зручною при передаванні сигналізації і коротких повідомлень. Друга схема CS2 призначена для передавання трафіку та дозволяє підвищити пропускну здатність мережі. Два інших варіанти кодування забезпечують найвищі швидкості передавання при високому відношенні сигнал/шум, проте при відношенні C/I менше, ніж 9 дБ поступаються CS1 і CS2. Слід відмітити, що реалізація CS3 та CS4 вимагає модернізації A-bis інтерфейсу.

Проведені дослідження швидкості мобільного з'єднання показали, що реально середня швидкість для вхідного з'єднання складає 130 Кбіт/с, а вихідного 57 Кбіт/с. Жоден з операторів мобільного інтернету не показав максимально можливу для використовуваного ними стандарту швидкість (474 Кбіт/с для EDGE у GSM). Окремо варто згадати, що швидкість передачі значно зростає при використанні технології EDGE.

EDGE (англ. Enhanced Data rates for GSM Evolution) – цифрова технологія для мобільного зв'язку, яка функціонує як надбудова над 2G і 2.5G (GPRS) мережами. Для підтримки EDGE у мережі GSM потрібні певні модифікації та вдосконалення. На основі EDGE можуть працювати: ECSD – прискорений доступ в інтернет по каналу CSD, EHSCSD – по каналу HSCSD та EGPRS –

по каналу GPRS. EDGE був уперше представлений в 2003 році в Північній Америці. Попри те, що EDGE не вимагає апаратних змін в NSS-частинах мережі GSM, модернізації має бути піддана підсистема базових станцій (BSS). Необхідно встановити трансивери, які підтримують EDGE (8PSK модуляцію) та оновити програмне забезпечення. Також потрібні телефони, що забезпечують апаратну та програмну підтримку модуляції та кодових схем, використовуваних в EDGE.

3.3 Аналіз моделі GSM каналу, щодо забезпечення необхідної зони покриття

3.3.1 На дальність радіозв'язку впливають наступні чинники:

1) Місце розташування BS і MS і рельєф місцевості.

2) Потужність і чутливість MS.

3) Потужність і чутливість BS.

4) Використовувані на MS та BS антени.

Зазвичай базові станції мають потужність 20-30 Вт. Антени застосовуються штирові або спрямовані. Чутливість базових станцій складає 100 дБ -115 дБ. Змінити або вплинути на всі ці параметри користувач, звичайно, не може. Більшість операторів використовують обмеження дальності роботи мобільного телефону від базової станції –
35 км для GSM-900 та близько 10 км для GSM-1800 , що обумовлено особливостями стандарту. Проте в GSM передбачена також нестандартна конфігурація стільника, при якій дальність зв'язку збільшується на 70-100 км (конфігурація Extended Cell). При такій конфігурації кількість розмовних каналів зменшується до 2-3, що зменшує місткість мережі. Використати такий режим у місті та околиці операторові не вигідно. Іноді цей режим використовується на морському узбережжі для створення прибережної зони покриття. Залізобетонні будови здатні послабляти сигнали, що проходять через них (при внутрішньому покритті), в 100-1000 разів (тобто на 20-30 дБ). До числа перешкод можна також віднести кузови автомобілів, крони дерев і так далі. Вплив можуть зробити і атмосферні опади.

При розрахунку зони покриття застосовується модель Хата, оскільки вона рекомендована Міжнародним Консультативним Комітетом з Радіозв'язку (МККР) та досить проста в застосуванні. Ця модель дозволяє обчислити втрати на радіотрасі для конкретної місцевості та параметрів базової станції.

Середній рівень втрат на радіотрасі, використовуючи емпіричну модель Хата, визначається таким чином:

$$L = 69{,}55 + 26{,}16\lg(f) - 13{,}82\lg(H_{bs}) + [44{,}9 - 6{,}55\lg(H_{bs})]\lg(r) + \alpha(h_{as}) + \alpha(U_r) + \alpha(b) + \alpha(H_{bs}, f), (\text{дБ})$$

де, $f = (100; 3000) -$ частота, (МГц);

$H_{bs} = (30; 300) -$ висота базової станції, (м);

$r = (1; 100) -$ відстань між базовою та абонентською станцією, (км)

$h_{as} = (1; 3) -$ висота абонентської станції, (м)

$\alpha(h_{as}) = (1 - U)\beta_1 + U(\beta_2 F_1 + \beta_3 F_2) -$ коефіцієнт, який враховує висоту антени абонентської станції (U=0, для невеликого або середнього міста; U=1 для великого міста)

$\alpha(U_r) = (1 - U_r)([1 - 2U_r]\gamma_1 + 4U_r\gamma_2) -$коефіцієнт, який враховує характер місцевості ($U_r = 0$ для сільської місцевості; $U_r = 0{,}5$ для пригороду та $U_r = 1$ для міста).

$\alpha(H_{bs}, f) = \left(27 + \frac{f}{230}\right) lg \frac{17(H_{bs}+20)}{17(H_{bs}+20)+r^2} + 1.3 - \frac{f-55}{750} -$ коефіцієнт, який враховує сферичність Землі (вводиться, якщо $0{,}2R_0 < r \leq 0{,}8R_0$, де R_0 – відстань прямої видимості).

$\alpha(b) = 25\lg(b) - 30 -$ коефіцієнт, який відображає вплив щільності забудови.

b=(3;50) – щільність забудови, (%).

$\beta_1 = (0{,}7 - 1{,}11\lg(f))h_{as} + 1{,}56\lg(f) - 0{,}8$.

$\beta_2 = 1{,}1 - 8{,}29lg^2(1{,}54h_{as})$.

$\beta_3 = 4{,}97 - 3{,}2lg^2(11{,}75h_{as})$.

$$F_1 = \frac{300^4}{f^4 + 300^4}$$

$$F_2 = \frac{f^4}{f^4 + 300^4}$$

$$\gamma_1 = 4{,}78lg^2(f) - 18{,}33\lg(f) + 40{,}94$$

$$\gamma_2 = 2lg^2\left(\frac{f}{28}\right) + 5{,}4$$

Тепер, виходячи з розрахунку в додатку А та вихідної потужності передавача Р(дБ), запасу по завмираннях S(дБ) та необхідного рівня сигналу на вході приймача Q(дБ), запишемо рівняння для знаходження R – максимальної відстані від БС, на якій досягається необхідна якість зв'язку:

$$P - L - S = Q;$$

$$P - \left(134{,}65 + 35lgR + 30{,}9\lg\left(1 + \frac{R^2}{884}\right)^{-1}\right) - S = Q.$$

Задаючи відповідні параметри Р(дБ), S(дБ) (зазвичай береться рівним 20 дБ), Q(дБ) (для МС береться – 110 дБ), можна обчислити відстань впевненого зв'язку R; на підставі цих даних будується зона покриття БС з точки зору якості сигналу (без урахування навантаження на стільнику та можливостей БС по пропускній спроможності).

На рисунку 3.2 показаний характерний вид функції рівня сигналу залежно від відстані між БС та абонентом. Перетин цієї функції з прямою Q дає значення максимального значення радіусу зони обслуговування, при якому ще надаються послуги потрібної якості. Для стандарту GSM-900 R~3-10 км (в окремих випадках до 30 км).

