Хмельницький національний університет
Факультет інформаційних технологій
Кафедра автоматизації та комп'ютерно-інтегрованих технологій

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Пристрій обмеження доступу до об'єктів
інфраструктури із застосуванням телекомунікаційних мереж
Назва теми

КвРТР.2019032.01.11 ПЗ

Галузь знань 17 «Електроніка та телекомунікації»
Шифр, назва
Спеціальність 172 «Телекомунікації та радіотехніка»
Шифр, назва
Освітня програма «Телекомунікації та інформаційно-комунікаційні технології»
Шифр, назва

Виконав:

студент IV курсу, група ТР1с-19 _____ Ярослав Шаламай
Підпис — Ім'я, ПРІЗВИЩЕ

Керівник _____ Олександр ЯНОВИЦЬКИЙ
Підпис, дата — Ім'я, ПРІЗВИЩЕ

Нормоконтролер _____ Людмила КОРЕЦЬКА
Підпис, дата — Ім'я, ПРІЗВИЩЕ

До захисту допускаю:
зав. кафедри автоматизації
та комп'ютерно-інтегрованих
технологій _____ Валерій МАРТИНЮК
Підпис, дата — Ім'я, ПРІЗВИЩЕ

«13» червня 2022 р.

Хмельницький 2022

Хмельницький національний університет

Факультет інформаційних технологій
Кафедра автоматизації та комп'ютерно-інтегрованих технологій
Освітній рівень бакалавр
Галузь знань 17 «Електроніка та телекомунікації»
Шифр, назва
Спеціальність 172 «Телекомунікації та радіотехніка»
Шифр, назва
Освітня програма «Телекомунікації та інформаційно-комунікаційні технології »
Шифр, назва

ЗАТВЕРДЖУЮ
Зав. кафедри Мартинюк В.В.
«01» 03 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ярославу ШАЛАМАЮ

1 Тема проєкту Пристрій обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж
керівник проєкту Олександр ЯНОВИЦЬКИЙ, кт.н., доцент
Затверджено наказом ректора університету від "01" 03 2022 р. № 18
2 Строк подання студентом проєкту на кафедру «01» 06 2022 р.
3 Вихідні дані до проєкту
Анотація. Вступ. Техніко-економічне обґрунтування доцільності розробки. Аналіз існуючих методів та засобів. Розробка структурної схеми. Електричні розрахунки. Комп'ютерне моделювання. Розрахунок надійності пристрою. Висновки. Список літератури. Додатки.
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
1. Вступ. 2. Розгляд тематики та економічне обґрунтування доцільності розробки блоку системи обмеження доступу. 3. Розробка структурної схеми пристрою. 4. Електричний розрахунок

Завдання отримав
Науковий керівник

Консультанти розділів кваліфікаційної роботи

Розділ	Ім'я, ПРІЗВИЩЕ та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
Антиплагіат	Микола ФЕДУЛА, к.т.н., доцент		
Нормоконтроль	Людмила КОРЕЦЬКА, к.т.н., доцент		

ПЛАН ІНДИВІДУАЛЬНОЇ РОБОТИ

№ п/п	Найменування виду роботи	Форма звітності, термін виконання	Відмітка наукового керівника
1	Вступ	15.02.2022	Виконано
2	Огляд літератури, аналіз доцільності розробки	15.03.2022	Виконано
3	Розробка структури пристрою	10.04.2022	Виконано
4	Розробка схеми електричної принципової та розрахунки	10.05.2022	Виконано
5	Висновки	15.05.2022	Виконано
6	Оформлення пояснювальної записки до КРБ	25.05.2022	Виконано
7	Оформлення презентаційних матеріалів	01.06.2022	Виконано

Студент _____ Ярослав ШАЛАМАЙ
(підпис, дата)

Науковий керівник _____ Олександр ЯНОВИЦЬКИЙ
(підпис, дата)

Зміст

КВРТР.2019032.01.11 ПЗ

Зм.	Арк.	№ докум.	Підпис	Дата
Виконав		Ю. Шевчук		
Перевір.		О. Новицький		
Н.контр.				
Н.контр.		Куцевол		
Затверд.		В.В. Мартинюк		

Пристрій обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж
Пояснювальна записка

Літера	Аркуш	Аркушів
	2	

ТРТКС-19, ФІТ, КНУ

ВСТУП

Охоронні системи з’явились дуже давно. Людина завжди намагалась зберегти свою власність. Спочатку це були найпростіші засоби, наприклад надлишок їжі первісні люди ховали в містях недоступних іншим племенам, в середні часи створювались різноманітні таємні сховища, та людську варту. Згодом системи охорони вдосконалювались і досягли сучасного рівня.

В сучасних системах використовуються величезна кількість засобів охорони. Це різноманітні датчики виявлення руху на охороняємо му обкті, датчики відкривання, датчики розбивання скла.

Останнім часом широко розповсюджуються системи стільникового зв’язку. Охоронні системи також не залишились в стороні. Адже завжди було великою проблемою реалізації передачі сповіщень від охоронних систем до центру моніторингу, або до власника об’єкту за умови відсутності дротяної телефонної мережі, яка часто використовувалась для цих цілей. Тому розробники охоронних систем просто немогли не використати принцип стільникового зв’язку в своїх розробках.

Стільникові системи зв’язку надають величезні можливості для створення систем нового зразка. Перевагою таких систем є моніторинг охороняємого об’єкту безпосередньо власником зі свого стільникового телефону, а канал передачі даних надає унікальну можливіст створення систем з передачою швидкісних кодованих протоколів обміну для реалізації пультової охорони.

Вже зараз в країну, у зв'язку з попитом, що підвищується, ввозяться західні зразки, проектуються оригінальні вітчизняні охоронні пристрої.

Матеріальний збиток при пожежах набагато перевершує збитки від розкрадань. Охоронні системи майже завжди містять протипожежні датчики і сповіщають про спалах.

Системи телевізійного спостереження за допомогою телекамер дозволяють отримати на телевізійних або комп'ютерних моніторах оброблене

відеозображення від різних точок об'єкту, що охороняється. Найпростіші індивідуальні системи - відеодомофони. Складні - системи обробки відеоінформації поєднують функції систем телевізійного спостереження і охоронних систем.

До охоронних систем відносять також технічні засоби несанкціонованого доступу. Оцінка можливої загрози проводиться на підставі життєвого досвіду, об'єктивних і суб'єктивних чинників. При цьому слід враховувати територіальне розташування, криміногенну обстановку в районі.

Достатньо багато випадків, коли надійні, неправильно встановлені технічні засоби, неправильне їх використовування або відсутність, дозволяють злочинцям проникати в будинки, офіси або квартири.

Офіси у багатьох випадках розташовуються на перших поверхах будівель. При неправильно встановлених гратах, слабих дверях або замку, навіть за наявності сигналізації, за 1,5...2 хвилини можуть винести оргтехніку. При цьому втрачається інформація, яка може представляти інтерес для злочинців і конкурентів.

У разі відсутності сигналізації або охорони злочинці безперешкодно відкривають двері або вікно, особливо, в погано освітлених місця.Коли не вдається відключити сигналізацію, зірвавши або відігнувши грати, вони розбивають вікно і проникають в приміщення. Однієї-двох хвилин виявляється достатньо, щоб винести декілька комп'ютерів.

Злочинці використовують як підручні засоби, так і спеціальні. Їх винахідливості немає межі. Вони знаходять можливість підключення електроінструментів. Під час пограбування блокують сусідні двері з тим, щоб їх не застали на місці злочину. Замість сходів вони можуть використовувати частину огорожі, ящики або бочки. Як лом - шматок арматури або водопровідної труби і так далі.

Діям злочинців, спільно з технічними засобами, слід протиставити ряд організаційних заходів.

Досвід показує, що середнє значення витрат на охорону матеріальних цінностей звичайно не перевищують десяти відсотків їх вартості.

Організаційні заходи не вимагають великих матеріальних витрат, але їх ефективність підтверджена життям і часто недооцінюється потенційними жертвами.

Відзначимо їх одну відмітну особливість порівняно з технічними засобами: організаційні заходи ніколи не стають провокуючим чинником агресії. Вони застосовуються до зіткнення із злочинцем. Останній не може скористатися їх перевагами, як у випадку, наприклад, самооборони із застосуванням зброї.

Дотримання основних принципів і простих правил дозволить запобігти можливому матеріальному, моральному збитку, фінансовим втратам і інцидентам на роботі і удома.

Потенційні жертви недооцінюють важливість організаційних заходів. Відбувається це тому, що їх виконання не можна здійснити технічними засобами.

До організаційних заходів відносяться:

- оцінка можливої загрози;

- вибір заходів по охороні квартири, дома, автомобіля, службових приміщень;

- вибір режиму роботи;

- підбір кадрів і т.д.

Одного з перших організаційних заходів, яку здійснює кожний різною мірою - оцінка можливої загрози. Робити це краще не чекаючи пограбування. З такою оцінкою стикається кожна людина при отриманні квартири, виборі приміщення під офіс, склад і т.д. Ступінь загрози визначається наявністю цінностей.

Цінності, вимагаючі охорони, можуть бути матеріальними і нематеріальними. До нематеріальних цінностей відноситься, наприклад, інформація.

При захисті приміщень задачу слід вирішувати комплексно, щоб не переробляти кілька разів дизайн приміщення і комунікації. Всі системи повинні встановлюватися з урахуванням наступних чинників:

- забезпечення надійності;
- забезпечення вартості;
- зручності використання;
- можливого їх впливу один на одного;
- можливість модернізації.

Відмітимо, що навіть пограбування не завжди надихає потерпілих і їх сусідів встановити сигналізацію. В більшості випадків обмежуються мінімальними додатковими заходами. Якщо обмежитися тільки зміцненням дверей і грат, це не захищає від повторних "відвідин".

При пограбуванні, що вдалося, злочинці час від часу спостерігають за потерпілим і через, наприклад, півроку.

Не слід забувати про протипожежну безпеку. Статистика показує, що втрати від пожеж значно перевершують збитки від розкрадань.

Найбільш гнучкими, не вимагаючими прокладки комунікацій, є безпроводні системи. Це можуть бути охоронні, протипожежні пристрої і системи телевізійного спостереження.

Організаційні заходи зв'язують в єдине ціле всі складові безпеки. Правильність вибору і проведення організаційних заходів визначає ступінь безпеки.

1 РОЗГЛЯД ТЕМАТИКИ ТА ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ БЛОКУ СИСТЕМИ ОБМЕЖЕННЯ ДОСТУПУ

1.1 Склад системи обмеження доступу

Система контролю та управління доступом зазвичай складається (див. [2]) із серверів системи обмеження доступу (СКУД) – звичайних комп'ютерів, які управляють підключеними до них контролерами СКУД. Контролер (контрольна панель) – це спеціалізований високонадійний комп'ютер. У ньому зберігається інформація про конфігурацію, режими роботи системи, список людей, які мають право доступу до ресурсу, а також їх привілеї доступу до цього ресурсу. У найпростіших випадках мінімальний варіант контролера може бути вбудований у зчитувач, турнікет, замок або інший виконавчий пристрій.

Наступною важливою ланкою СКУД є такі пристрої, як зчитувачі, які можна підключити до контролерів. Зчитувач є пристроєм, який дозволяє зчитувати інформацію, записану на картці. Цю інформацію він передає контролеру, який приймає рішення про допуск людини до ресурсу. Можна налаштувати контролер так, що він запитуватиме підтвердження прийнятого рішення у комп'ютера.

Будь-який зчитувач передбачає частину у відповідь – ключ-ідентифікатор, який містить інформацію, за допомогою якої відбувається ідентифікація людини. Кожній картці приписаний певний рівень доступу, відповідно до якого користувач має право отримати доступ до того чи іншого ресурсу у певний проміжок часу. Класифікація ключів представлена у підрозділі 1.2.

Для підвищення надійності ідентифікації, крім зчитувачів, до контролера може підключатися клавіатура для набору персонального ідентифікаційного номера (ПІН-коду).

Інший тип пристроїв, які можна підключити до контролера, – це охоронні панелі. Це також спеціалізований контролер, який відстежує стан охоронних датчиків (датчики на дверях, вікнах, об'ємні датчики та інші). Якщо стан якого-небудь датчика змінюється, то інформація про це відразу надходить до основного контролера.

У охоронної панелі може бути набір реле, з допомогою яких здійснює управління виконавчими пристроями: електромеханічними замками, турнікетами, ліфтами, автоматичними воротами тощо.

1.2 Способи ідентифікації

Існує два різні напрями в способах ідентифікації. Це ідентифікація з використанням електронних карт, і ідентифікація, що використовує біометричні параметри людини. Зараз застосовуються наступні типи карт, кожному з яких відповідає певний тип зчтувача (см [3]) :

- ***магнітні карти*** - прочитуються, при проведенні в певному напрямі і з певною швидкістю по щілині зчитувача. Магнітна смуга із записаною на ній інформацією нанесена на одну із сторін пластикової картки. Сучасні магнітні смуги виготовлені з матеріалів, що вимагають сильних магнітних полів для запису інформації і, відповідно, для її знищення, тому можна не боятися випадкового розмагнічування. Проте магнітні карти досить чутливі до зовнішніх дій іншого роду - забруднення, вологи, подряпин. Ще один недолік пов'язаний з необхідністю точного позиціонування в зчитувача. Середній термін служби магнітних карт складає близько року, потім магнітний шар стирається. Тому магнітні картки застосовують, як правило, в системах, де передбачена часта заміна карт, наприклад, в готелях або на автостоянках.

- ***безконтактні радіочастотні (PROXIMITY) карти*** - найбільш перспективний на сьогодні тип карт. Безконтактні картки діють на відстані і не вимагають чіткого позиціонування, що забезпечує їх стійку роботу і зручність використання, високу пропускну спроможність. Для прочитування інформації з безконтактної картки її досить просто піднести до зчитувача. Зчитувач генерує електромагнітне випромінювання певної частоти і, при внесенні карти в зону дії зчитувача, це випромінювання через вбудовану в карті антену живить чіп карти. Отримавши необхідну енергію для роботи, карта пересилає на зчитувач свій ідентифікаційний номер за допомогою електромагнітного імпульсу певної форми і частоти. При цьому картка може знаходитися в кишені або в гаманці.