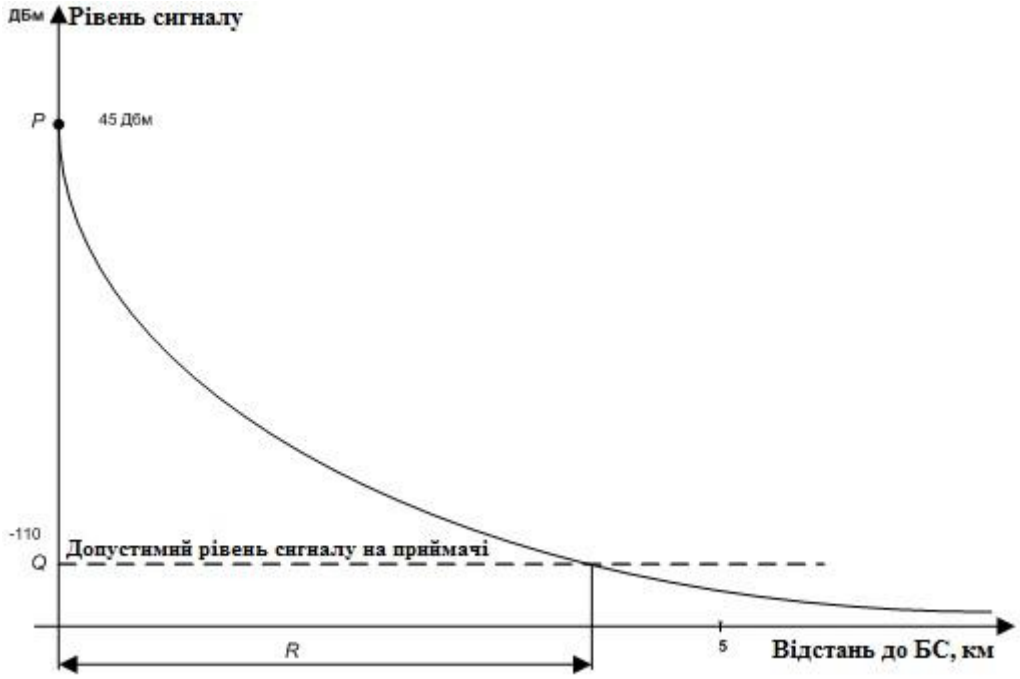

Рисунок 3.2 – Залежність рівня сигналу від відстані до БС

Тому доводиться звужувати зону покриття та збільшувати кількість БС, виходячи з прогнозів абонентського навантаження на стільнику. При розрахунку абонентського навантаження та місткості, стільники часто користуються моделлю Ерланга для систем з відмовою. У цьому випадку вірогідність відмови в обслуговуванні (вірогідність виклику у момент зайнятості всіх каналів) обчислюється так:

$$P_n = \frac{\frac{A^n}{n!}}{\sum_{i=0}^{n} \frac{A^i}{i!}},$$

де $A = \lambda \cdot T$ – навантаження, n – загальна кількість каналів

Розрахуємо навантаження на БС, яка обслуговує селище на 50 котеджів, обладнаних охоронною системою, яка використовує голосовий канал передачі повідомлень.

Навантаження на БС складається з системних дзвінків (раз в 5 хвилин тривалістю - 5 секунд, так як перші 5 секунд безкоштовні) та дзвінків, здійснюваних цивільними абонентами. Приблизно при такому навантаженні

A=1. Вірогідність відмови в обслуговуванні (вірогідність виклику у момент зайнятості всіх каналів) обчислюється як:

$$P_n = \frac{\frac{A^n}{n!}}{\sum_{i=0}^{n} \frac{A^i}{i!}}$$

Тоді залежність вірогідності відмови від кількості каналів буде представлена на рисунку 3.3.

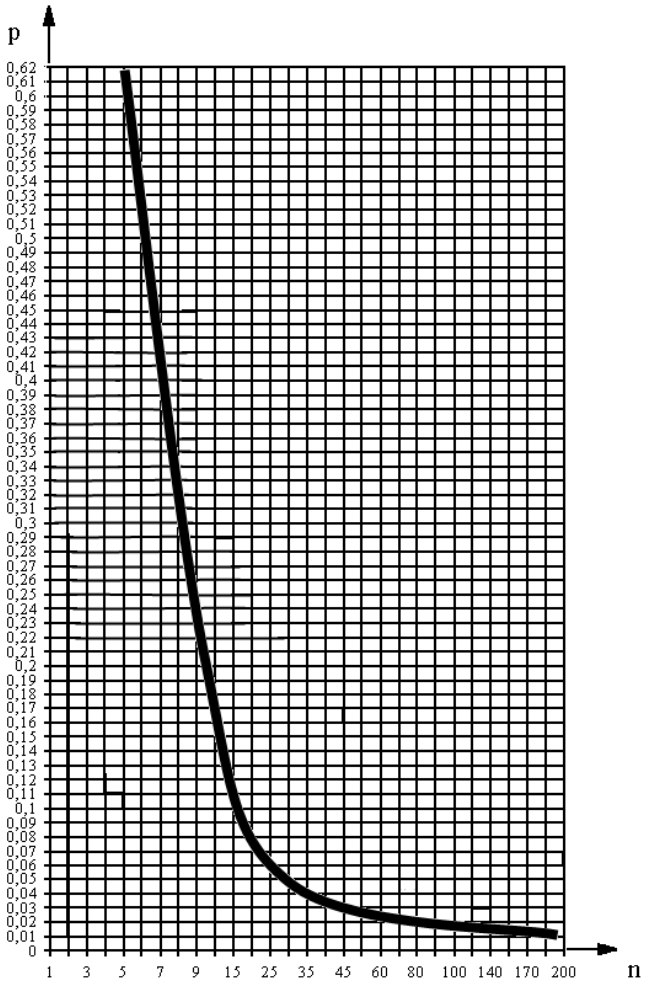

Рисунок 3.3 – Залежність вірогідності відмови від числа каналів

Проведемо розрахунок втрат передачі у великому місті за допомогою емпіричної моделі Олсбрук–Парсона .

Вихідні данні:

$f = 160$ МГц $-$ робоча частота;

$r = 5$ км $-$ відстань між антенами базової та мобільної станції;

$h_{ms} = 10$ м $-$ висота мобільної антени;

$h_{bs} = 30$ м $-$ висота базової антени;

$\lambda = 1{,}875$ м $-$ довжина хвилі;

$b = 5$ м $-$ глибина вулиці, на якій розташована мобільна антена;

$h = 30$ м $-$ середня висота будинків поблизу мобільної антени;

$\gamma = 0$ $-$ коригуючий коефіцієнт, що залежить від частоти, для

$f < 200$ МГц $-$ $\gamma = 0$.

Розв'язок:

$$L = L_F + \sqrt{(L_P - L_F)^2 + {L_D}^2} + \gamma$$

$L_F = 32{,}45 + 20\lg(f) + 20\lg(r) = 32{,}45 + 20lg(160) + 20\lg(5) = 32{,}45 + 44 + 14 = 90{,}45$ дБ – втрати передачі у вільному просторі;

$L_P = 120 - 20\lg(h_{ms}) - 20\lg(h_{bs}) + 40\lg(r) = 120 - 20\lg(10) - 20\lg(30) + 40\lg(5) = 120 - 20 - 29{,}4 + 28 = 98{,}6$ дБ - втрати поширення над плоскою землею;

$L_D + \gamma = 20lg\left[\frac{h - h_{ms}}{\sqrt{b\lambda}}\right] + 16 + \gamma = 20lg\left[\frac{30 - 10}{\sqrt{5 \cdot 1{,}875}}\right] + 16 = 16{,}2 + 16 + 0 = 32{,}2$ дБ - дифракційні втрати, обумовлені характером рельєфу місцевості під міською забудовою;

$L = L_F + \sqrt{(L_P - L_F)^2 + {L_D}^2} + \gamma = 90{,}45 + \sqrt{(98{,}6 - 90{,}45)^2 + 32{,}2^2} + 0 = 90{,}45 + \sqrt{66{,}42 + 1036{,}84} = 90{,}45 + 33{,}21 = 123{,}66$ дБ – втрати передачі.

З розрахованих даних можна зробити висновок. Отримані результати достатні для побудови системи. При таких втратах передачі буде підвищене ослаблення, яке обумовлено великою кількістю перешкод типу кам'яних і залізобетонних будівель, великої кількості дротів, дахів будівель.

Велика неоднорідність поля у різних точках спостереження обумовлена інтерференцією великого числа хвиль, відбитих від різних перешкод у межах міста. Розрахунки показали, що рівень відбитих сигналів становить 50 – 60% від прямого сигналу.

3.3.2 З точки зору підтримки стабільного радіозв’язку потрібно використання таких елементів як виносні антени (рисунок 3.4). Існують три ситуації, у яких стаціонарні спрямовані пасивні антени можуть допомогти:

- нестійкий зв’язок на межі зони покриття з граничною віддаленістю від найближчої базової станції (БС);

- робота всередині зони покриття, але в місцях радіо тіні (складки рельєфу, екранування великими природними та штучними спорудами);

- зв’язок всередині приміщення з високою мірою послаблення сигналу (підвали та напівпідвали; металеві споруди; будівлі, які обшиті металом).

Рисунок 3.4 – Виносні антени

На закритих трасах, що проходять в гірських районах, напруженість поля УКХ визначається особливостями гірського рельєфу, з яких основними є великі перепади висот рельєфу місцевості і наявність перешкод у вигляді окремих гір або ряду гірських хребтів. Форма перешкод може бути найрізноманітнішою: від гострих гір великої висоти до пологих пагорбів порівняно малої висоти. Для визначення поля в точці прийому на такому виді траси застосовують добре розроблені у фізичній оптиці методики розрахунку дифракційного поля, головним чином, у відповідності принципом Гюйгенса–Френеля. Електричні параметри перешкод не враховуються, бо вважають, що вони «непрозорі».

При цьому гірський хребет апроксимується одиночною клиноподібною перешкодою. Можливі два випадки поширення радіохвиль за наявності клиноподібної перешкоди (абсолютно поглинаючий екран):

- екран не перетинає повністю прямолінійного шляху поширення і лише в деякій мірі вклинюється в область, яка ефективно бере участь в перенесенні енергії (умовно вважаємо в цьому випадку висоту позитивною (H > 0, освітлена зона); введемо визначення справжнього просвіту (H) як найкоротшої відстані між кромкою екрану і прямою AB, яка з'єднує точку передачі і прийому. На рисунку 3.5 зображено схему поширення радіохвиль при наявності на шляху клиновидного екрану в освітленій зоні (H> 0).

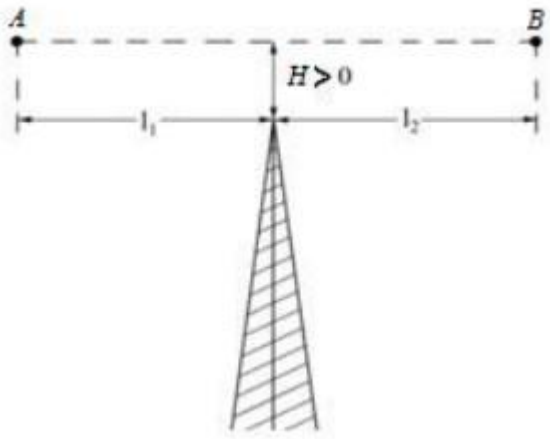

Рисунок 3.5 – Схема поширення радіохвиль

- екран перетинає шлях AB (висота H в цьому випадку має негативний знак, H < 0, область тіні).

На рисунку 3.6 зображено схему поширення радіохвиль при наявності на шляху клиновидного екрану в зоні тіні (H < 0). Реальне розширення зони покриття за рахунок застосування виносної антени може бути здійснене. Причому це збільшення сильно залежить від використовуваного стандарту. Досить потужний ефект дає використання GSM-репітерів, але з-за високої вартості застосовувати їх раціонально на великих об'єктах. Серйозну проблему складає перевантаженість ліній зв'язку по великим святам. Вирішенням проблеми є установка об'єктового приладу з SIM картами двох

різних мобільних операторів зв’язку. Оптимальним для GSM-сигналізацій є комбінування різних функцій (SMS, Voice).

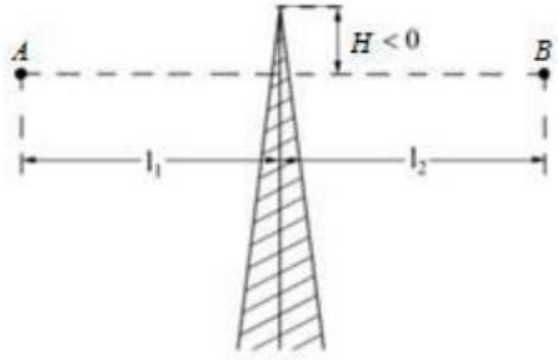

Рисунок 3.6 – Схема поширення радіохвиль

Також ефективно використання GSM як дублюючого або додаткового каналу дротяним та іншим радіо-канальним системам передачі сповіщення. З точки зору пропускної спроможності каналу виправдано використання технології EDGE, 3G.

3.4 Розробка рекомендацій, щодо покращення технічних характеристик систем безпеки, які використовують GSM канали.

Охоронні системи на основі GSM можна використати, як для особистих цілей, так і в комплексних централізованих системах охорони та моніторингу. Дуже вигідно використання GSM сигналізації на об’єктах, де ускладнено прокладення кабельних та телефонних мереж. GSM-сигналізація підвищує захищеність об’єкту власності завдяки наступним чинникам:

- факт наявності сигналізації змусить не досвідчених злочинців відмовитися від своїх злочинних намірів;

- оперативна передача тривожного повідомлення на телефон власника або на ПЦС, а так само спрацьовування сирени, приведуть до прибуття на місце групи швидкого реагування або наряду міліції, що приведе до затримання злочинців.

Виходячи з попереднього розгляду систем безпеки, які використовують GSM канали можна сформулювати наступні рекомендації:

1) Пристрої сигналізації мають бути стійкими до механічних пошкоджень - знаходитися у металевих боксах, де встановлені всі елементи (GSM-термінал, колодки підключення шлейфів, блок живлення).

2) Прилади повинні мати не менше чотирьох з'єднувачів для підключення різних датчиків. Ці зони повинні бути програмованими під різні типи датчиків.

3) Системи безпеки повинні оснащуватися вбудованими джерелами безперебійного живлення для забезпечення надійної роботи централі і підключених до неї датчиків при відключенні зовнішнього живлення, як мінімум протягом доби.

4) Системи безпеки повинні мати виносну світлову індикацію, яка дозволяє контролювати стан приладів.

5) Системи безпеки повинні забезпечувати в одному повідомленні повний опис стану всієї системи: тривоги з вказівкою зони, ідентифікацію включення реле датчиків, залишковий заряд батареї, стан телефонної лінії (якщо вона є).

6) Системи повинні забезпечувати додаткові функції –можливість реагувати на зовнішні подразники: при блокуванні стільникової мережі в окрузі завадами «глушилки» система повинна не тільки перебирати номери для повідомлення такої події, а відразу відкривати клітини з собаками-охоронцями, запалювати світло, включати сирену або пускати сльозогінний газ.

7) Система повинна подавати сигнал попередньої тривоги власникові будівлі при погіршенні якості сигналу від базової станції. Важливо якщо GSM панель передає повідомлення одночасно декільком користувачам та пультам централізованого спостереження. Повідомлення для ПЦС повинні передаватися в зашифрованому вигляді.

8) Для підтримки стабільного радіозв'язку потрібно використання виносних антен.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

У даному розділі визначені основні потенційні шкідливі та небезпечні виробничі фактори, а також розроблені заходи щодо покращення умов праці в робочих приміщеннях при виконанні дослідницької роботи частотно-територіального планування та оптимизація параметрів баз даних рухомого мобільного GSM зв'язку. Також запропоновані технічні рішення та організаційні заходи із гігієни праці, виробничої санітарії і техніки безпеки. Враховуючи специфіку даної роботи основна увага була приділена заходам щодо створення безпечних умов праці користувачів ВДТ ПЕОМ з урахуванням ДСанПІН 3.3.2.007-98 та НПАОП 0.00-4.33-99. Крім цього визначені основні заходи з безпеки в надзвичайних ситуаціях.