- ***карти Виганда*** - названі по імені вченого, такого, що відкрило сплав, що має прямокутну петлю гістерезису. Усередині карти розміщені відрізки дроти з цього сплаву, які при переміщенні повз прочитуючу голівку дозволяють рахувати інформацію. Ці карти довговічніші, ніж магнітні, але і дорожчі. Один з недоліків - те, що код в карту занесений при виготовленні раз і назавжди.

- ***штрих-кодові карти*** - на карту наноситься штриховий код. Існує складніший варіант - штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, прочитування відбувається в інфрачервоній області.

- ***Touch - memory*** - металева пігулка, усередині якої розташований чіп ПЗП. При торканні пігулки зчитувача, з пам'яті пігулки в контроллер пересилається унікальний код ідентифікатора. Досить дешеві і зручні.

До біометричних способів ідентифікації відносять (детальніше за см в [4]) :

- ***Сканування відбитків пальців*** - сканування відбитків пальців є найзручнішим методом, а вживані при цьому пристрої - найдешевшими. Перевагою є і надійність сканування відбитків пальців : несанкціонований доступ можливий приблизно в одному випадку з мільйона, а відмова в доступі уповноваженому користувачеві виникає приблизно в 3% випадків і пов'язаний в основному з правильним доглядом за сканером.

- ***Геометрія долоні і кисті рук -*** скануються не лінії, як у відбитків пальців, а геометрія руки : форма долоні або кисті, довжина пальців і т. д. В принципі, по надійності цей метод практично не поступається попередньому, але подібні системи займають значно більше місця, що утрудняє їх використання на звичайному комп'ютері, та і коштують вони дорожче.

- ***Сканування ока -*** розрізняють два типи: сканування веселкової оболонки і сканування сітківки. Перший метод простіший і зручніший, але і менш надійний. Другий є найнадійнішим, але і найдорожчим.

- ***Ідентифікація по голосу -*** Перевагою є зручність використання. Але цей метод має низьку надійність, оскільки для того, щоб голос людини значно змінився, досить простудитися.

- ***Підпис -*** людина розписується на спеціальному облаштуванні типу графічного планшета. Комп'ютер порівнює отриману написану інформацію з тією, яка зберігається в його базі, і залежно від результатів порівняння надає доступ або відмовляє в ньому. Сам підпис легко підробити, але сучасні зчитувачі вимірюють ще і характеристики руху руки при письмі, що підвищує надійність методу.

- ***Геометрія особи, Клавіатурний почерк -*** ці методи слабо розроблені, реально діючих систем не існує.

1.3 Принципи роботи систем контролю доступу

У основі роботи систем контролю і управління доступом закладений принцип порівняння тих або інших ідентифікаційних ознак, що належать конкретній фізичній особі або об'єкту, з даними, закладеними в систему [5].

Кожен із співробітників (відвідувачів) отримує карту доступу або брелок, що містить індивідуальний код, що привласнюється при видачі карти доступу у бюро пропусків. В якості коду можуть використовуватися також біометричні дані людини.

При проході на територію, що охороняється, або в приміщення, що охороняється, проводиться прочитування даних з носія коду через зчитувачі. Інформація про відвідувача передається в систему, де проводиться аналіз і дається сигнал, що адекватно реагує на ситуацію, що склалася : <Прохід дозволений>, <Прохід заборонений>, <Повторний прохід по одній карті>, виведення сигналу <Тривога> на пульт охоронця при порушенні території, що охороняється, без відповідних прав і так далі

При необхідності втручання охорони в ситуацію, що склалася, на екран комп'ютера поста охорони виводиться тривожний сигнал і інструкція, що визначає дії персоналу в цій ситуації. Причому, система тут же може відреагувати на тривожну ситуацію, заблокувавши замки в приміщення, що охороняється, і шляхи проходу по точках доступу.

Для аналізу подій, що сталися, є можливість перегляду і роздруку протоколу подій за певний період часу. Для виключення зловживань у використанні карт і посилення прохідного режиму в особливо важливі зони є ряд функцій, що дозволяють : (см [5])

- виключити подвійний прохід в зону по одній карті (розрізняють можливості блокування повторного проходу на певний час - для систем, не обладнаних зчитувачами на виході і заборона на вхід в несуміжну зону для повних систем контролю доступу);
- дозволити доступ тільки після 2-го картам (увійти можуть тільки дві людини, зустрівшись разом і що мають відповідні повноваження);
- обмежити кількість осіб в приміщенні і зоні (при перевищенні встановленого порогового значення контроллер не пропустить в зону чергової людини);
- встановити режим <вхід під примусом> (непомітно для оточення охороні подається сигнал тривоги);
- охоронцеві надається право на самостійне ухвалення рішення про дозвіл на прохід відвідувача (при прочитуванні карти на монітор охоронця

виводиться фотографія власника, яка звіряється із зображенням, що видається відеокамерою);

- встановити режим лічильника на використання карти (кількість читань карти на конкретному зчитувачі обмежується);

- встановити прихований контроль в приміщенні (подати сигнал тривоги на пульт охорони при проникненні в приміщення, що захищається, і відсутності відповідних прав, причому для зловмисника факт виявлення залишається невідомим).

1.4 Класифікація СКУД

Розглянемо деякі важливі класифікації систем контролю і управління доступом, представлені в [6].

Класифікація СКУД за способом управління :

- ***автономні*** - для управління одним або декількома пристроями, що перегороджують, без передачі інформації на центральний пульт і без контролю з боку оператора. Звичайно це прості СКУД, точніше електронні замки, які обмежують доступ в приміщення. До переваг таких систем можна також віднести можливість легкого видалення номера ключа з енергозалежної пам'яті системи при його втраті, таким чином, ключ, що знайшов, ніколи не зможе їм скористатися. Автономні системи знайшли застосування, як правило, на невеликих об'єктах (входи до житлових будинків, котеджі і тому подібне). Існують і автономні системи контролю доступу з функціями охорони.

- ***централізовані*** (мережеві) - для управління пристроями, що перегороджують, за рахунок обміну інформацією з центральним пультом, для контролю (управління) з боку оператора. Мережеві системи контролю застосовуються там, де потрібно постійний контроль стану об'єкту, можливість оперативного втручання в роботу системи і отримання різних статистичних даних про рух персоналу. Управління доступом в мережевих системах в основному здійснюється автоматично, на основі різних об'єктних і тимчасових

обмежень доступу, що задаються як для окремих власників ключів, так і для груп власників, виділених за якою-небудь ознакою за допомогою спеціальної програми. Оператор має можливість працювати з базами цих користувачів, реєструвати і редагувати права доступу. При запущеній програмі усі події, що відбуваються в системі, виводяться на монітор в режимі реального часу і протоколюються для подальшого отримання звітів по кожному користувачеві. Система дозволяє отримати повний набір стандартних звітів про переміщення співробітників, а також вести облік робочого часу. Мережі зв'язку в системі захищені від зловмисників апаратно і програмно. Мережеві системи оптимальні для застосування в невеликих і середніх офісах або підприємствах (до 256 контрольованих точок проходу).

- ***універсальні*** - включаючі функції як автономних, так і мережевих систем, працюючі в мережевому режимі під управлінням центрального облаштування управління і що переходять в автономний режим при виникненні відмов в мережевому устаткуванні, в центральному пристрої або обриві зв'язку.

По кількості контрольованих точок доступу розрізняють:

- системи малої місткості (менше 16 точок);
- системи середньої місткості (не менше 16 і не більше 64 точок);
- системи великої місткості (64 точки і більше).

Класифікація по виду об'єктів контролю :

- для контролю доступу до фізичних об'єктів;
- для контролю доступу до інформації.

1.5 Системи контролю доступу в автоматизації маркетингу

Нині найширше поширено розуміння «системи контролю доступу» як засоби організації контрольно-перепускного режиму на підприємстві. У цих системах в якості користувачів розуміються співробітники підприємства - власника СКУД, і найбільша увага приділяється безпосередньому забезпеченню безпечного доступу в зони і приміщення. Таке використання СКУД, сприяє зменшенню витрат підприємства на організацію безпеки.

Використання систем контролю доступу як засобів автоматизації маркетингу переслідує вже дещо інші цілі: отримання прибутку за рахунок продажу можливості доступу до ресурсу. У цьому сенсі система контролю доступу стає спеціалізованою системою автоматизації маркетингу. Детальніше про карткові системи в автоматизації маркетингу викладено в [7].

У таких системах користувачі розуміються ширше - як підприємства і приватних осіб. Тут вже величезне значення придбаває механізм організації розрахунків цих користувачів з власником СКУД, який зовсім відсутній в первинному розумінні систем контролю доступу, де користувачами виступали співробітники.

Якщо в першому випадку угрупування користувачів затребується лише як засіб зручнішого управління доступом, то в системах автоматизації маркетингу, вона придбаває велику значущість завдяки впровадженню поняття рахунку. Один рахунок може використовуватися як однією людиною, так і групою людей (підприємство, сім'я і ін.) і навіть групою груп (асоціація груп), що задає можливості побудов складних ієрархій.

В цілому розуміння СКУД як системи автоматизації маркетингу можна вважати узагальненням первинного поняття, оскільки уся взаємодія співробітників з системою можна інтерпретувати через механізм рахунків. Наприклад, для співробітників вартість доступу може бути нульовою. Інакше, рахунки природним чином дозволяють оцінювати інтенсивність використання системи цим співробітником.

Системи автоматизації маркетингу навантажують додатковим сенсом і різні звіти, формовані СКУД, дозволяючи на їх основі проводити статистичні дослідження затребуваності ресурсу в конкретній точці доступу. Ці дослідження можуть використовуватися для гнучкого налаштування системи на потреби користувачів. Статистика доступу конкретного користувача або групи дозволяє ефективно стимулювати постійних клієнтів за допомогою різних схем знижок і заохочень.

Використання СКУД відкриває широкі можливості по автоматизації роботи різних готелів, курортів, дискотек і інших установ, що торгують доступом в різні приміщення. Наприклад, система контролю доступу, що автоматизує роботу готелю, дозволяє не лише понизити витрати на забезпечення безпеки, але і організувати платне використання сауни, бару, ресторану або інших сервісів готелю. СКУД гірськолижного курорту може організувати зручний для клієнтів платний доступ до підйомників і так далі.

1.6 Особливості систем контролю доступу, як систем реального часу

В силу своєї специфіки, системи контролю доступу є системами реального часу (СРВ). СРВ, як апаратно-програмний комплекс, включає датчики, що реєструють події на об'єкті, модулі введення-виводу, перетворюючі показники датчиків в цифровий вид, придатний для обробки цих свідчень на комп'ютері, і, нарешті, комп'ютер з програмою, що реагує на події, що відбуваються на об'єкті. Всяка СРВ орієнтована на обробку зовнішніх подій. Її основне завдання - реагувати в передбачувані часи, на непередбачуваний потік зовнішніх подій. Це означає, що система повинна відреагувати на подію, що сталася на об'єкті, своєчасно, тобто впродовж часу, критичного для цієї події. Величина критичного часу для кожної події визначається об'єктом і самою подією, і, природно, може бути різною, але час реакції системи має бути передбачений (вичислено) при створенні системи. Відсутність реакції в передбачений час вважається помилкою для систем реального часу [8].

Окрім цього, система повинна устигати реагувати на події, що одночасно відбуваються. Навіть якщо два або більше число зовнішніх подій відбуваються одночасно, система повинна встигнути зреагувати на кожне з них впродовж тимчасових інтервалів, критичних для цих подій [8]. Розрізняють системи реального часу двох типів - системи жорсткого реального часу і системи м'якого реального часу. Системи жорсткого реального часу не допускають ніяких затримок реакції системи, оскільки:

- результати можуть виявитися даремними у разі запізнення;
- може статися катастрофа у разі затримки реакції;
- вартість запізнення може виявитися нескінченно велика.

Системи м'якого реального часу характеризуються тим, що затримка реакції допустима, хоча і може привести до збільшення вартості результатів і зниження продуктивності системи в цілому. СКУД відносять саме до цього типу систем. Взагалі, основна відмінність між системами жорсткого і м'якого реального часу можна виразити так: система жорсткого реального часу ніколи не спізнюється з реакцією на подію, система м'якого реального часу - не повинна спізнюватися з реакцією на подію.

Розуміння системи контролю доступу як системи реального часу вимагає від розробника використання ряду специфічних механізмів, що роблять істотний вплив на архітектуру усієї системи.

1.7 Суть технічної проблеми, яка виникла на сучасному етапі розвитку науки і техніки

Характерною особливістю останнім часом стала надзвичайна різноманітність предметів розкрадання. Красти стали все: від поношених речей і продуктів харчування до діамантів і дорогої апаратури.

В теперішній час посягання проти власності складають значно більше половини всіх злочинів. Вірогідність стати жертвою злочину для звичайної людини не так вже велика (її можна оцінити, розділивши число жителів на число злочинів). Та оскільки вирогідність така є, то чи варто ризикувати, а потім шукати причини?

Для більшості людей важливо знати мінімальні заходи запобігання злочинів. Основна задача роботи проаналізувати існуючі засоби охорони і розробити охоронну систему на рівні структурних схем.

В роботі описуються організаційні заходи і технічні засоби безпеки. Приводяться відомості про злочини і способи їх здійснення, що часто зустрічаються.

Достатньо багато випадків, коли надійні, але не правильно встановлені технічні засоби дозволяють зловмисникам проникати в будинки, офіси або квартири.

Втрати, які можна понести у разі просочування інформації, можуть перекреслити багаторічні зусилля. Продумати безпеку інтер'єру, способи зберігання цінностей і організувати роботу з конфіденційною інформацією може тільки кожен сам, оскільки схема організаційних заходів є ключем для посягань, а у разі її відсутності - такої перешкоди немає.