4.1 Визначення основних потенційно небезпечних та шкідливих виробничих факторів у робочих приміщеннях

Визначимо основні потенційно шкідливі та небезпечні виробничі фактори, які виникають при проведенні експериментальних вимірювань та під час експлуатації ЕОМ, відео дисплейних терміналів (ВДТ). Небезпечними та шкідливими факторами можуть бути:

- підвищений рівень електромагнітного випромінювання радіочастотного діапазону;
- можливість ураження електричним струмом;
- невідповідність параметрів мікроклімату санітарним нормам та правилам;
- недостатня освітленість робочої зони;
- група психофізичних факторів: перевантаження фізичне та психологічне;
- підвищений рівень інфрачервоного (ІЧ) випромінювання;
- підвищений рівень шуму на робочих місцях;
- можливість виникнення пожежі в робочих приміщеннях.

Далі проведемо аналіз найбільш небезпечних та шкідливих виробничих факторів.

4.2 Технічні рішення та організаційні заходи із гігієни праці, виробничої санітарії та техніки безпеки.

4.2.1 Правила безпеки під час експлуатації електронно-обчислювальних машин

Правила безпеки під час експлуатації ВДТ ПЕОМ регламентуються ДСанПІН 3.3.2.007–98 та НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями, які встановлюють вимоги безпеки та санітарно-гігієнічні вимоги до обладнання робочих місць користувачів ЕОМ і працівників, що виконують обслуговування, ремонт та налагодження ЕОМ, та роботи з застосуванням ЕОМ, відповідно до сучасного стану техніки та наукових досліджень у сфері безпечної організації робіт з експлуатації ЕОМ та з урахуванням положень міжнародних нормативно-правових актів з цих питань (директиви Ради Європейського союзу 90/270/ЄЕС, 89/391/ЄЕС, 89/654/ЄЕС, 89/655/ЄЕС, стандарти ISO, MPRII).

4.2.2 Вимоги до приміщень в яких розміщені ЕОМ.

Облаштування робочих місць, обладнаних ЕОМ, ВДТ, повинно забезпечувати:

- належні умови освітлення приміщення і робочого місця, відсутність відблисків;
- оптимальні параметри мікроклімату (температура, відносна вологість, швидкість руху, рівень іонізації повітря);
- належні ергономічні характеристики основних елементів робочого місця;

Будівлі та приміщення, в яких експлуатуються ЕОМ та виконуються їх обслуговування, налагодження і ремонт, повинні відповідати вимогам:

ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин". №382/3675 , 1998 р. , НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями, що затверджено наказом Міністерства соціальної політики України 14.02.2018 № 207.

Заборонено розміщувати робочі місця з ВДТ, ЕОМ у підвальних приміщеннях, на цокольних поверхах, поряд з приміщеннями, в яких рівні шуму та вібрації перевищують допустимі значення (поряд з механічними цехами, майстернями тощо), з мокрими виробництвами, з вибухонебезпечними та пожежо-небезпечними приміщеннями категорій А і Б, а також над такими приміщеннями або під ними.

Приміщення мають бути обладнані системами водяного опалення, кондиціонування або припливно-витяжною вентиляцією відповідно до ДБН В.2.5 – 67:2013 «Опалення, вентиляція та кондиціонування».

Згідно з ДСП 173-96 «Державні санітарні правила планування та забудови населених пунктів» площу приміщень визначають із розрахунку, що на одне робоче місце вона має становити не менше ніж 6 м^2, а об'єм не менше ніж 20 м^3 з урахуванням максимальної кількості осіб, які одночасно працюють у зміні. Приміщення являє собою кімнату розміром 7 х 5 м., висотою 4 м. Розмір дверного прорізу 1,5м.

Площа й об'єм приміщення знаходимо по формулах

$$S = a \cdot b,$$

$$V = S \cdot h,$$

де a - довжина, b - ширина, h - висота приміщення.

Маємо:

$S=7 \cdot 5=35$ м^2, $V=35 \cdot 4^{=}140$ м^3.

Зведемо нормативні та фактичні дані приміщення в таблицю 4.1.

Табл. 4.1. Параметри приміщення

Назва характеристики	Нормативне	Фактичне
Площа приміщення з розрахунку	>6 м^2	35 м^2
Об'єм приміщення з розрахунку на 1	>20 м^3	140 м^3
Висота приміщення	3,5 – 4 м	4 м
Розміри дверей	≥1,1х1.8м	1,5х2 м
Відстань від стіни зі світловими прорізами до ВДТ	≥1м	1,5 м

На підставі отриманих результатів можна зробити висновок, що геометричні розміри приміщення цілком відповідають нормативним вимогам.

Оздоблюють стіни, стелю, підлогу приміщення з матеріалів, які дозволені органами державного санітарно-епідеміологічного нагляду. Заборонено застосовувати полімерні матеріали (деревостружкові плити, шпалери, що можна мити, рулонні синтетичні матеріали, шаруватий паперовий пластик, тощо), що виділяють у повітря шкідливі хімічні речовини. За розміщенням робочих місць з ВДТ, ЕОМ потрібно витримувати такі відстані: від стін зі світловими прорізами не менше 1 м; між бічними поверхнями ВДТ не менше 1,2 м; між тильною поверхнею одного ВДТ та екраном іншого не менше 2,5 м; прохід між рядами робочих місць не менше 1 м. Робочі місця з ВДТ щодо світлових прорізів розміщують так, щоб природне світло падало збоку, переважно зліва. Екран ВДТ і клавіатура мають розміщуватися на оптимальний відстані від очей користувача, але не ближче 600 мм з урахуванням розміру алфавітно-цифрових знаків і символів. Розміщення екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом ± 30° від лінії зору працівника.

Усі вище перераховані вимоги відповідають робочому приміщенню, де проводяться дослідження.

4.2.3 Відповідність параметрів мікроклімату та повітря робочої зони санітарним нормам

Для підвищення працездатності і збереження здоров'я важливо створити для людини стабільні метеорологічні умови - мікроклімат повітряного середовища, у поняття якого входять температура, відносна вологість, швидкість руху повітря та інтенсивність теплового опромінення.

Стан повітряного середовища визначається метеорологічними умовами в лабораторії, виробничим мікрокліматом, а також запиленістю повітря і його загазованістю.

Мікроклімат виробничого приміщення визначається поєднаннями температури, вологості, швидкості руху повітря та інтенсивності теплового випромінювання, що впливають на організм людини.

Для того, щоб фізіологічні процеси в організмі людини протікали нормально, температура його тіла повинна бути постійною. Надлишкова теплота повинна виділятися в навколишнє середовище. Відповідність між цією теплотою та охолоджувальною здатністю навколишнього середовища визначає комфортні умови.

При відхиленні параметрів мікроклімату від комфортних в організмі людини відбуваються процеси, спрямовані на терморегулювання. Розрізняють хімічну і фізичну терморегуляцію організму. Хімічна відбувається зниженням рівня обміну речовин, а фізична - за допомогою теплопровідності, конвекції, випромінювання і випарювання.

Значні відхилення параметрів мікроклімату від оптимальних можуть стати причиною ряду простудних захворювань.

Робочою зоною вважається простір, обмежений конструкціями виробничих приміщень, що мають висоту 2 м над рівнем підлоги чи площадки, на яких знаходяться місця постійного чи непостійного перебування працюючих. Склад повітря робочої зони залежить від складу атмосферного повітря і

впливу на нього виробничих факторів, що утворюються в процесі трудової діяльності людини.

Для нормальної життєдіяльності людини важливий парціальний тиск кисню - 21331 Па (160 мм рт.ст.) і необхідно, щоб у повітрі приміщень містилось не менш 19,5 - 20% кисню.

Вміст шкідливих речовин у повітрі робочої зони не має перевищувати ГДК. Відповідно до ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» - К.: МОЗ вміст озону - не більше 0,1 мг/м3, вміст оксидів азоту - не більше 5 мг/м3, вміст пилу - не більше 4 мг/м3.

Важливо, щоб повітря мало визначений іонний склад. У повітрі містяться негативні і позитивні іони, що по рухливості розділяють на легкі, середні і важкі. На життєдіяльність організму людини благотворно впливають негативні іони кисню. Вміст легких іонів у повітрі виробничих і громадських приміщень, повітряне середовище яких піддається спеціальній обробці в системах кондиціонування, приведено в таблиці. 4.2. Іонний склад повітря має відповідати вимогам ДБН В.2.5-67:2013.

Таблиця 4.2. Припустимий вміст легких іонів у повітрі робочої зони.

Рівень іонізації повітря	Число іонів у 1 $см^2$ повітря		Значення показника полярності
	n^+	n^-	
Мінімально необхідний	400	600	-0,2
Оптимальний	1000-3000	3000-5000	від -0,67 до 0
Максимально припустимий	5000	5000	від -0,05 до +0,05

Норми метеорологічних умов при розробці пристрою регламентуються ДСН 3.3.6.042-99. Значення оптимальних, припустимих і фактичних параметрів мікроклімату на постійному робочому місці розробника пристрою

для категорії виконуваних їм робіт в холодний і теплий період року приведені в таблиці 4.3.

Таблиця 4.3. Нормовані значення параметрів мікроклімату в робочій зоні розробника

Період року	Параметр мікроклімату	Нормовані значення параметрів мікроклімату		Фактичні значення параметрів мікроклімату
		оптимальні	допустимі	
Холодний	Температура, °С	22-24	21-25	21-22
	Відносна вологість, %	40-60	75	65-75
	Швидкість руху, м/с	не більше 0,1	не більше 0,1	не більше 0,1
Теплий	Температура, °С	23-25	22-28	22-28
	Відносна вологість, %	40-60	55, при 28 °С 75, при 22 °С	70-75
	Швидкість руху, м/с	не більш 0,1	0,1-0,2	не більш 0,2

Як видно з таблиці, фактичні значення параметрів мікроклімату в приміщенні лабораторії відповідають допустимим значенням цих параметрів.

4.2.4 Вимоги до освітлення робочого місця користувачів ВДТ ПЕОМ

Приміщення з ЕОМ повинні мати природне і штучне освітлення відповідно до ДБН В 2.5–28–2006. Природне світло повинно проникати через бічні світло-прорізи, зорієнтовані, як правило, на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1,5%. Розрахунки КПО проводяться відповідно до ДБН В.2.5-28-2006. Приміщення з ВДТ, ЕОМ мають бути оснащені природним і штучним освітленням відповідно до ДБН В.2.5-28-2006. Природне освітлення має здійснюватись через світлові прорізи, які орієнтовані переважно на північ чи північний схід і обладнані регулювальними пристроями відкривання та жалюзями, завісками, зовнішніми козирками.

Приміщення має бічне природне та штучне освітлення, центральне водяне опалення. У приміщенні три вікна розміром 2 х 2,2 м. Штучне освітлення забезпечує чотири люмінесцентних світильники з лампами ЛБ-40, розміщених у ряд.

Отже, усі вимоги до освітлення робочого місця відповідають параметрам освітлення приміщення, де проводяться дослідження.

4.3 Електробезпека

Відповідно до НПАОП 40.1-1.32-01 електроустаткування в робочому приміщенні (крім ВДТ ПЕОМ - II клас та вимірювальної техніки – 0I клас) відноситься до I класу, так як воно має робочу ізоляцію відповідно до НПАОП 40.1-1.32-01 і підключається до електромережі за допомогою трьох контактних вилок, один з виводів яких підключений до заземленого виводу розетки. Підключення устаткування виконане відповідно до вимог НАОП 0.00-1.21-98.

Робоче приміщення нежарке, сухе, відноситься до класу приміщень без підвищеної небезпеки поразки персоналом електричним струмом, оскільки відносна вологість повітря не перевищує 75%, температура не більше 35Cº, відсутні хімічно агресивні середовища, а також відсутня можливість одночасного дотику до металоконструкцій будівлі, що мають контакт із землею, та до струмопровідних елементів електроустаткування. Живлення електроприладів у робочому приміщенні здійснюється від трьохфазної мережі із глухо заземленою нейтраллю напругою 220 В та частотою 50 Гц із використанням автоматів струмового захисту. У приміщенні застосована схема занулення.

Для зменшення значень напруг дотику й відповідних їм величин струму, при нормальному й аварійному режимах роботи електроустаткування необхідно виконати повторне захисне заземлення нульового дроту. Виконаємо електричний розрахунок електромережі на перевірку вимикаючої здатності автоматів струмового захисту.

Розрахунок на вимикаючу здатність, включає визначення значення струму К.З. і перевірку кратності його стосовно номінального струму пристроїв максимального струмового захисту. Вихідні дані для розрахунку:

а) $U_ф$ = 220В - фазова напруга ;

б) кабель чотирьох жильний, матеріал - алюміній(ρ = 0,028 Ом*мм^2/м);

в) відстань від трансформатора до споживача (L) =150м;

г) номінальний струм спрацьовування автомата захисту ($I_{ном}$) =20 А.

Струм однофазного К.З. визначається по формулі:

$$I_{к.з.} = \frac{U_ф}{R_ф + R_0 + \frac{Zm}{3}} = \frac{220}{2{,}3 + 2{,}4 + 2{,}9} = 29\ A.$$

де:$R_ф$ = 2,3 Ом - активний опір фазного проводу;

R_0 = 2,4 Ом - активний опір нульового проводу;

$Z_т$ = 8,72 Ом - розрахунковий опір трансформатора потужністю 250 Вт.

Кратність струму однофазного короткого замикання стосовно номінального струму спрацьовування автомата захисту для надійної роботи має задовольняти нерівність ($K_м \geq 1{,}4$). Практичне значення $K_м$ становить:

$$K_м = \frac{I_{к.з.}}{I_{ном}} = \frac{29}{20} = 1{,}45$$

Отримане значення $K_{м.доп} \geq 1{,}4$.

З розрахунків видно, що при однофазному К.З. автомат струмового захисту буде надійно спрацьовувати.

При однофазному К.З. максимальне значення напруги яка появиться на корпусі при аварійному режимі за час спрацювання максимального струмового захисту, $U_{max.}$ щодо землі: $U_{max.} = I_{к.з.} \cdot R_0 = 29 \cdot 2{,}4 = 69{,}6$ В. Ця напруга менша $U_{доп}$ =500 В ($t_{дії} < 0{,}1$ сек.) згідно з «Санітарно-гігієнічними нормами допустимої напруженості електростатичного поля». №1757-77.

З метою зниження $U_{max.}$ як у нормальному, так і в аварійному режимі варто використовувати повторне заземлення нульового дроту.

4.4 Безпека в надзвичайних ситуаціях

Технічні рішення та організаційні заходи щодо забезпечення безпеки в надзвичайних ситуаціях регламентуються планами локалізації та ліквідації аварійних ситуацій (ПЛАС) відповідно до вимог ДНАОП 0.00-4.33 -99. Однією з основних складових ПЛАС є розробка технічних рішень та організаційних заходів щодо оповіщення та дій, евакуації персоналу у разі виникнення надзвичайних ситуацій.

Відповідно до НАПБ А.01.003-2009 робоче приміщення лабораторії відноситься до категорії В по вибухо-пожежній небезпеці. Відповідно до НПАОП 40.1-1.32-01 клас робочих зон приміщення лабораторії по пожежонебезпеці - П-IIа. Можливими причинами пожежі в приміщенні є несправність електроустаткування, коротке замикання проводки, і порушення протипожежного режиму (використання побутових нагрівальних приладів, паління). У зв’язку з цим, відповідно до вимог ПБЕ та ПУЕ, необхідно передбачити наступні заходи:

1. Ретельну ізоляцію всіх струмоведучих провідників до робочих місць, періодичний огляд та перевірку ізоляції.