Витрати на додаткові захисні пристрої не сумірно малі, порівняно із збитком від одного єдиного злому. Прості пристрої не дорогі, але універсальні. При дотриманні правил використовування, вони дають значний виграш порівняно з людьми, які їх не використовують.

В кожній галузі народного господарства бувають етапи розвитку, при яких потрібен перехід на якісно новий підхід до вирішення проблем, наприклад перехід на нових технологічний процес, запровадження нових систем, станків тощо. Предметом дослідження став блок керування радіоохоронної системи стандарту GSM, що встановлюється на будь-якому охороняємому об’єкті і є серцем усієї системи [1].

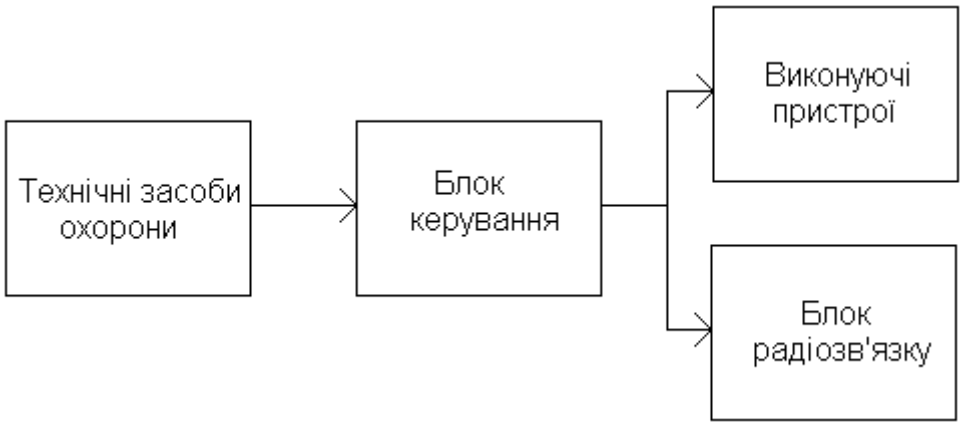


Рисунок 1.1 – Структура класичної побудови радіоохоронної системи

Класична побудова радіоохоронної системи (рисунок 1.1) в загальному вигляді складається з чотирьох частин:

1) Технічні засоби охорони;
2) Блок керування системою;
3) Виконуючі пристрої.
4) Блок радіозв’язку

Існує також два принципи охорони об’єктів:

1) Охорона з передачою сповіщень на пульт спостереження (пульт міліції);
2) Автономна охорона без передачі сповіщень.

При автономній охороні використовуються виконуючі пристрої місцевого оповіщення, такі як сирени, ревуни, індикаторні табло та світлові оповіщувачі, що знаходяться беспосередньо на охороняємому об’єкті. Досить тривалий час при застосуванні принципу охорони з передачою сповіщень, використовувались телефонні лінії зв’язку, а це має ряд суттєвих недоліків. Поперше уразливість дротів, мала швидкість передачі інформації і як наслідок низька інформативність. Всіх цих недоліків можна позбутися завдяки використанню поширеного стільникового радіозв’язку стандарту GSM.

1.8 Обґрунтування і вибір аналогів

Продовж останніх років сформувались основні вимоги до блоків керування охоронними системами:

- контроль датчиків в шлейфах сигналізації;
- керування виконавчими пристроями;
- індикатор постановки під охорону;
- програмування охоронної системи з клавіатури, а також з відстані за допомогою стільникового телефону;

- передача голосових сповіщень про стан датчиків та охоронної системи.

Існує велика кількість різновидів конструктивного та функціонального виконання.

Наприклад, існують виконання, зі встроєним модулем для передачі сповіщень. Перевагою такого виконання є відсутність аккумуляторної батареї стільникового телефону, що збільшує час наробки на відмову.

Також існує тип виконання приладів, що передають сповіщення використовуючи готовий окремий прилад стільниковий телефон, а це підвищує ремонтну здатність приладу у разі виходу з ладу телефону його просто замінюють на новий. Така властивість є важливою, адже ремонт охоронної системи не може тривати тривалий час і мусить виконуватися майже миттєво [2]. Саме такого типу прилад буде розроблятися в дипломному проекті.

Отже, потрібно визначити найближчих конкурентів. Лідерами в області виготовлення охоронних систем з використанням GSM каналу для передачі сповіщень є фірма "Промінь" (Київ), польська компанія „Satel” та ін.. Усі ці фірми відомі на ринку охоронних систем. Усі вони пропонують свої системи, що не тільки відрізняються за технічними характеристиками, алей за ціною. Цілком ймовірно припустити, що для українських споживачів висока ціна приладів буде значним гальмівним фактором. Прилади які виробляються за кордоном можна використати як зразкові і опиратися в подальшому, при розробці приладу.

Для зручного перегляду видимих переваг і недоліків проведемо якісний аналіз аналога і нової розробки, звівши до таблиці основні показники (таблиця 1.1) і проаналізувавши значення і відношення параметрів у якісному куті зору на проблему нової розробки і застосування існуючих аналогів.

Явним конкурентом для нової розробки оберемо прилад зі схожими показниками і характеристиками, що виконує ту ж функцію «GSM GUARD SYSTEM» .

Таблиця 1.1 – Основні технічні параметри аналога і нової розробки

Параметри	Одиниця виміру	Аналог	Нова розробка	Відношення параметрів
Інформаційна ємність	од.	8	4	0,5
Інформативність	од.	4	8	2
Реакція на розрив шлейфу	мс	70	70	1
Керування прибором		Клавіатура	Клавіатура, Телефон	
Кількість груп шлейфів	од	1	1	1
Програмований час затримки	с	10-990	10-990	1
Опір кінцевого резистора	кОм	3±1%	3±1%	1
Величина напруги в черговому режимі	В	8-12	8-12	1
Величина струму в черговому режимі	мА	2,5-5	2,5-5	1
Максимальний відсоток похибки порогу спрацювання	%	1,2	1,5	1,25
Потужність споживання	Вт	35	25	0,7
Об’єм	$м^3$	0,1	0,07	0,7
Маса без аккумулятора	кг	2,7	1,6	0,6
Ціна	грн	3045	1716	0,6

1.9 Аналіз результатів порівняння

Більшість порівнюємих параметрів співпадає, так як прилади фактично виконують ті ж функції і повинні відповідати єдиному стандартові (таблиця 1.1) існують різні підходи, які і відрізняють два прилади за іншими ознаками.

Зменшивши інформаційну ємність до більш раціонального значення отримаємо значну економію по радіодеталям, що в свою чергу відображається на вартості приладу.

Збільшення інформативності планується досягнути за рахунок вдосконалення програмного забезпечення.

Розширення керуючих пристроїв досягнемо також за рахунок вдосконалення програмного забезпечення.

Потужність споживання – так як обидва прилади працюють в цілодобовому режимі то відповідно у аналога кількість спожитої енергії за час одного року роботи більша (аналог 306,60 кВт/рік., розробка 219 кВт/рік.). Такий результат планується досягти за рахунок зменшення кількості радіоелементів та використання більш енергоекономічних компонентів. Отже, розробка краще за аналог по цьому параметру.

Об’єм, що займає прилад – розробка займає менше місця за аналог – це благотворно позначиться на габаритних показниках системи, куди монтуватиметься прилад.

Маса – із-за того, що аналог виконують в металевому корпусі він має значне перевищення параметру маса відносно розробки. Аналог тяжчий за розробку. Отже, розробка краще за аналог по цьому параметру.

Ціна – заявлена ціна аналога по перерахунку в гривні 3045 грн., нової розробки орієнтовна ціна складає 1716 грн. Як і попереджалося у аналога значне перевищення ціни приладу. Зазначимо, що ціна не враховує вартості на перевезення і обслуговування. Розробка буде складатися на підприємствах України і тому вартість обслуговування і транспортні витрати цілком можливо будуть менші.

Висновки по параметрам аналога і розробки. За рахунок зменшення інформаційної ємності до більш раціонального значення, вдалось створити прилад-розробку, що відповідає всім основним технічним, масо-габаритним показникам і по ціні не гірше, а й краще аналога подекуди навіть у 2 рази. Усе

вищезгадане реалізується шляхом використання новітньої елементної бази, нових технологій при монтажі, і новітніх підходах у галузі програмного забезпечення. Тому рекомендовано впроваджувати розробку у виробництво, відмовившись від аналога.

1.10 Висновки до першого розділу

В ході техніко-економічного обґрунтування, при розрахунках економічних показників було отримано абсолютну економію як питомих капіталовкладень, так і експлуатаційних витрат, що вказує на доцільність впровадження нової розробки у виробництво і досягнення прицьому позитивного економічного ефекту.

З викладеного вище випливає, що на сьогоднішній день існує потреба у даній продукції і можливо отримати прибуток при її виготовленні. Також прилад сконструйований таким чином, що можливе його удосконалення та інваріантність.

2 РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ПРИСТРОЮ

2.1 Принцип реалізації стандарту GSM

Загальноєвропейський стандарт GSM - перший у світі стандарт на цифрові ССРЗ, що передбачає їхнє створення в діапазоні 900 МГц і є основою стандарту DCS1800 (діапазон 1800 МГц) з мікростільниковою структурою, прийнятого в даний час у Європі. Стандарт GSM реалізується в даний час і в Північній Америці в діапазоні 1900 МГц (PCS-1900).

Зазначені стандарти відрізняються по своїх характеристиках, але побудовані по єдиних принципах і використовують тимчасовий поділ каналів зв'язку TDMA, що відповідає вимогам сучасних інформаційних технологій.

В даний час популярність стандарту GSM настільки велика, що тепер він розуміється як глобальна система рухомого зв'язку. GSM і його варіанти, - DCS-1800 (Digital Cellular Systems 1800) і PCS-1900 (Personal Communication Service), прийняті і розвиваються в Європі, Азії, Африці, Австралії і Північній Америці (по стану на лютий 1998 року цей стандарт прийнятий у 105 країнах). З огляду на цю обставину, абревіатура GSM, спочатку утворена з перших букв назви спеціальної групи (Group Special/Mobile), у даний час розшифровується як Global System for Mobile Comriiunications (глобальна система для рухомого зв'язку).

Стосовно інших цифрових стандартів GSM забезпечує кращі енергетичні і якісні характеристики зв'язку, найвищі характеристики безпеки і конфіденційності зв'язку. Цей стандарт передбачає роботу передавачів у двох діапазонах частот: 890-915 МГц (для передавачів рухливих станцій), 935-960 МГц (для передавачів базових станцій). У цьому стандарті використовується вузькосмуговий багатостанційний доступ з тимчасовим поділом каналів (NB TDMA), що дозволяє організувати 8 фізичних каналів на кожній з 124 несучих частот.

Характеристика цифрового стандарту стільникової систем зв'язку GSM наведені в таблиці 2.1.

Для захисту від помилок у радіоканалах при передачі повідомлень приймається блокове і згорткове кодування з перемеженням. Підвищення ефективності кодування і перемеження при малій швидкості переміщення рухливих станцій досягається повільним переключенням робочих частот (SFH) у процесі сеансу зв'язку зі швидкістю 217 стрибків у секунду.

Для боротьби з інтерференційними завмираннями прийнятих сигналів, викликаними багатопроменевим поширенням радіохвиль в умовах міста, в апаратурі зв'язку використовуються еквалайзери, що забезпечують вирівнювання імпульсних сигналів зі середньоквадратичним часом затримки до 16 мкс.

Система синхронізації розрахована на компенсацію абсолютного часу затримки сигналів до 233 мкс, що відповідає максимальній дальності зв'язку чи максимальному радіусу осередку (стільника) 35 км.

У стандарті GSM обрана гаусова частотна маніпуляція з мінімальним частотним зрушенням (GMSK). Обробка мови здійснюється в рамках прийнятої системи переривчастої передачі мови (DTX), що забезпечує включення передавача тільки при наявності мовного сигналу і відключення передавача в паузах і наприкінці розмови. У якості мовоперетворюючого пристрою обраний мовний кодек з регулярним порушенням (довгостроковим пророкуванням і лінійним предикативним кодуванням із пророкуванням (PRE/LTR-LTP-кодек). Загальна швидкість перетворення мовного сигналу - 13 Кбіт/с. За даними фірми Ericsson, прийнятна якість прийнятих мовних повідомлень забезпечується в GSM при відношенні сигнал/шум на вході приймача 9 дБ, для американського стандарту D-AMPS це відношення складає вже 16 дБ. У реальних каналах зв'язку при завмираннях сигналів енергетичні витрати в D-AMPS вище на 6-10 дБ стосовно GSM.

Таблиця 2.1 – Характеристика цифрового стандарту стільникової систем зв'язку GSM

Характеристики стандарту	GSM (DCS1800, PCS1900)
Метод доступу	TDMA
Рознос частот, кГц	200
Кількість мовних каналів на несучу	8(16)
Швидкість перетворення мови, Кбіт/с	13 (6,5)
Алгоритм перетворення мови	RPE-LTP
Загальна швидкість передачі. Кбіт/с	270
Еквівалентна смуга частот на мовний канал, кГц	25 (12,5)
Необхідне відношення сигнал/шум, дБ	9
Метод рознесення	перемеження, стрибки по частоті
Радіус стільника, км	0,5-35
Робочий діапазон частот, МГц	935-960 (GSM) 890-915 (GSM) 1710-1785 (DCS) 1805-1880 (DCS)

Крім того, стандарт GSM представляє ряд послуг, що не реалізовані в інших стандартах стільникового зв'язку. До них відносяться:

• використання інтелектуальних SIM-карт для доступу до каналу і послуг зв'язку;

• закритий для прослуховування радіоінтерфейс;

• шифрування переданих повідомлень,

• аутентифікація абонента та ідентифікація абонентського устаткування по криптографічних алгоритмах;

• використання служб коротких повідомлень, переданих у сигналах сигналізації;

• автоматичний роумінг абонентів різних мереж GSM (міжнародний і національний);

• міжоператорський роумінг абонентів GSM з абонентами мереж DCS1800, PCS 1900, DECT, а також із супутниковими мережами наземного рухомого зв'язку (Iridium, GlobalStar, Inmarsat-P).