2. Строге дотримання норм протипожежної безпеки на робочих місцях.

3. Відповідні організаційні заходи (заборона паління, інструктаж).

Приміщення обладнане чотирма пожежними датчиками типу ДТЛ (площа, що знаходиться під захистом одного датчика, становить 15 м2), відстань між датчиками рівна 4 м, що відповідає нормам ДБН В.2.5-56:2014. Відповідно до ДСТУ Б В.1.1-36:2016 та ДБН В.2.5-56:2010 для гасіння пожежі в робочому приміщені лабораторії (клас пожежі „Е”- наявність електрообладнання під напругою) використовуються два вогнегасники вуглекислотно-брометиленові ВВБ-3. Вибір вогнегасної речовини ґрунтується на тому, що у вогні можуть опинитись електричні пристрої, що знаходяться під напругою.

Кількість та розміщення первинних засобів гасіння пожеж також цілком задовольняють всім вимогам ДСТУ Б В.1.1-36:2016. Крім того, у коридорі є 2

пожежних крана і ящик з піском. Дотримано усіх заходів безпеки відповідно до ДСТУ Б В.1.1-36:2016 та НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні».

Табл. 4.4. Характеристики і норми евакуаційних виходів

Параметр	Фактичне значення	Норма
Висота дверних прорізів	2,0 м	Не менше 2 м
Ширина дверних прорізів	1,5 м	Не менше 0,8 м
Ширина проходу для евакуації	Більше 1,5 м	Не менше 1 м
Ширина коридору	3 м	Не менше 2 м
Число виходів з коридору	2	Не менше 2
Ширина сходової клітки	1,5 м	Не менше 1 м
Висота поруччя сходів	1 м	Не менше 0,9 м

Дотримано усі вимоги НАПБ А.01.003-2009 по вогнестійкості будинку і ширині евакуаційних проходів і виходів із приміщень назовні. Значення основних параметрів шляхів евакуації приведені в таблиці 6.4.

Визначимо час евакуації із лабораторії співробітників при виникненні пожежі в будинку по методиці приведеній в ДСТУ Б В.1.1-36:2016. Будівля п’ятиповерхова, має розміри 15х35 м, в коридорах шириною 2 м є схеми евакуації людей при пожежі. Кабінет об'ємом 140 м3 розташований на другому поверсі в безпосередній близькості від сходової клітки, що веде на перший поверх. Сходові клітки мають ширину 1,5 м і довжину 10 м. У кабінеті працює 5 осіб. Всього на поверсі працюють 50 чоловік. На першому поверсі працює 30 чоловік. Схема евакуації з будівлі представлена на рисунку 4.1.

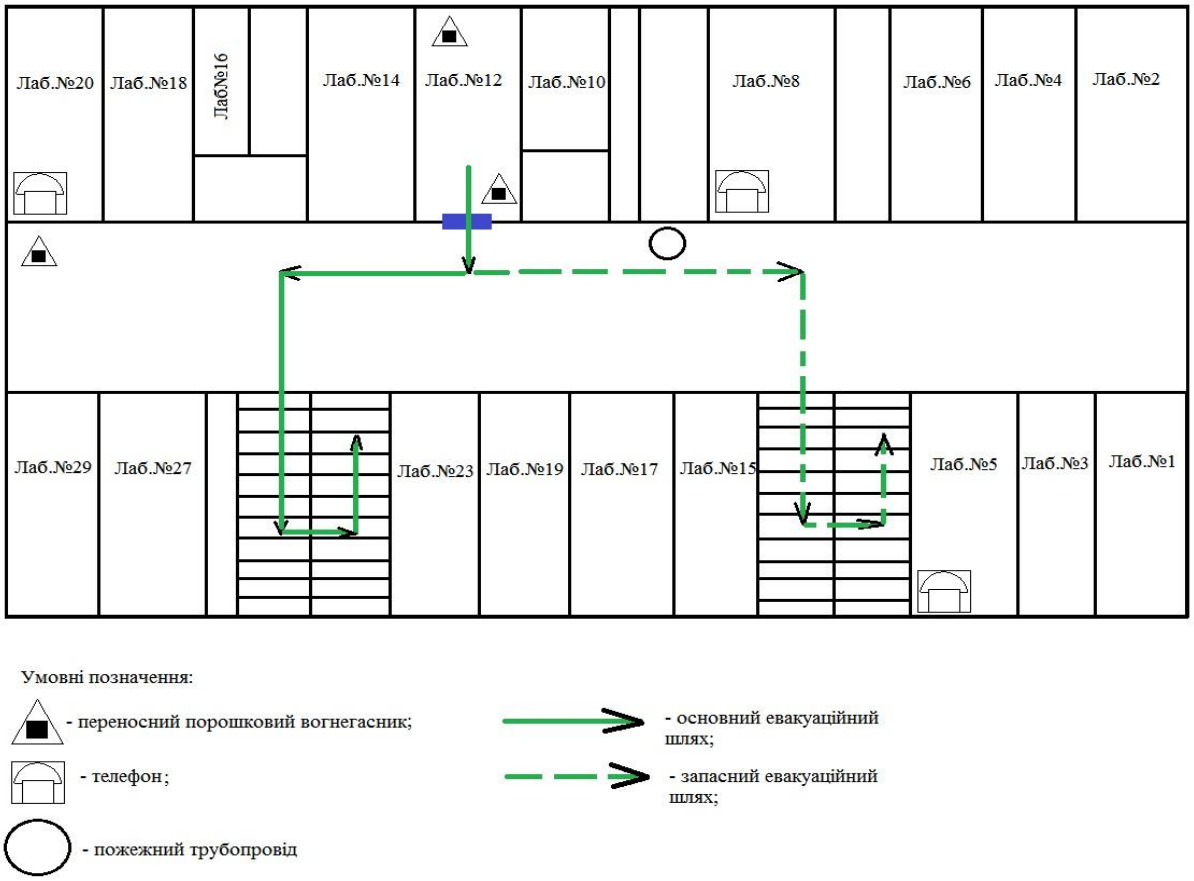

Рисунок 4.1 – Схема евакуації співробітників із лабораторії

Критична тривалість пожежі по температурі розраховується з урахуванням меблів у приміщенні:

$$t_{кр\,j}^{T}=\left\{\frac{B}{A_j}\cdot\ln\left[1+\frac{70-t_0}{(273+t_0)\cdot z}\right]\right\}^{1/n_j}$$

$$\tau_{n.k.}=\left\{\frac{350}{5{,}59\cdot10^{-5}}\cdot\ln\left[1+\frac{70-20}{(273+20)\cdot 2.979}\right]\right\}^{\frac{1}{3}}=1.17\ \text{хв.}$$

Критична тривалість пожежі по концентрації кисню:

$$t_{кр\,j}^{O_2}=\left\{\frac{B}{A_j}\cdot\ln\left[1-\frac{0,044}{\left(\frac{B\cdot L_{O_2}}{V}+0,27\right)\cdot z}\right]^{-1}\right\}^{1/n_j}$$

$$\tau_{n.k.} = \left\{ \frac{350}{5{,}59 \cdot 10^{-5}} \cdot \ln \left[1 - \frac{0.044}{\left(\frac{350 \cdot 1.15}{140} + 0.27 \right) \cdot 2.979} \right] \right\}^{\frac{1}{3}} = 7.55 \text{ хв.}$$