Стандарт GSM призначений для надання послуг рухомого зв'язку поза залежністю від національних границь на всьому Європейському континенті. У 1990 році була довершена специфікація цієї системи в обсязі фази 1. Однак незабаром стало ясно, що виділеної для цієї системи смуги частот шириною 2х25 МГц недостатньо для великих міст із високою щільністю абонентів. У 1991 році специфікацію системи GSM доповнили вимогами до системи DCS1800, для якої була виділена смуга частот 2х75 МГц у діапазоні 1800 МГц. У 1992 році послугами стільникового зв'язку на комерційній основі були охоплені всі країни Європи - учасниці підписаного в 1987 році Меморандуму про взаєморозуміння.

У 1995 році була довершена в обсязі фази 2 специфікація системи з розширеним набором послуг і функціональних можливостей. В даний час ведеться інтенсивна робота над специфікацією майбутніх можливостей системи в рамках фази 2+.

У Північній Америці стандарт GSM був прийнятий у якості одного зі стандартів для системи персонального зв'язку в діапазоні 1900 МГц, він одержав назву PCS 1900. Є всі підстави думати, що стандарт GSM послужить прототипом для специфікації системи третього покоління - майбутньої системи сухопутного рухомого зв'язку загального користування (FPLMTS/IMT2000), що розробляється в рамках Міжнародного союзу електрозв'язку і повинний бути введений в експлуатацію, приблизно з 2000 року.

2.2 Опис ефірного інтерфейсу

Протокол обміну між мережею і опонентом по радіоканалу отримав назву ефірного інтерфейсу (U_m). Частотний канал - це смуга частот, яка відводиться для передачі інформації одного каналу зв'язку. При використанні методу TDMA (Time Division Multiple Access) в одному частотному каналі передається інформація декількох каналів зв'язку, тобто в одному частотному каналі розміщуються декілька фізичних каналів (ФК).

ФК в системі TDMA - це часовий слот з визначеним номером в послідовності кадрів радіоінтерфейсу.

Логічні канали (ЛК) розрізняються по виду інформації, яка передається в ФК. В принципі в ФК може бути реалізований один із двох видів ЛК - канал трафіка (КТ) або канал керування (КК). Кожен з них може в загальному випадку існувати в одному з декількох варіантів (типів). Логічний КТ - це канал передачі мови або даних. Логічний канал керування призначений для передачі керуючої інформації (сигналізації). В таблиці 2.2 наведена загальна класифікація ЛК, що використовуються в системах стільникового зв'язку (ССЗ), а в таблиці 2.3. наведена структура логічних каналів стандарту GSM.

Канали трафіку ТСН (Traffic Channels) поділяються на повношвидкісні (22,8 Кбіт/с - TCH/FS (із повношвидкісним кодуванням; F - Full - повний; S Speech - мова) і напівшвидкісні (11,4 Кбіт/с) - TCH/HS (H - Half- половина). Також передбачені канали трафіка для передачі даних зі швидкістю від 2,4 Кбіт/с до 9,6 Кбіт/с (TCH/F9.6, TCH/F4.8, TCH/H4.8 і т.п.).

Канали керування ССН (Control Channels) поділяються на 4 типи: віщальні BCCH (Broadcast Control Channels); загальні CCCH (Common Control Channels); виділені закріплені SDCCH (Standalone Dedicated Control Channels); суміщені (асоційовані) ACCH (Associated Control Channels).

Канали BCCH призначені для передачі інформації від БС до РС у віщальному режимі, тобто без адресування до якої-небудь конкретної РС. У число віщальних КК входять: канал корекції частоти FCCH (Frequency

Correction Channel) - для підстроювання частоти РС під частоту БС; канал синхронізації SCH для циклової синхронізації РС; канал загальної інформації, що не має окремої назви.

Таблиця 2.2 – Класифікація і типові позначення каналів

Ознака	Позначення	Назва каналу
Напрямок зв'язку	F	Прямий (Forward)
	R	Зворотній (Reverse)
Тип каналу	L	Логічний (Logical)
	P	Фізичний (Physical)
Призначення каналу	A	Доступ (Access)
	P	Виклик (Paging)
	S	Сигналізація (Signaling)
	T	Трафік (Traffic)
	C	Керування (Control)
Спосіб організація зв'язку	A	Суміщений (Associated)
	B	Широкомовний (Broadcast)
	C	Загальний (Common)
	D	Виділений (Dedicated)
	SD	Автономний (Stand-alone)
Допоміжні канали	A	Допоміжний (Auxiliary)
	PL	Пілот-сигнал (Pilot)
	S або SYNC	Синхроканал (Synchronization)

Загальні канали керування CCCH включають: канал виклику PCH, який використовується для виклику рухомої станції базовою; канал дозволу доступу AGCH (Access Grant Channel) - для призначення закріпленого КК, що також передається від БС на РС; канал випадкового доступу RACH - для виходу з РС на БС із запитом про призначення виділеного КК.

При передачі інформації по загальним КК, прийом інформації не супроводжується підтвердженням.

Таблиця 2.3 – Структура логічних каналів стандарту GSM

Види логічних каналів	Типи каналів
Канали трафіку TCH	TCH/FS, TCH/HS
Канали керування CCH	BCCH, FCCH, SCH, CCCH, PCH, RACH, AGCH, SDCCH, ACCH, FACCH, SACCH

Виділені закріплені канали керування SDCCH - автономні КК, використовуються для сигналізації в процесі встановлення з'єднання до призначення каналу користувача, наприклад, для аутентифікації і реєстрації.

Суміщені канали керування ACCH, також використовувані для передачі інформації в обох напрямках, містять у собі: повільний суміщений канал керування SACCH - поєднується з каналом трафіка (кадр 13 мультикадра каналу трафіка) чи з каналом SDCCH, застосовується для передачі інформації, наприклад: результатів виміру рівня сигналу свого і суміжного стільника, регулювання потужності РС, часової синхронізації; швидкий суміщений канал керування FACCH - сполучається з каналом трафіка, заміняючи у відповідному слоті інформацію мови, причому ця заміна позначається скритим прапорцем (поле S). Використовується поряд із каналом користувача, коли в процесі обміну інформацією користувача необхідно передати обсяг інформації більше, ніж може забезпечити повільний асоційований канал. У цьому випадку замість 20 мс інформації користувача передається, наприклад, інформація, необхідна

для переключення виклику. Переривання в передачі інформації користувача незначне. При цьому абоненту повторно передається інформація попереднього циклу.

У стандарті GSM є 124 радіоканали, які відповідно до плану розподілу частот розподілені між БС (BTS). Кожна з BTS має n двосторонніх радіоканалів C_0, C_1,... C_n, кожен з яких містить по 8 ФК. Використовуючи ці ФК, необхідно організувати всі необхідні логічні канали.

Логічні канали корекції частоти - F (FCCH), синхронізації - S (SCH), віщальний - B (BCCH) і загальні - C (AGCH/PCH) мають напрямок передачі від БС до РС (прямий канал), а загальний канал випадкового доступу - R (RACH) - від РС до БС (зворотний канал). Виділений індивідуальний сигнальний - D (SDCCH), повільний суміщений - A (SACCH) і швидкий суміщений - A' (SACCH) є двосторонніми. При цьому ЛК керування F, S і B мають конфігурацію «крапка-три крапки», і досить мати по одному каналові даного типу в кожному із стільників. Необхідне число логічних КК типів C, R, D, A залежить від навантаження, створюваного РС у кожному стільнику. В залежності від навантаження, для організації логічних КК використовуються один чи більш ФК.

На відміну від дуплексних каналів - трафіка і суміщених КК, які розташовуються у КТ ефірного інтерфейсу, - симплексні канали керування BCCH і CCCH розміщуються в нульовому слоті кадрів КК ефірного інтерфейсу на так званих несучих BCCH, які присутні в комірці.

Повідомлення каналів BCCH і CCCH, передані від БС до РС (прямий канал), розміщуються в нульових слотах 50 кадрів мультикадра КК. Останній, 51-й, кадр мультикадра залишається вільним (I - Idle), його тривалість відводиться РС для реалізації процедури виміру рівня сигналів свого і суміжного стільника. Перші 50 кадрів поділяються на 5 блоків по 10 кадрів. На початку кожного блоку передається повідомлення каналу FCCH (структура слота - інтервал підстроювання частоти), далі - повідомлення каналу SCH

(структура слота - інтервал синхронізації), потім в першому блоці передається чотири повідомлення каналу BCCH і чотири повідомлення каналу AGCH чи каналу PCH, а в інших чотирьох блоках усі вісім повідомлень відводяться під канал AGCH чи PCH. Повідомлення логічних КК в більшості випадків кодуються зі значною надмірністю з метою захисту від помилок при передачі інформації.

Повідомлення каналу RACH можуть бути передані в нульовому слоті будь-якого кадру в межах 51-кадрового мультикадра КК. Повідомлення RACH передається РС раз у 235 мс, тобто тільки в одному з кадрів мультикадра, при цьому використовується структура слота, що відповідає інтервалу доступу. У зворотному каналі мультицикл не розбивається на групи циклів доступу, а 0-й слот кожного кадру мультикадра використовується для організації логічного каналу R.

Інформація швидкого суміщеного каналу A' передається по каналах користування. Логічні канали D і A є двосторонніми, і для їхньої організації використовується 1-й слот радіоканалу. Для забезпечення необхідної якості обслуговування викликів у даному випадку, досить у кожному стільникові мати по 8 логічних каналів D зі швидкістю передачі 1.94 Кбіт/с і таку ж кількість суміщених з ними каналів А зі швидкістю передачі в два рази нижче.

З огляду на це, для того щоб одержати по 8 ЛК кожного типу, необхідно два мультикадра по 51 кадру в кожному. ЛК прямого і зворотного напрямків передачі зміщені один відносно одного. Це необхідно для забезпечення більш ефективної взаємодії РС і БС, тобто РС має можливість формувати відповідну інформацію.

Логічні канали користування (Т) організуються в такий спосіб. Нульовий і перший слоти радіоканалу С0 вже зайняті під логічні КК, і на цій частоті для організації ЛК користування залишаються тільки слоти з другого по сьомий. При організації ЛК користування необхідно враховувати, що кожний з них повинний мати повільний асоційований логічний канал А зі швидкістю

передачі 950 біт/с, що використовується, наприклад, для регулювання потужності РС в процесі обміну інформацією користування. Крім того, РС потрібно виділити час для реалізації процедури зміни рівня сигналу. З огляду на вищесказане, при розміщенні ЛК користування організовується мультикадр, що містить 26 кадрів. У повношвидкісному каналі 13-й кадр мультикадра використовується для розміщення ЛК керування А, а 26-й залишається порожнім. Інші 24 кадру мультикадра призначені для розміщення одного ЛК користувача зі швидкістю передачі 22,8 Кбіт/с (24х114 біт за 120 мс).

У напівшвидкісному каналі інформація каналу керування А передається в кожному 13-му і 26-му кадрах мультикадра.

Структури мультикадрів прямого і зворотного каналів ідентичні. Однак варто враховувати, що РС не може одночасно здійснювати передачу і прийом інформації, тому цикли доступу прямого і зворотного напрямків передачі зміщені в часі.

2.3 Загальні принципи побудови стільникової мережі

Застосування стільникових систем забезпечує економію частотного ресурсу за рахунок його багаторазового використання в зоні обслуговування. Для цього вона розбивається на більш дрібні зони (кластери), що складаються з рівного числа первинних осередків - стільників. Між стільниками розподілені всі доступні телефонні канали, число яких визначається дозволеним для стільникового зв'язку частотним діапазоном. Кількість стільників у кластері залежить від відстані між осередками сполученого каналу в сусідніх кластерах і радіуса стільника і називається розмірністю кластера, що, як правило, знаходиться в межах від 4 до 12 км.

На території кожного стільника знаходиться цілком автоматизована базова станція невеликої потужності, що забезпечує радіозв'язок з переносною чи розташованою в будинку станцією охоронноъ системи (рисунок 2.2). Базова станція має канал керування, набір мовних каналів зв'язку і приймач, що

вимірює інтенсивність сигналу. Число мовних каналів, діаграма повторного використання частот, зона обслуговування кожного стільника вибираються таким чином, щоб забезпечити необхідну ємність стільникової мережі за графіком.

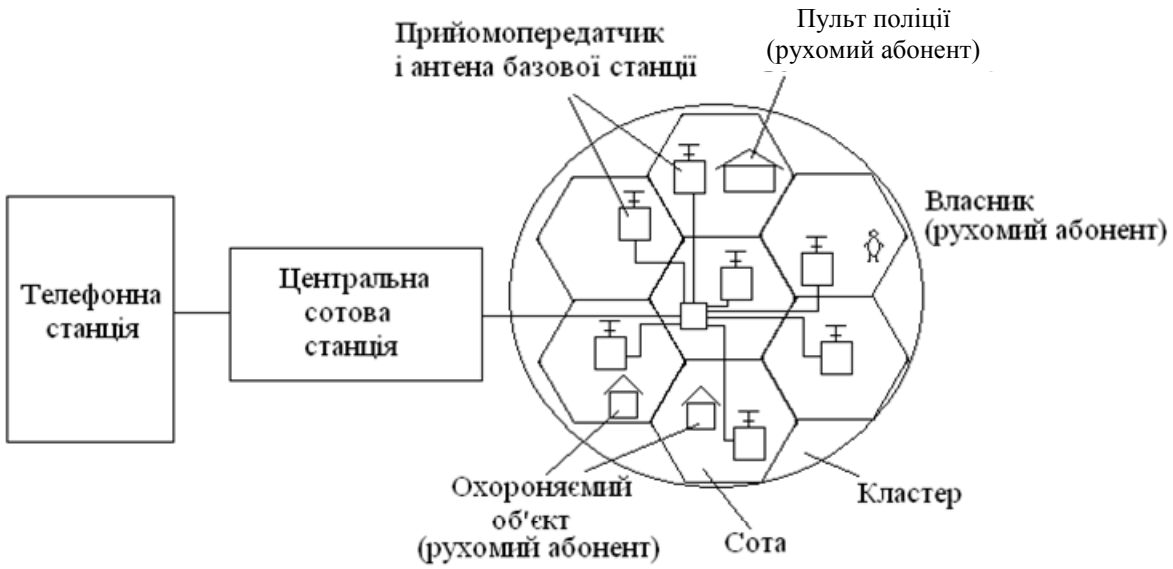


Рисунок 2.2 – Структурна схема системи охорони з використанням стільникової мережі

Кожна базова станція з'єднана з центром комутації рухливої мережі (центральна стільникова станція), що забезпечує зв'язок з телефонною мережею загального користування, що комутується, (ТМЗК), а також з іншими базовими станціями. Рухомі абоненти стільникової мережі зв'язуються тільки з найближчою базовою станцією. Таким чином, на великому просторі може бути створена мережа з великої кількості взаємозалежних радіостанцій. При цьому невелика потужність передавачів дозволяє робити апаратуру дуже компактною і відносно недорогою.