Мінімальна тривалість пожежі по температурі становить 1,17 хв. Допустима тривалість евакуації для даного приміщення:

$$t_{доп} = K_б \cdot t_{кр} = 1 \cdot 1.17 = 1.17 \text{ хв.}$$

Розрахунковий час евакуації людей слід визначати як суму часу руху потоку людей по окремим ділянкам шляху за формулою:

$$t_p = t_1 + t_2 + t_3 + ... + t_i ,$$

де t_1 – час руху потоку людей на першій (початковій) ділянці, хв.;

t_2, t_3, …, t_i – час руху потоку людей на кожному наступному із наступних після першої ділянки шляху, хв.;

Для визначення часу руху людей на першій ділянці, з урахуванням габаритних розмірів кабінету 5х7 м, визначається щільність руху людського потоку на першій ділянці:

$$D_1 = \frac{N_1 \cdot f}{L_1 \cdot b_1} = \frac{5 \cdot 0{,}1}{5 \cdot 7} = 0{,}014 \quad м^2 / м^2 .$$

Швидкість руху складає 100 м/хв, інтенсивність руху 1 м/хв, тобто час руху на першій ділянці:

$$t_1 = \frac{L_1}{V_1} = \frac{7}{100} = 0{,}07 \ хв.$$

Довжина дверного прорізу приймається рівною нулю. Найбільша можлива інтенсивність руху в прорізі в нормальних умовах q_{max}=19,6 м/хв, інтенсивність руху в прорізі шириною 1,5 м:

$$q_d = 2{,}5 + 3{,}75 \cdot b = 2{,}5 + 3{,}75 \cdot 1{,}5 = 8{,}125 \ м/хв.$$

$q_d \le q_{max}$ тому рух через проріз проходить безперешкодно.

Час руху в прорізі:

$$t_{d1} = \frac{N \cdot f}{q_d \cdot b} = \frac{5 \cdot 0{,}1}{8{,}125 \cdot 1{,}5} = 0{,}041 \text{ хв.}$$

Так як на другому поверсі працює 50 чоловік, щільність людського потоку другого поверху складе:

$$D_2 = \frac{N_2 \cdot f}{l_2 \cdot b_2} = \frac{50 \cdot 0{,}1}{30 \cdot 3} = 0{,}056 \text{ м}^2 / \text{м}^2.$$

Швидкість руху становить 100 м/хв, інтенсивність руху 5 м/хв, тобто час руху на другій ділянці (з коридору на сходи):

$$t_2 = \frac{L_2}{V_2} = \frac{30}{100} = 0{,}3 \text{ хв.}$$

Для визначення швидкості руху по сходах розраховується інтенсивність руху на третій ділянці:

$$q_i = \frac{q_{i-1} \cdot b_{i-1}}{b_i} = \frac{5 \cdot 3}{1{,}5} = 10 \text{ м / хв.}$$

Це показує, що на сходах швидкість людського потоку знижується до 70 м/хв. Час руху по сходах вниз (третя ділянка):

$$t_3 = \frac{L_3}{V_3} = \frac{10}{70} = 0{,}143 \text{ хв.}$$

При переході на перший поверх відбувається змішування з потоком людей, що рухаються по першому поверху. Щільність людського потоку для першого поверху:

$$D_4 = \frac{N_4 \cdot f}{L_4 \cdot b_4} = \frac{30 \cdot 0{,}1}{30 \cdot 3} = 0{,}033 \text{ м / хв.}$$

При цьому інтенсивність руху складе близько 5 м/хв.

При переході на четверту ділянку відбувається злиття людських потоків, тому інтенсивність руху буде такою:

$$q_i \frac{\sum q_{q-1} \cdot b_{i-1}}{b_i} = \frac{(16 \cdot 1{,}5) + (5 \cdot 3)}{3} = 13 \text{ м / хв.}$$

Швидкість руху дорівнює 50 м/хв, тому швидкість руху по коридору першого поверху:

$$t_4 = \frac{L_4}{V_4} = \frac{30}{50} = 0{,}6 \text{ хв.}$$

Тамбур при виході на вулицю має довжину 5 метрів, на цій ділянці утворюється максимальна щільність людського потоку тоді швидкість падає до 15 м / хв, а час руху по тамбуру складе:

$$t_5 = \frac{L_5}{V_5} = \frac{5}{15} = 0{,}3 \text{ хв.}$$

При максимальній щільності людського потоку інтенсивність руху через дверний проріз на вулицю шириною більше 1,6 м - 8,5 м/хв, час руху через нього:

$$t_{d2} = \frac{N \cdot f}{q \cdot b} = \frac{80 \cdot 0{,}1}{8{,}5 \cdot 2} = 0{,}471 \text{ хв.}$$

Розрахований час евакуації:

$$t_p = t_1 + t_{d1} + t_2 + t_3 + t_4 + t_5 + t_{d2} = 0{,}07 + 0{,}041 + 0{,}3 + 0{,}143 + 0{,}6 + 0{,}3 + 0{,}471 = 1{,}925 \text{ хв.}$$

Таким чином, розрахунковий час евакуації з лабораторії більше допустимого. Тому будівлю, у якій розташована лабораторія, необхідно обладнати системою оповіщення про пожежу та засобами автоматичної сигналізації.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

1. У роботі були розглянуті тенденції розвитку GSM-систем охорони, основні технічні характеристики стільникових мереж стосовно систем охорони. Були зроблені технічно обґрунтовані висновки про те, що GSM-системи є найбільш оптимальними серед інших радіо-канальних систем для використання.

2. Зроблено висновок, що вкрай ефективним є використання GSM-каналу у поєднанні з іншими каналами передачі сповіщень.

3. Був проведений аналіз основних функцій GSM-мереж, їх використання у системах охорони. Було проведено дослідження швидкості передачі даних та пропускної спроможності GSM каналу.

4. Розраховано середню зону покриття базової станції GS-900 та навантаження на стільнику, на підставі чого зроблено висновок про достатню надійність для охорони дачного селища.

5. Сформульовано ряд рекомендацій по покращенню технічних характеристик систем безпеки, які використовують GSM-канали. На їх основі логічним висновком є те, що існують можливі шляхи розвитку безпровідних систем охорони.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Поширення земних радіохвиль та мобільний зв’язок / Л. М. Логачова, Т. І. Бугрова / Навчальний посібник. – Запоріжжя: ЗНТУ, 2019. – 236 с.

2. Системы и сети передачи информации: Учеб. пособие для вузов / М.В. Гаранин, В.И. Журавлев, С.В. Кунегин. - М.: Радио и связь, 2001. - 336 с.

3. Захист інформації в комп’ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.

4. Кирилов В.И. Многоканальные системы передачи: учебник / В.И. Кирилов. - 2-е изд. - М.: Новое знание, 2003. - 751 с.: ил.

5. [Текст] : конспект лекцій з дисципліни “Основи теорії передавання та кодування інформації” для студ. радіотехнічного ф-ту / Уклад. Г.І. Бондаренко - К.: НТУУ "КПІ", 2019. – 307 с.

6. Тепляков И.М. Основы построения телекоммуникационных систем и сетей: учебное пособие / И.М. Тепляков. - М.: Радио и связь, 2004. - 328 с.: ил.

7. Системи рухомого зв’язку. Навчальний посібник / О. О. Семенова, А. О. Семенов, В. С. Бєлов. – Вінниця: ВНТУ, 2017. – 185 с.

8. Антенно-фидерные устройства и распространение радиоволн: учебник для вузов / Г.А. Ерохин, О.В. Чернышов, Н.Д. Козырев, В.Г. Кочержевский; под. ред. Г.А. Ерохина. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2004. - 491 с.: ил.

9. Системы мобильной связи: учебное пособие для вузов / В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов; под ред.В.П. Ипатова. - М.: Горячая линия - Телеком, 2003. - 272 с., ил.

10. Карташевский В.Г. Сети подвижной связи / В.Г. Карташевский, С.Н. Семенов, Т.В. Фирстова. - М.: Эко-Трендз, 2001.

11. Телекомунікаційні мережі рухомого (мобільного) зв’язку загального користування. Телекомунікаційні послуги. Показники якості. Методи випробування СОУ 64.2–00017584–006:2009 / Державне підприємство «Український державний центр радіочастот»; Товариство з обмеженою відповідальністю "Науково-дослідний інститут Радіо"; Приватне підприємство «Ай Бі Консалтінг» - В.Корсак (науковий керівник); І. Гепко, док. техн. наук; Є. Свиридов, канд. техн. наук

12. Ксенофонтов С.Н. Направляющие системы электросвязи: учебное пособие для вузов / С.Н. Ксенофонтов, Э.Л. Портнов. - М.: Горячая линия - Телеком, 2004, - 268 с.: ил.

13. ДСТУ 3254-94. Радіозв’язок. Терміни та визначення.

14. Ратынский М.В. Основы сотовой связи / М.В. Ратынский. - М.: Радио и связь, 1998.

15. Бова Н. Т., Резников Г. Б.. Антенны и устройства СВЧ. — К. : Вища школа, 1982. — 272 с.

16. Адрианов В.И. Средства мобильной связи / В.И. Адрианов, А.В. Соколов. - СПб.: BHV - Санкт-Петербург, 1998.

17. Системы и сети передачи информации: Учеб. пособие для вузов / М.В. Гаранин, В.И. Журавлев, С.В. Кунегин. - М.: Радио и связь, 2001. - 336 с.

18. Закон України від 18.11.2003 № 1280-IV «Про телекомунікації».

19 БВН В.2.5-78.11.01-2003 «Системи сигналізації охоронного призначення»

20 ГСТУ 78.11.001-98 «Укріпленість об’єктів, що охороняються за допомогою пультів централізованого спостереження Державної служби охорони. Загальні технічні вимоги»

21 ГОСТ 26342-84 «Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры».

22. https://uk.wikipedia.org/

23. http://p-sec.eu/

24. http://biss.ua/
25. https://www.satel.pl/
26. https://seatest.org/

Додаток А

ЗАТВЕРДЖЕНО
ВО завідувача кафедри РОС
РТФ НТУУ «КПІ»

_____А.В. Мовчанюк

«_____»._____ 2020 р

ТЕХНІЧНЕ ЗАВДАННЯ
на дипломну роботу

«СИСТЕМИ БЕЗПЕКИ, ЯКІ ВИКОРИСТОВУЮТЬ GSM КАНАЛИ»

Київ 2020

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота виконується на підставі наказу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» №_____ від _____

2 МЕТА І ПРИЗНАЧЕННЯ НДР

Метою роботи є розробка пропозицій щодо підвищення ефективності систем безпеки що використовують канали передачі систем мобільного зв’язку.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ НДР

При проведенні роботи повинні виконуватися вимоги

БВН В.2.5-78.11.01-2003 «Системи сигналізації охоронного призначення»,

ГСТУ 78.11.001-98 «Укріпленість об’єктів, що охороняються за допомогою пультів централізованого спостереження Державної служби охорони. Загальні технічні вимоги;

ГОСТ 26342-84 «Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры».

4 ВИКОНАВЦІ НДР

Виконавець роботи - студент групи РА-г61-1 Павленко Богдан Вікторович

5 ВИМОГИ ДО ВИКОНАННЯ НДР

При виконанні роботи повинні бути виконані:

5.1 Огляд існуючих систем безпеки, які використовують GSM канали.

5.2 Аналіз завадостійкої і завадо-захищеності GSM каналу.

5.3 Дослідження швидкості передачі даних і пропускної спроможності GSM каналу.

5.4 Аналіз моделі GSM каналу по забезпеченню необхідної зони покриття.

5.5 Розробка рекомендацій по поліпшенню технічних характеристик систем безпеки, які використовують GSM канали.

5.6 Розгляд питань безпеки життєдіяльності функціонування систем безпеки, які використовують GSM канали.

6 ЕТАПИ НДР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№ п.п.	Стадії розробки	Терміни виконання	Форма завершення стадії
1	Розробка технічного завдання	15.05.2020 р.	Текст технічного завдання
2	Розробка основних розділів звіту	01.06.2020 р.	Текст звіту
3	Розробка розділу з охорони праці	12.05.2020 р.	Текст розділу з охорони праці
4	Розробка презентації для захисту роботи	05.06.2020 р.	Презентація у форматі PowerPoint
5	Представлення матеріалів роботи на рецензію	10.06.2020 р.	Комплект матеріалів по роботі
6	Захист роботи на засідання ЕК	15-16.062020 р.	Захист роботи

7 МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІД ЧАС ЗАКІНЧЕННЯ НДР ТА ЇЇ ЕТАПІВ

По закінченні роботи подаються:

7.1 звіт (пояснювальна записка);

7.2 презентація у форматі PowerPoint.

9 ПОРЯДОК ПРИЙМАННЯ НДР ТА ЇЇ ЕТАПІВ

Приймання роботи проводиться відповідно до «Положення про випускну атестацію студентів КПІ імені Ігоря Сікорського» Затверджено Вченою радою КПІ ім. Ігоря Сікорського (протокол № 2 від 12.02.2018 р.).

10 ВИМОГИ ДО РОЗРОБЛЕННЯ ДОКУМЕНТАЦІЇ

Матеріали, що подаються до захисту повинні відповідати:

ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»,

ГОСТ 2.105-95. «Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам»,

ГОСТ 2.301. «Межгосударственный стандарт. Единая система конструкторской документации. Форматы».

Виконавець	Керівник
_____Павленко Б.В.	_____ст. вик. Бондаренко Г.І.

Додаток Б

МОДЕЛЬ ХАТА РОЗРАХУНОК ЗОНИ ПОКРИТТЯ БС СТАНДАРТУ GSM-900

Необхідно розрахувати зону покриття, БС стандарту GSM-900, у великому місті з щільністю забудови 35%, виходячи з вимоги забезпечення належної якості сигналу.

Умова:

$f = 900$ МГц

$H_{bs} = 32$ м

$h_{as} = 1{,}7$ м

Розрахунок:

$$\beta_1 = (0{,}7 - 1{,}11\lg(900)) \cdot 1{,}7 + 1{,}56\lg(900) - 0{,}8 = -0{,}526\ ;$$

$$\beta_2 = 1{,}1 - 8{,}29lg^2(1{,}542 \cdot 1{,}7) = -0{,}348\ ;$$

$$\beta_3 = 4{,}97 - 3{,}2lg^2(11{,}75 \cdot 1{,}7) = -0{,}442\ ;$$

$$F_1 = \frac{300^4}{900^4 + 300^4} = 0{,}012\ ;$$

$$F_2 = \frac{900^4}{900^4 + 300^4} = 0{,}988\ ;$$

$$\alpha(h_{as}) = (1-1)\beta_1 + 1 \cdot (\beta_2 F_1 + \beta_3 F_2) =$$

$$-0{,}348 \cdot 0{,}012 - 0{,}442 \cdot 0{,}988 = -0{,}441$$

$\alpha(U_r) = 0$, для міста $(U_r = 1)$;

$\alpha(b) = 25\lg(35) - 30 = 8{,}6$

$$\alpha(H_{bs}, f) = \left(27 + \frac{900}{230}\right) lg\frac{17(32+20)}{17(32+20) + r^2} + 1.3 - \frac{900-55}{750} =$$

$$30{,}9\lg\left(1 + \frac{r^2}{884}\right)^{-1} + 0{,}17$$

Середній рівень втрат на радіотрасі:

$$L = 69{,}55 + 26{,}16\lg(900) - 13{,}82\lg(32) + [44{,}9 - 6{,}55\lg(32)]\lg(r) - 0{,}441$$
$$+ 8{,}6 + 30{,}9\lg\left(1 + \frac{r^2}{884}\right)^{-1} + 0{,}17, (\partial Б)$$

$$L = 134{,}65 + 35\lg(r) + 30{,}9\lg\left(1 + \frac{r^2}{884}\right)^{-1}, (\partial Б)$$