Кожній базовій станції, що оснащена приймально-передавальною апаратурою, дається набір частотних каналів, які забезпечують кілька двосторонніх телефонних розмов одночасно. На станціях, що розділені

захисним інтервалом D, ті самі канали використовуються повторно. Цей основний принцип стільникових систем телефонного зв'язку рухливих абонентів визначає високу частотну ефективність системи. Суміжні базові станції, що використовують різні канали, утворять групу з С станцій. Величина С є частотним параметром системи, тому що визначає мінімально можливе число каналів системи.

2.4 Технічні засоби охорони

До технічних засобів охорони відносяться:

- системи охоронної і пожежної сигналізації;
- системи обмеження доступу;
- системи телевізійного спостереження;
- комплекси, на базі ЕОМ, включаючи перераховані системи.

Приведені вище системи можуть працювати як в комплексі, так і окремо. Наприклад, охорона і телевізійне спостереження може здійснюватися за великим числом об'єктів або однією квартирою або офісом.

Системи будь-якої складності будуються на базі одних і тих же технічних пристроїв. При рішенні технічних задач охорони в першу чергу необхідно вибрати основні параметри пристроїв, які забезпечать достатню надійність виконання покладених на них функцій.

Системи охоронної сигналізації фіксують факт несанкціонованого доступу на територію, що охороняється, передають сигнал тривоги, наприклад, на пульт охорони і включають виконуючі пристрої.

Системи охоронної сигналізації включають:

- датчики;
- пульт-концентратор;
- виконуючі пристрої.

Датчик - чутливий елемент, перетворюючий контрольований параметр в електричний сигнал.

Особливість датчиків для систем охоронної сигналізації полягає в тому, що вони реєструють, в основному, неелектричні величини. Вимірювання неелектричних величин - складна задача і при цьому датчики повинні забезпечувати високу надійність і достовірність контролю.

Надійність датчиків забезпечується, в основному, цифровими методами обробки сигналів.

Датчики об'єднуються в зони. Під зоною розуміється один або декілька датчиків, що охороняють певний об'єкт або ділянку об'єкту.

В системах охоронної сигналізації використовуються датчики наступних типів:

- пасивні інфрачервоні датчики руху;
- датчики розбиття скла;
- активні інфрачервоні датчики руху і присутності;
- фотоелектричні датчики;
- мікрохвильові датчики;
- ультразвукові датчики;
- вібродатчики;
- датчики температури;
- датчики наявності пари і газів;
- магнітні (герконові) датчики;
- шлейфи.

Пульт-концентратор - центральний пристрій системи охоронної сигналізації. Він виконується на базі мікропроцесора. Всі функції системи визначаються програмою мікропроцесора. Параметри програми задає користувач, залежно від його повноважень, із спеціального пульта.

Пульти-концентратори можуть підключатися до персональних ЕОМ для обробки і реєстрації сигналів тривоги, автоматичного аналізу стану датчиків і функціонування всієї системи.

Пульти-концентратори можуть приймати і передавати повідомлення по телефонній мережі через комунікаційний модуль в автоматичному режимі.

Більшість систем охоронної сигналізації доповнюється датчиками пожежної безпеки. Найбільш розвинуті системи можуть включати інші підсистеми і доповнюватися, наприклад, пультами дистанційного керування.

За способом підключення датчиків до пультів-концентраторам охоронні пристрої розділяються на провідні і безпровідні.

В провідних системах зв'язок між всіма пристроями системи здійснюється по кабелю. При високій надійності провідних систем вони менш гнучкі, ніж бездротові.

В безпровідних системах кожний датчик оснащується власним передавачем, а пульт-концентратор - багатоканальним приймачем. Приймач і передавач можуть бути вбудованим, або виконаними у вигляді окремих модулів.

Безпровідні системи охоронної сигналізації більш зручні при монтажі і використовуванні. Вони можуть доповнюватися сервісними пристроями дистанційного керування.

Дешеві безпровідні системи характеризуються більшою вірогідністю помилкових спрацьовувань. Стійкість безпровідних систем охоронної сигналізації нижче в місцях з високим рівнем промислових радіоперешкод.

Дальність зв'язку датчик - головний пульт, як правило, складає від 30 до 300 м для стандартних систем і до 3 км для систем збільшеного радіусу дії.

Надійність зв'язку визначається характеристиками приймача і передавача, архітектурою будівлі і рівнем промислових радіоперешкод.

Безпровідні системи випускаються фірмами ROCONET, LINEAR, VISONIC, POWERHOUSE і ін.

Для охорони внутрішніх приміщень найбільше розповсюдження отримали пасивні ІК-датчики руху і суміщені датчики типу пасивний + мікрохвильової.

Наибольшей популярністю користуються датчики:

- серії MH і D&D фірми CROW;
- серії BRAVO фірми DSC;
- серії Paradox фірми PIROTEC;
- серії DXR фірми CROW;
- серії Force-2 фірми DSC;
- серії XJ фірми C&K.

Суміщені датчики відрізняє набагато більш висока надійність і стійкість до помилкових спрацьовувань.

Для охорони периметра і приміщень використовуються:

- активні інфрачервоні датчики руху і присутності;
- пасивні і дуальні датчики руху;
- датчики розбиття скла;
- магнітні датчики;
- шлейфи.

Пасивні інфрачервоні датчики руху спрацьовують при попаданні об'єкту, випромінюючого тепло (наприклад, людини), що рухається, в зону чутливості датчика.

Датчики відрізняються, в основному, формою зони чутливості і стійкістю до помилкових спрацьовувань. Зона чутливості датчиків для систем охоронної сигналізації є сектором (90^0-110^0). В технічному описі датчиків приводяться діаграми, які наочно демонструють зони чутливості датчиків.

Діаграма датчика може бути змінена. Відповідно до розташування датчика і особливостей плану приміщення змінити діаграму можна використовуючи прикладені до датчика змінні лінзи Френеля або накладки, які перекривають частину чутливого елемента датчика.

Недолік найпростіших і дешевих датчиків в тому, що вони спрацьовують при певній швидкості зміни теплового потоку.

Досконаліші (і більш дорогі) датчики не мають цих недоліків. Їх надійність і стійкість до теплових перешкод забезпечується багатоканальними чутливими головками і складною обробкою сигналу в самому датчику.

До найпростіших відносяться датчики сімейства Bravo-2 фірми DSC і Paradox Light фірми PIROTEC. До найскладнішим - Paradox Vision-510 і UP350 фірми Alarmcom.

Датчики розбиття скла реагують на дзвін скла, що б'ється. Найбільш досконалі моделі аналізують спектр звукових шумів в приміщенні.

Якщо спектр шуму містить складову, співпадаючу із спектром ушкоджуваного скла, то датчик спрацьовує. Один такий датчик може охороняти скляні вікна, вітрини і т.п., площею до 10 $м^2$.

Двохпорогові датчики реєструють звук удару по склу і дзвін скла, що розбивається. Для індикації тривоги такий датчик повинен зареєструвати два відповідні сигнали з інтервалом не більше 150 мс.

Чутливість датчиків розбиття скла регулюється із застосуванням імітатора розбивання скла, наприклад DG-50 або FG-700.

Фотоелектричні датчики випромінюють і приймають відображений сигнал інфрачервоного випромінювання з довжиною хвилі порядка 1 мкм. Вони використовуються у складі систем захисту внутрішнього і зовнішнього периметра для безконтактного блокування прольотів, дверей, ліфтів, отворів, коридорів і т.п. Їх відрізняє висока стійкість і надійність роботи.

Фотоелектричні датчики складаються з двох частин - передавача і приймача. Вони розносяться уздовж лінії охорони. Між ними проходить система модульованого інфрачервоного проміння.

Мікрохвильові датчики випромінюють і приймають відображений сигнал поля надвисокої частоти. В плані охорони внутрішніх приміщень, їх характеристики аналогічні характеристикам вище перелічених пристроїв, але мікрохвильові датчики мають:

- набагато більш високі ціни;

- більш низьку стійкість до помилкових спрацьовувань;

- високий рівень шкідливих випромінювань.

При охороні зовнішнього периметра датчики даної групи програють по своїх характеристиках активних ІК-датчикам фотоелектричного типу.

Ультразвукові датчики

Ультразвукові датчики випромінюють і приймають відображений сигнал ультразвукового поля. Їх відрізняє:

- мала чутливість;

- високий рівень помилкових спрацьовувань;

- залежність настройок від перепадів температури, протягу, акустичних шумів, коливань вогкості.

Тому цей тип датчиків знайшов застосування, в основному, в недорогих системах для захисту малих замкнутих ізольованих об'ємів, наприклад, салону автомобіля.

Вибро-датчики реагують на наявність вібрації і ударів. Працюють на основі п'єзоефекту або електромагнітної індукції. Відрізняються низькою вартістю і високим рівнем помилкових спрацьовувань.

Магнітні датчики відносяться до найпростіших і встановлюються на вікна, двері і люки. Випускаються двох видів:

- для зовнішньої установки;

- для скритої установки. (Зазвичай розміщуються у верхній частині двері або вікна).

З метою підвищення надійності встановлюється по два датчики, з’єднаних послідовно. При установці на вікнах кожна фрамуга вікна захищається парою "геркон + магніт".

Магнітні датчики є парою геркон плюс магніт і спрацьовують при відкритті/закритті дверей або вікна.

Шлейфи є стрічкою з тонкої алюмінієвої фольги. Вона клеїтися на скло, стіну двері і т.д. При руйнуванні підстави, на яку вона наклеєна, стрічка рветься і розриває коло протікання електричного струму. Для підключення до кола охоронної сигналізації стрічка і провідник затискаються в утримувачі, який клеїтися до тої ж підставки, що і стрічка.

Пульт-концентратор приймає сигнали від пультів дистанційного керування і від датчиків зон, що охороняються.

Залежно від стану датчиків, зони і режиму роботи, пульт-концентратор включає виконуючі пристрої в режимах, заданих користувачем і запам'ятовує інформацію про події.

Більшість професійних пультів-концентраторів має вбудований цифровий комунікаційний модуль, призначений для прийому і передачі кодованих повідомлень по телефонній лінії в повністю автоматичному режимі.

Комунікаційний модуль дозволяє приймати сигнал тривоги по телефону на міському (районному) пульті охорони, обладнаному декодуючою апаратурою, і подавати команди по телефонній лінії на пульт-концентратор.

Існують спеціальні пристрої, (наприклад, ESCORT фірми DSC), дозволяючі вести діалог з пультом-концентратором за допомогою звичайного телефону. Вам достатньо набрати телефонний номер, до якого через ESCORT підключений пульт-концентратор, і набрати на телефонному номеронабирачі пароль доступу до системи. Після цього пульт-концентратор через голосовий синтезатор пристрою ESCORT повідомить поточний стан та відповість на інші задані Вами запитання.

Весь діалог з системою протікає за принципом: інформація від пульта-концентратора - голосовими повідомленнями (Ваші команди);

- через номеронабирач.

Залежно від моделі пульт-концентратор дозволяє створювати системи охорони як невеликих об'єктів (квартири, офіси), так і крупних (підприємство, велика будівля або комплекс будівель).

Виконуючі пристрої підключаються до центрального пульта за допомогою провідної або безпровідного зв'язку. В системах охоронної сигналізації можуть використовуватися наступні виконуючі пристрої:

- потужна сирена;
- мигаюче світло;
- графічні панелі з планом приміщень;
- система підсвічування;
- принтер для реєстрації часу, місця і характеру порушення, і ін.

В якості сирени використовуються потужні п'єзоелектричні сирени потужністю до 120 дБ. Більш потужні джерела звукових коливань можуть привести до травми слухового апарату не тільки порушника, але і власника системи.

Найкращі зразки сирен для систем охоронної сигналізації є захищені від механічних дій пристроями з автономним живленням.

Вони містять джерела звукової і світлової сигналізації. У разі відключення провідників такі сирени спрацьовують, попереджаючи про порушення.

Мигаюче світло призначено для залучення уваги оточуючих при спрацьовуванні сигналізації. Він може включатися як попереджувальний сигнал при спробі порушення підходів до зон охорони.

Графічні панелі з планом приміщення використовуються в складних системах і відображають на плані місце порушення.

Структурна схема блоку керування радіоохоронної системи, яка використовує стільникову мережу стандарту GSM для передачі сповіщень на пульт міліції чи власнику об’єкта, що охороняється, приведена на Рисунок 2.3.

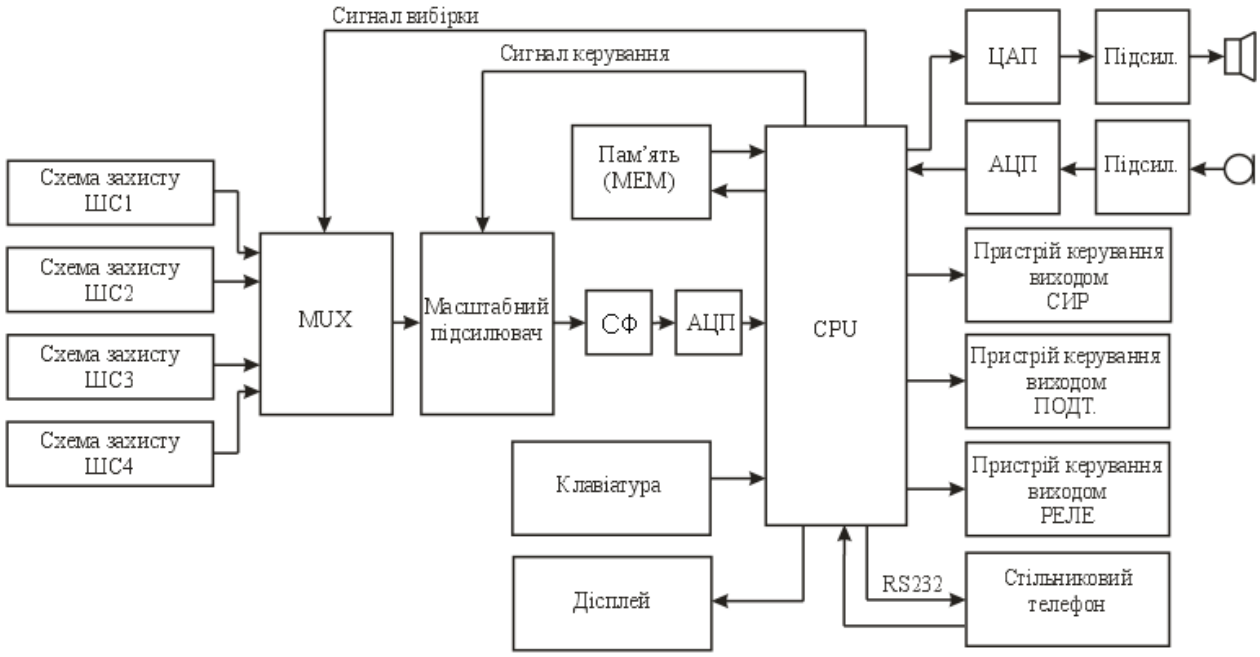


Рисунок 2.3 - Структурна схема радіоохоронної системи

Так як датчики розташовуються на певній відстані від радіоохоронної системи, використовуються схеми захисту шлейфів сигналізації (ШС1-ШС4), що захищають систему від наводок та попадання на них високої напруги. Опит шлейфів відбувається по черзі, тому для реалізації такого алгоритму опиту використовується мультиплексор (MUX). Масштабний підсилювач забезпечує підсилення сигналу отриманого в результаті опитування шлейфу сигналізації до необхідного рівня. Смуговий фільтр (СФ) служить для відфільтровування можливих завад до 100 кГц. Аналогово-цифровий перетворювач перетворює підсилений сигнал в цифровий еквівалент. З клавіатури задаються параметри роботи радіоохоронної системи (під час програмування), та виконується контроль всієї системи (постановка, зняття з охорони та інші сервісні команди). Дисплей служить для наочного відображення стану радіоохоронної системи, датчиків сигналізації та виконуючих пристроїв. Пам'ять (MEM) зберігає програму керування, поточні дані та інформацію про спрацювання датчиків.

Цифро-аналоговий перетворювач перетворює цифровий запис в аналоговий для подальшого підсилення та відтворення на гучномовці (дана

функція служить для прослуховування записаних в пам’ять повідомлень). Пристрій керування виходом „СИР” служить для вмикання (вимикання) виконуючого пристрою сирена у випадку спрацювання охоронного чи пожежного датчика. Пристрій керування виходом „ПОДТ” служить для вмикання (вимикання) виконуючого пристрою індикатор підтвердження. Індикатором підтвердження може служити звичайний світлодіодний індикатор з подільником напруги, або лампочка 12В. Пристрій керування виходом РЕЛЕ служить для керування релейним виходом. Цей вихід може контролювати роботу додаткових виконуючих пристроїв, або об’єднувати охоронну систему з іншими охоронними системами для створення комплексу охоронних систем. Стільниковий телефон служить для передачі сповіщень на мобільний телефон власника об’єкту, або на пульт міліції. Стільниковий телефон контролюється охоронною системою через стандартний протокол обміну RS232. CPU – мікропроцесор фірми Microchip PIC16F874.

2.5 Висновок до другого розділу

Сукупність різноманітних датчиків як контактної дії так і безконтактних дозволяє контролювати довільну зону та виконувати задачі визначення порушення умов обмеження доступу.

Виявлені стани фіксуються в пристрої контролю, порівнюються та передаються до інших пристроїв мережі.

3 ЕЛЕКТРИЧНИЙ РОЗРАХУНОК

Однією із функцій розробляємого блоку керування радіоохоронної системи стандарту GSM є передача голосових повідомлень на пульт поліції чи безпосередньо на телефон власника приміщення, що охороняється. Тому для зберігання та передачі цих повідомлень потрібні сигнали (повідомлення) достатнього рівня. Для забезпечення рівня таких сигналів можна використати звичайні підсилювачі на ОП.

Характеристики підсилювачів були істотно покращені з активним впровадженням симетричного зняття сигналу з дифкаскаду та застосуванням зустрічного динамічного навантаження у другому каскаді за допомогою так званих струмових дзеркал.

Останнім часом в зарубіжній літературі з'явилися статті з описами ППЗЧ, побудованих на основі схеми ОП із струмовим входом (мається на увазі ОП з низькоомним інвертуючим входом, наприклад, серій AD8001, КМ1432УД1). Ці підсилювачі більш широкосмугові і мають високу швидкість наростання вихідної напруги. Така побудова УМЗЧ дозволяє значно знизити нелінійні спотворення в цілому і повністю позбавитися динамічних, що у результаті приводить до підвищення якості звуковідтворення.

Структурна схема типового ОП з послідовною ООС на струмовий вхід показана на рисунку 3.1. Він має вхідний підсилювач на транзисторах VT1, VT2 з ланцюгами зсуву G1, G2, VD1, VD2, два струмові дзеркала VT3-VT6 і вихідний неінвертуючий підсилювач A1 (резистори R1, R2 є елементами зовнішнього ВЗЗ).

Високоомні базові кола транзисторів VT1, VT2 утворюють неінвертуючий вхід підсилювача, а їх емітери, сполучені разом, – інвертуючий, низькоомний або, іншими словами, струмовий (звідки і виникла назва: "підсилювач із струмовим зворотним зв'язком" — Current Feedback Audio Amplifier).

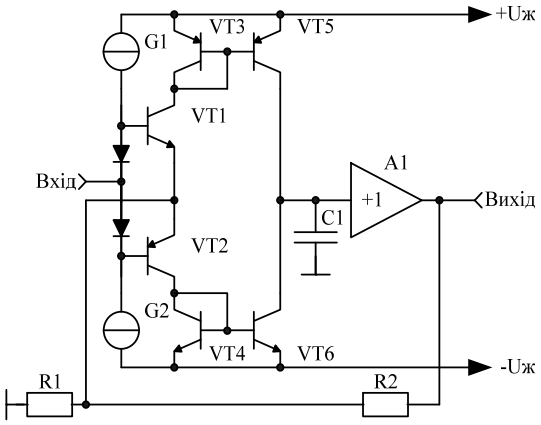


Рисунок 3.1 – Схема типового ОП з послідовним ВЗЗ на струмовий вхід

Колекторні струми транзисторів VT1, VT2 відбиваються у "струмових дзеркалах" і підсумовуються на вході повторювача А1, що служить для забезпечення низького вихідного опору підсилювача. Підсилення напруги тут відбувається в результаті перетворення різницевого струму колекторів транзисторів VT5, VT6 в напругу на високому вхідному опорі А1. При цьому коефіцієнт посилення на постійному струмі і низьких частотах підсилювача з розімкненим колом ВЗЗ рівний відношенню цього опору до загального опору ланцюга інвертуючого входу. Із замкнутим колом ВЗЗ коефіцієнт підсилення можна знайти з наближеного співвідношення, зручного для якісної оцінки частотних властивостей підсилювача:

$$U_{ВХ} \Big/ U_{ВИХ} = \frac{1 + R2/R1}{1 + j\omega C1R2}. \qquad (3.1)$$

З цього співвідношення виходить, що коефіцієнт передачі на низьких частотах тут, як і у звичного ОУ, визначається відношенням опорів резисторів R1, R2, а на високих залежить від ємності коректуючого конденсатора С1. При цьому частоту, на якій підсилення падає на 3 дБ, можна виразити таким чином:

$$f_{-3} = \frac{1}{2\pi \cdot C1R2}. \qquad (3.2)$$

Останнє співвідношення показує, що частотна смуга підсилювача із струмовим ВЗЗ не залежить від опору резистора R1, відповідним вибором якого можна забезпечити необхідний коефіцієнт передачі. При цьому смуга частот не змінюватиметься обернено пропорційно до підсилення (як у звичних ОП) і підсилювач з невисокою частотою одиничного підсилення зможе мати непогані частотні властивості при великому підсиленні. Крім цього, оскільки струм перезарядки конденсатора С1 приблизно рівний струму інвертуючого входу, визначуваному зовнішніми колами, теоретично можна одержати необмежену швидкість наростання вихідної напруги. В результаті цього частотна смуга для великого сигналу стає практично рівною малосигнальній. Тут варто обмовитися, що на практиці швидкість наростання і смуга підсилення все-таки обмежені деякими величинами, а наведені співвідношення справедливі для обмеженого діапазону опору резисторів R1, R2 і їх відношення.

Описана структура (рисунок 3.1) приваблива для побудови ППЗЧ, оскільки окрім високих динамічних характеристик вона повністю симетрична, проста в реалізації і має всього один каскад підсилення напруги, проте у неї є і недоліки — невисока точність на постійному струмові і складність реалізації на її основі інвертуючого підсилювача. Низькоомний інвертуючий вхід викликає труднощі при побудові УМЗЧ по інвертуючій схемі, яка є більш прийнятною через відсутність спотворень, обумовлених синфазним вхідним сигналом.

На рисунку 3.2 зображена дещо модернізована схема, зручна для побудови інвертуючого підсилювача. Як видно, на відміну від попередньої схеми, замість „струмових дзеркал” включений симетричний каскад зі спільним базом (VT3, VT4), що є повторювачем струму, внаслідок чого високоомний вхід в цій схемі стає інвертуючим.

Видно, що, змінюючи опір резистора R3 обернено пропорційно до коефіцієнта передачі кола ВЗЗ 1+R2/R1, можна, також отримати незалежність частотної смуги підсилення від коефіцієнта передачі. Струм перезарядки конденсатора С1 приблизно рівний струму низькоомного входу, тому і швидкість наростання вихідної напруги в цій схемі теж може бути дуже великою. Таким чином, остання схема здатна реалізувати такі ж високі динамічні характеристики, як і перша. Тут, проте, є одне "але". Річ у тому, що в структурі, зображеній на рисунку 3.1, підсилювач напруги, споживаючи невеликий струм спокою, здатний забезпечити значний струм перезарядки конденсатора С1. Іншими словами, працює він в режимі класу АВ. Звідси випливає одна з основних переваг ОП із струмовим входом — мале споживання енергії. У схемі ж, зображеній на рисунку 3.2, підсилювач напруги працює тільки в режимі класу А, тобто максимальний струм перезарядки конденсатора С1, що розвивається, рівний струму спокою, що протікає через резистори R4, R5. Відповідно, цей струм завідомо повинен бути заданий, виходячи з вимог швидкодії підсилювача.

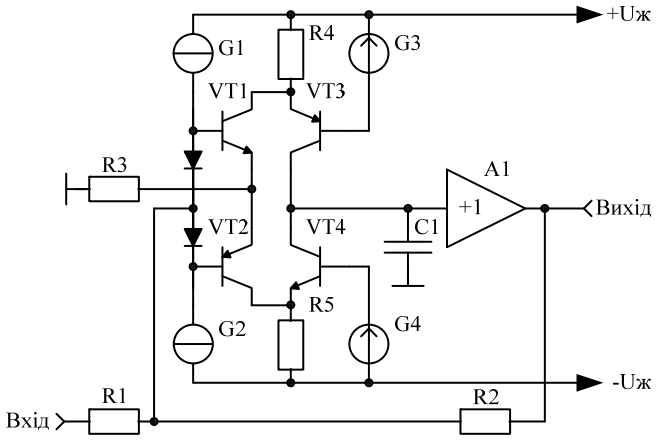


Рисунок 3.2 – Схема ОП з каскадами зі спільним базом

Проте недолік даної схеми для попередніх підсилювачів не є суттєвим, оскільки струм, споживаний ними не перевищує 2-5% від струму, споживаного

всім пристроєм, а робота його в класі А сприяє підвищенню його лінійності. Отже, попередній ПЗЧ буде побудовано з попереднім каскадом за схемою на рисунку 3.2. До даного каскаду не висувається вимог забезпечення значного вихідного струму, оскільки його навантаженням буде каскад підсилення потужності, зібраний на ПТР, ввімкнених по схемі зі спільним стоком.

3.1 Електричний розрахунок вхідного лінійного підсилювача

Даний каскад призначений для доведення рівня вхідної напруги давачів до рівня 0,775 В на вході попереднього лінійного підсилювача. Оскільки у вузлі змішування, що являє собою подільник, сигнал послаблюється у 3 рази, вхідний підсилювач повинен це послаблення компенсувати. Слід також врахувати, що рівень сигналу 0,775 В з вузла змішування повинен забезпечуватись при 75%-му введенні регулятора рівня від максимального положення, тобто отримане значення коефіцієнта передачі вхідного підсилювача слід збільшити в 1,25 рази. Отже:

$$K_U = \frac{0{,}775}{0{,}5} \cdot 3 \cdot 1{,}25 = 5{,}81\, p\, (\approx 15{,}3\, \partial Б). \qquad (3.3)$$

Каскад повинен бути побудований по схемі неінвертуючого.

Викреслюємо електричну принципову схему підсилювача (рисунок 3.3):

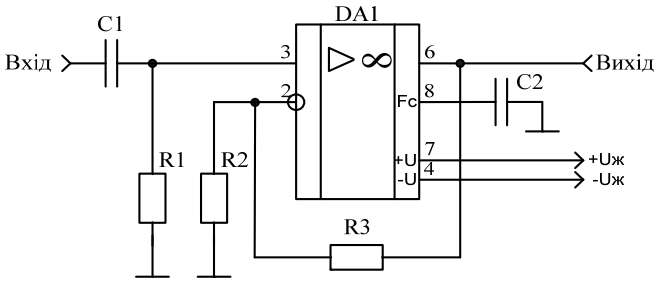


Рисунок 3.3 – Схема електрична принципова вхідного лінійного підсилювача

Висхідні дані:

Коефіцієнт передачі, дБ – 15,3 (5,81 р.);

Діапазон робочих частот, Гц – 200…2000;

Частотні спотворення, дБ – 0;

Вхідний опір, кОм – 47;

Напруга живлення, В – ±15.

В якості ОП в даній схемі застосуємо швидкодіючий ОП КР544УД2.

Перевіримо можливість використання даного ОП в схемі регулятора.

Максимальне підсилення, що здатний забезпечити обраний ОП на верхній межі робочого діапазону:

$$\frac{f_{1ОП}}{F_B} \geq K_U; \quad \frac{15 \cdot 10^6}{2000} = 7500 > 5{,}81.$$

Отже, обраний ОП підходить.

Розрахуємо елементи схеми.

Резистор *R1* визначає вхідний опір каскаду і приймається рівним 47 кОм.

Задаємось величиною резистора *R2 = 27 кОм*. Тоді:

$$R3 = (K_U - 1) \cdot R2 = (5{,}81 - 1) \cdot 27000 = 129938 (Ом).$$

Приймаємо значення *R3 = 130 (кОм)*.

Величину ємності конденсатора *C1* при однакових умовах було розраховано.

Отже, *C1 = 2,0 (мкФ)*.

Проведемо перевірку на можливість нехтування частотними спотвореннями каскаду.

Визначимо частотні спотворення, що вносить ІМС у схему:

$$M_B = \frac{K_U}{K_\beta};$$

$$K_\beta = \frac{K_0}{1 + K_0 \cdot \beta}; \qquad (3.4)$$

$$K_0 = \frac{f_1}{F_B} = \frac{15 \cdot 10^6}{2000} = 7500;$$

$$\beta = \frac{1}{K_U} = \frac{1}{5{,}81};$$

$$K_\beta = \frac{7500}{1 + \left(\frac{7500}{5{,}81}\right)} = 5{,}8;$$

$$M_B = \frac{5{,}81}{5{,}77} = 1{,}007 \approx 0{,}06 (дБ).$$

Отже, оскільки значення M_B значно менші за допустимі, ними можна знехтувати.

Ємність конденсатора *С2* вибирається, виходячи з ТУ на мікросхему і приймається рівною 20 пФ.

За розрахованими значеннями резисторів і конденсаторів виберемо згідно Е рядів стандартні елементи:

R1 – С2-23 - 0,125 Вт – 47 кОм ±5%;

R2 – С2-23 - 0,125 Вт – 20 кОм ±5%;

R3 – С2-23 - 0,125 Вт – 11 кОм ±5%;

С1 – К10-17б – 25 В – 2,0 мкФ ±5%;

С2 – К10-17б – 25 В – 20 пФ ±5%.

3.2 Електричний розрахунок попереднього лінійного підсилювача

Оскільки вхідна напруга від здавачів може бути різною за полярністю використовуємо інвертуючий підсилювач.

Викреслюємо електричну принципову схему підсилювача (рисунок 3.4):

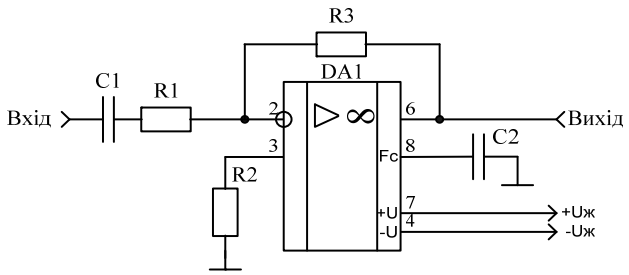


Рисунок 3.4 – Схема електрична принципова попереднього лінійного підсилювача

Висхідні дані:

Коефіцієнт передачі, дБ – 2,22 (1,29 р.);

Діапазон робочих частот, Гц – 100…1000;

Частотні спотворення, дБ – 0;

Вхідний опір, кОм – 47;

Напруга живлення, В – ±15.

В якості ОП в даній схемі застосуємо швидкодіючий ОП КР544УД2.

Даний ОП було перевірено на можливість використання при коефіцієнті передачі рівному 5,81. Отже він підходить і для даного каскаду з коефіцієнтом передачі 1,29.

Розрахуємо елементи схеми. Для неї:

$$K_U = \frac{R3}{R1}. \qquad (3.5)$$

Резистор *R1* визначає вхідний опір каскаду і приймається рівним 47 кОм. Тоді:

$$R3 = K_U \cdot R1 = 1{,}29 \cdot 47000 = 60630\,(Ом).$$

Оскільки стандартного резистора такого номіналу не існує, використаємо два з'єднані паралельно резистора опорами 100 кОм та 160 кОм.

Резистор *R2* призначений для зменшення дрейфу нуля ОП і орієнтовно вибирається зі співвідношення:

$$R2 \approx 0{,}05...0{,}5 \cdot \frac{R1 \cdot R3}{R1 + R3} = 0{,}05 \cdot \frac{47000 \cdot 60630}{47000 + 60630} = 1323\,(Ом).$$

Приймаємо величину резистора *R2 = 1,5 кОм*.

Величину ємності конденсатора *C1* при однакових умовах було розраховано в п.3.1. Отже, *C1 = 2,0 мкФ*.

Перевірка частотних спотворень не проводиться, оскільки її було проведено в п.3.2 при рівних умовах.

Ємність конденсатора *C2* вибирається, виходячи з ТУ на мікросхему і приймається рівною 20 пФ.

За розрахованими значеннями резисторів і конденсаторів виберемо згідно Е рядів стандартні елементи:

R1 – С2-23 - 0,125 Вт – 47 кОм ±5%;

R2 – С2-23 - 0,125 Вт – 1,5 кОм ±5%;

R3 – С2-23 - 0,125 Вт – 100 кОм ±5%;

С2-23 – 0,123 Вт – 160 кОм ±5%;

С1 – К10-17б – 25 В – 2,0 мкФ ±5%;

С2 – К10-17б – 25 В – 20 пФ ±5%.

3.3 Електричний розрахунок буферного підсилювача

Оскільки даний каскад не повинен інвертувати фазу, він виконується по схемі неінвертуючого.

Викреслюємо електричну принципову схему підсилювача (рисунок 3.5):

Висхідні дані:

Коефіцієнт передачі, дБ – 0 (1,0 р.);

Діапазон робочих частот, Гц – 200…10000;

Вхідний опір, кОм – 47;

Частотні спотворення, дБ – 0;

Напруга живлення, В – ±15.

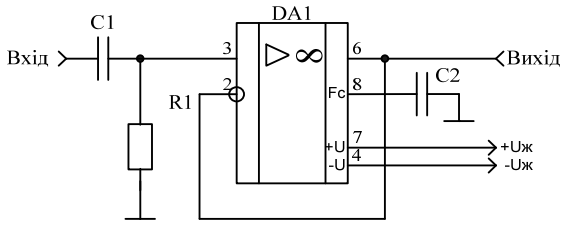


Рисунок 3.5 – Схема електрична принципова буферного підсилювача

В якості ОП в даній схемі застосуємо швидкодіючий ОП КР544УД2.

Даний ОП було перевірено на можливість використання при коефіцієнті передачі рівному 5,81, отже він підходить і для даного каскаду з коефіцієнтом передачі 1.

Електричний розрахунок даного каскаду зводиться до вибору розв'язуючої ємності *C1* та резистору *R1*, що визначає вхідний опір схеми.

Величину ємності конденсатора *C1* при однакових умовах було розраховано в п.3.1. Отже, *C1 = 2,0 мкФ*.

Із умов узгодження величина вхідного опору прийнята рівною 47 кОм, тоді R1 = 47 кОм.

Ємність конденсатора *C2* вибирається, виходячи з ТУ на мікросхему і приймається рівною 20 пФ.

3.4 Електричний розрахунок мікрофонного підсилювача

Планується, що розробляєма радіоохоронна система буде передавати голосові повідомлення, які будуть надиктовуватись через мікрофон. Мікрофонний підсилювач доцільно виконати на спеціалізованій інтегральній мікросхемі SSM2017 фірми Analog Devices. Дана мікросхема являє собою надмалошумлячий підсилювач з програмованим коефіцієнтом підсилення.

Основні технічні характеристики мікросхеми:

Коефіцієнт передачі, р. – 100…1000;

Відношення с/ш при $K_U=1000$, дБ – 60;

Коефіцієнт гармонік при $K_U=1000$, % – 0,01;

Вхідний опір, кОм – 100;

Мінімальний опір навантаження, Ом – 500;

Макс. вхідна напруга, В – ±4,5;

Напруга живлення, В – ±15;

Макс. струм споживання, мА – 15.

Основою даного підсилювача є мікросхема SSM2017. Простота реалізації та високі показники роблять доцільним її застосування у конструкції. Навісні елементи складають вхідне коло (*VD1-VD4*, *L1-L2*, *R1-R2* та *C1*) та коло фільтрації напруги живлення (*C2-C5* та *L3-L4*). Резистор *R3* визначає коефіцієнт підсилення мікросхеми.

Викреслюємо електричну принципіальну схему підсилювача:

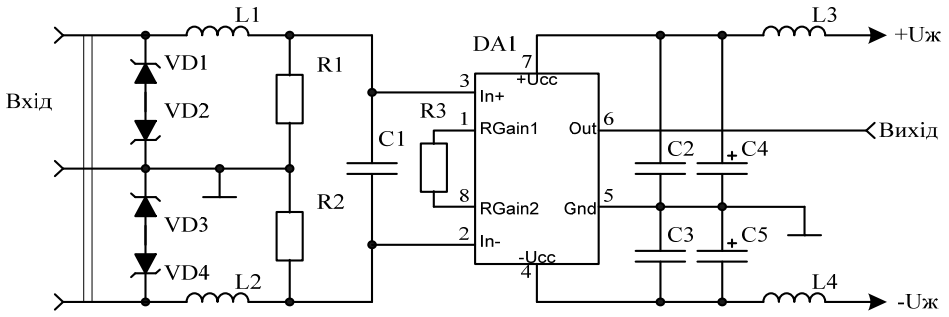


Рисунок 3.6 – Схема електрична мікрофонного підсилювача

Розрахунок даного каскаду зводиться до розрахунку вхідного фільтру *L1,L2-R1,R2-C1*, вибору захисних стабілітронів *VD1-VD4* та розрахунку резистору *R3*.

Вхідний фільтр призначений для придушення радіозавад з частотами вище 1 МГц. Розрахунок ведеться за типовими співвідношеннями:

$$L1 + L2 \approx \frac{1{,}41 \cdot (R1 + R2)}{2 \cdot \pi \cdot f_{зр}}; \quad C1 \approx \frac{1}{2{,}82 \cdot \pi \cdot f_{зр} \cdot (R1 + R2)}. \qquad (3.6)$$

Резистори R1 та R2 визначають вхідний опір мікрофонного підсилювача. Задаємось значеннями *R1=R2=1 кОм.*

Тоді:

$$L1 + L2 \approx \frac{1{,}41 \cdot (510 + 510)}{2 \cdot 3{,}14 \cdot 1 \cdot 10^{6}} = 228 \cdot 10^{-6}\ (Гн);$$

$$C1 \approx \frac{1}{2{,}82 \cdot 3{,}14 \cdot 1 \cdot 10^{6} \cdot (510 + 510)} = 0{,}11 \cdot 10^{-9}\ (Ф).$$

Приймаємо стандартні значення *L1=L2=100 мкГн*, *C1=120 пФ*.

Стабілітрони *VD1-VD4* призначені для запобігання потрапляння високої напруги на вхід мікросхеми. За паспортом вхідна напруга не повинна перевищувати ±4,5 В. Оскільки стабілітрони ввімкнені зустрічно-послідовно, слід врахувати падіння напруги на відкритому прямозміщенному p-n-переході, що складає 0,7 В. Обираємо стабілітрони КС133А з напругою стабілізації 3,3 В. Тоді результуюча напруга стабілізації складе *3,3 + 0,7 = 4,0 В*, що задовольняє ТУ на мікросхему.

3.5 Розрахунок смугового резонансного фільтру

Шлейфи сигналізації можуть досягати досить великої довжини і на них можуть формуватись завади. для відфільтровування завад вводимо всхему резонансний фільтр. Розрахуємо смугові резонансні фільтри з багатоконтурним зворотнім зв’язком (СФ1, СФ2).

Дані для розрахунку СФ1:

R1=1 кОм; R2=100 кОм; R5=100 кОм; C1=4700 пФ; f_1=300 Гц, f_2=1 кГц,

Знайдемо верхню та нижню граничні смуги пропускання:

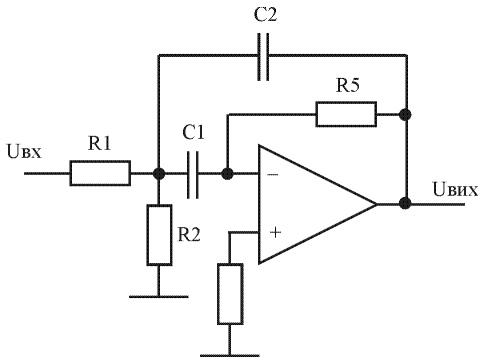


Рисунок 3.7 – Схема смугового фільтра з багатоконтурним зворотнім зв’язком

$$\omega_2=2\pi f_2;\ \omega_1=2\pi f_1,$$

$$\omega_2=2\cdot 3,14\cdot 1000=6280 \text{ рад/с};\ \omega_1=2\cdot 3,14\cdot 300=1884 \text{ (рад/с)}.$$

Смуга пропускання:

$$\Delta\omega = \omega_0\xi = \omega_2 - \omega_1, \tag{3.7}$$

$$\Delta\omega = 6280 - 1884 = 4396\,(рад/с).$$

Резонансна частота:

$$\omega_0 = \sqrt{\omega_2\omega_1}, \tag{3.8}$$

$$\omega_0 = \sqrt{6280\cdot 1884} = 3439,7(рад/с).$$

Знайдемо значення ємності С2 з формули:

$$\omega_0 = \sqrt{\frac{1}{R_5C_1C_2}\left(\frac{1}{R_1}+\frac{1}{R_2}\right)}; \tag{3.9}$$

$$C_2 = \frac{R_1+R_2}{\omega_0{}^2C_1R_1R_2R_5}; \tag{3.10}$$

$$C_2 = \frac{100\cdot 10^3 + 1\cdot 10^3}{3439,7^2\cdot 4700\cdot 10^{-12}\cdot 1\cdot 10^3\cdot 100\cdot 10^3\cdot 100\cdot 10^3} = 181,65\,(нФ).$$

Коефіцієнт затухання коливання

$$\xi = \sqrt{\frac{1}{R_5\left(\frac{1}{R_1}+\frac{1}{R_2}\right)}}\left[\sqrt{\frac{C_1}{C_2}}+\sqrt{\frac{C_2}{C_1}}\right]; \tag{3.11}$$

$$\xi = \sqrt{\frac{1}{100\cdot 10^3\left(\frac{1}{1\cdot 10^3}+\frac{1}{100\cdot 10^3}\right)}}\left[\sqrt{\frac{4700\cdot 10^{-12}}{181{,}65\cdot 10^{-9}}}+\sqrt{\frac{181{,}65\cdot 10^{-9}}{4700\cdot 10^{-12}}}\right] = 0{,}63.$$

Коефіцієнт підсилення

$$K_0 = -\frac{R_5}{R_1}\cdot\frac{1}{1+\frac{C_2}{C_1}}; \qquad (3.12)$$

$$K_0 = -\frac{100\cdot 10^3}{1\cdot 10^3}\cdot\frac{1}{1+\frac{181{,}65\cdot 10^{-9}}{4700\cdot 10^{-12}}} = -2{,}5.$$

Дані для розрахунку СФ2:

R1=1 кОм; R2=100 кОм; R5=100 кОм; C1=4700 пФ; f_1=1000 Гц, f_2=3,4 кГц,

Знайдемо верхню та нижню граничні смуги пропускання:

$$\omega_2=2\pi f_2;\ \omega_1=2\pi f_1,$$

ω_2=2·3,14·3400=21352 рад/с; ω_1=2·3,14·1000=6280 (рад/с).

Смуга пропускання:

$$\Delta\omega = \omega_0\xi = \omega_2 - \omega_1, \qquad (3.13)$$

$$\Delta\omega = 21352 - 6280 = 15072\,(рад/с).$$

Резонансна частота:

$$\omega_0 = \sqrt{\omega_2\omega_1}, \qquad (3.14)$$

$$\omega_0 = \sqrt{21352 \cdot 6280} = 11579{,}7(рад/с).$$

Знайдемо значення ємності С2 з формули:

$$\omega_0 = \sqrt{\frac{1}{R_5 C_1 C_2}\left(\frac{1}{R_1} + \frac{1}{R_2}\right)}; \tag{3.15}$$

$$C_2 = \frac{R_1 + R_2}{\omega_0^2 C_1 R_1 R_2 R_5};$$

$$C_2 = \frac{100 \cdot 10^3 + 1 \cdot 10^3}{11579{,}7^2 \cdot 4700 \cdot 10^{-12} \cdot 1 \cdot 10^3 \cdot 100 \cdot 10^3 \cdot 100 \cdot 10^3} = 16{,}026\,(нФ).$$

Коефіцієнт затухання коливання:

$$\xi = \sqrt{\frac{1}{R_5\left(\frac{1}{R_1} + \frac{1}{R_2}\right)}}\left[\sqrt{\frac{C_1}{C_2}} + \sqrt{\frac{C_2}{C_1}}\right]; \tag{3.16}$$

$$\xi = \sqrt{\frac{1}{100 \cdot 10^3\left(\frac{1}{1 \cdot 10^3} + \frac{1}{100 \cdot 10^3}\right)}}\left[\sqrt{\frac{4700 \cdot 10^{-12}}{16{,}026 \cdot 10^{-9}}} + \sqrt{\frac{16{,}026 \cdot 10^{-9}}{4700 \cdot 10^{-12}}}\right] = 0{,}5.$$

Коефіцієнт підсилення:

$$K_0 = -\frac{R_5}{R_1} \cdot \frac{1}{1 + \frac{C_2}{C_1}}; \tag{3.17}$$

$$K_0 = -\frac{100 \cdot 10^3}{1 \cdot 10^3} \cdot \frac{1}{1 + \frac{16{,}026 \cdot 10^{-9}}{4700 \cdot 10^{-12}}} = -22{,}7.$$

3.6 Розрахунок підсилювача низьких частот

Планується, що розробляємо радіоохоронна система буде передавати голосові повідомлення, тому для забезпечення достатнього рівня вихідного сигналу використовуємо кінцевий підсилювач низьких частот. Вихідні дані для розрахунку:

$P_{вих}$=0,1 Вт; $R_н$=240 Ом; $К_н$=0,1%; $М_н$=0,5 дБ; $М_в$=0,1 дБ;

$Е_к$=9 В; $К_р$(дБ)=10 дБ; $F_н$=400 Гц; $F_в$=3,5 кГц.

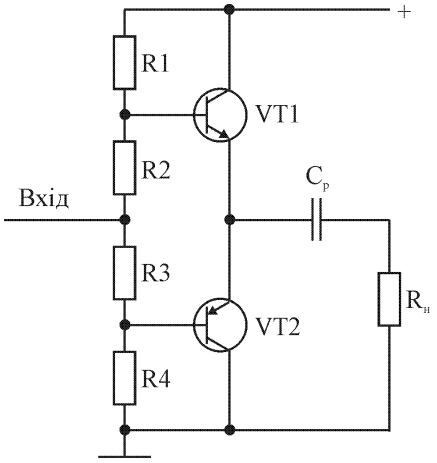


Рисунок 3.8 – Підсилювач низької частоти

Визначаємо на вихідних характеристиках кінцевих транзисторів значення амплітуди напруги на колекторі.

$$U_{кmin(T1,\ T2)} \approx 1 \text{ (В)}.$$

Знаходимо амплітуду імпульсу колекторної напруги та струму:

$$U_{КМ(T1,T2)} = \frac{E_К}{2} - U_{К\min(T1,T2)};$$

$$U_{КМ(T1,T2)} = \frac{9}{2} - 1 = 3{,}5\,В;$$

$$I_{KM(T1,T2)} = 2\frac{P_{вих}}{U_{KM(T1,T2)}}; \quad (3.18)$$

$$I_{KM(T1,T2)} = 2\frac{0,1}{3,5} = 0,057\,(A);$$

$$P_{вих} = \frac{U_{KM(T1,T2)} \cdot I_{KM(T1,T2)}}{2}; \quad (3.19)$$

$$P_{вих} = \frac{3,5 \cdot 0,057}{2} = 0,1\,(Bm).$$

Розраховуємо середнє значення струму, що споживається від джерела транзисторами кінцевого каскаду Т1, Т2:

$$I_{K0} \geq (0,01...0,1) I_{KM(T1,T2)}; \quad (3.20)$$

$$I_{K0} \geq 0,02 \cdot 0,057 = 1,14\,(мА);$$

$$I_{K\max} = I_{KM(T1,T2)} + I_{K0}; \quad (3.21)$$

$$I_{K\max} = 0,057 + 0,00114 \approx 2,2\,мА < I_{K\max.доп} = 100\,мА.$$

Вибираємо транзистори VT1-КТ3102В, VT2-КТ3107Г параметри яких:

КТ3102В	КТ3107Г
$I_к$=100 мА;	$I_к$=100 мА;
$U_{кe}$=30 В;	$U_{кe}$=30 В;
h_{21}=400;	h_{21}=220;
$C_к$=6 пФ;	$C_к$=7 пФ;

На статичних характеристиках транзисторів КТ3102В (КТ3107Г) рисунку 3.9 будуємо динамічну характеристику. По вхідних характеристиках транзисторів визначаємо відповідне значення:

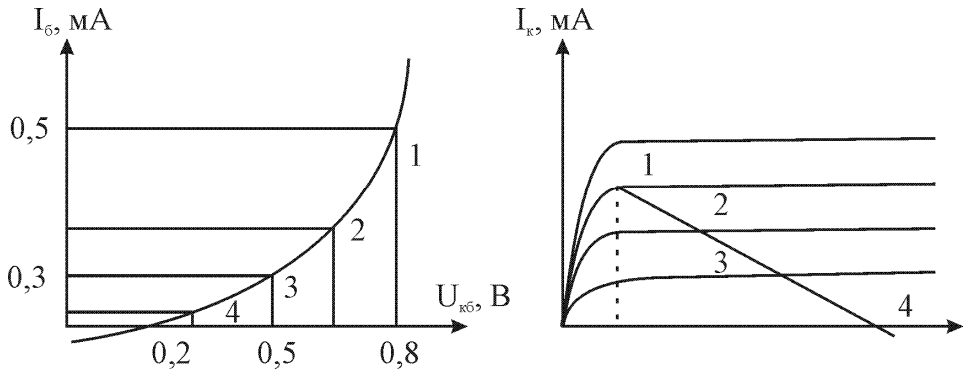


Рисунок 3.9 – Статичні характеристики транзисторів КТ3102В (КТ3107Г)

$I_{бм(Т1,\ Т2)}$=0,5 мА; $I_{б0(Т1,\ Т2)}$=0,1 мА; $U_{б0(Т1,\ Т2)}$=0,2 В; $U_{бм(Т1,\ Т2)}$=0,9 В,

Визначаємо потужність, що розсіюється на колекторі кожного з них.

$$P_{вх} = (U_{КМ} + U_{бМ})\frac{I_{бм}}{2}; \qquad (3.22)$$

$$P_{вх} = (3{,}5 + 0{,}8)\frac{0{,}5 \cdot 10^{-3}}{2} = 1\,(мВт).$$

Що не перевищує максимальної потужності операційного підсилювача.

Визначаємо вхідний опір змінному струму ділянки база-емітер транзисторів VT1, VT2.

$$R_{вх.пл.\sim} = \frac{(U_{бМ} + U_{КМ})}{I_{бм}}; \qquad (3.23)$$

$$R_{вх.пл.\sim} = \frac{(0{,}8 + 3{,}5)}{0{,}5 \cdot 10^{-3}} = 8{,}6\,(кОм).$$

Визначаємо коефіцієнт підсилення потужності і по напрузі:

$$K_p = 10 \lg \frac{P_{вих}}{P_{вх}}; \qquad (3.24)$$

$$K_p = 10 \lg \frac{0,1}{0,01} = 10 (дБ);$$

$$K_U = \frac{U_{км}}{U_{км} + U_{бм}}; \qquad (3.25)$$

$$K_U = \frac{3,5}{3,5 + 0,8} = 0,813.$$

Розраховуємо коефіцієнт нелінійних спотворень підсилювача потужності.

а) Загальний коефіцієнт нелінійних спотворень складного кінцевого каскаду дорівнює сумі коефіцієнта нелінійних спотворень каскадів на транзисторі Т1, Т2. Розрахунок проводимо методом п’яти ординат:

$$R_{г(Т1, Т2)}=(0,2...0,5)R_{вх.пл.\sim},$$
$$R_{г(Т1, Т2)}=0,4 \cdot 8,6 \cdot 10^3=3,44 \text{ (кОм)}.$$

б) Будуємо прохідну характеристику $I_к=f(E_г)$, рисунок 3.10, де $E_г$ – напруга еквівалентного генератора, $E_{гі}=I_{бі}R_г+U_{бі}$, де $R_г=0,5R_{вх.пл.\sim}$. Розрахуємо значення $E_г$ для всіх значень колекторного струму.

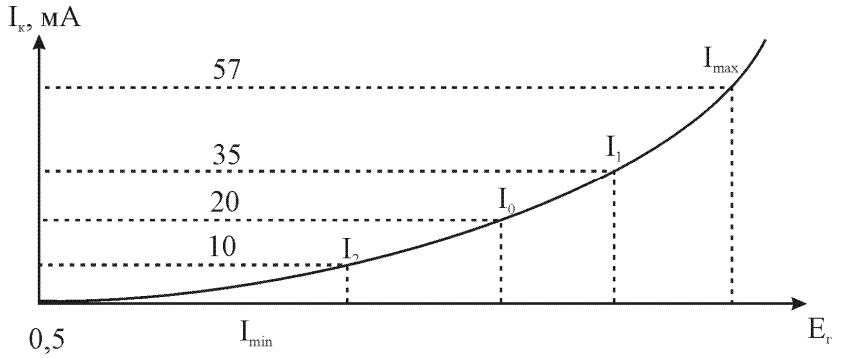


Рисунок 3.10 – Прохідна характеристика $I_к=f(E_г)$

$$E_{г1}=0,5\cdot10^3\cdot3,44\cdot10^3+0,8=2,52,$$

$$E_{г2}=0,4\cdot10^3\cdot3,44\cdot10^3+1,3=1,97,$$

$$E_{г3}=0,3\cdot10^3\cdot3,44\cdot10^3+0,45=1,48,$$

$$E_{г4}=0,1\cdot10^3\cdot3,44\cdot10^3+0,6=0,544,$$

в) На прохідній характеристиці відстань по осі напруги ділимо на чотири рівні відрізки та визначаємо значення додаткових величин колекторних струмів: $I_{max}=57$, $I_1=35$, $I_0=20$, $I_2=10$, $I_{min}=0,5$.

г) Для методу п’яти ординат визначаємо п’ять значень величин струму і амплітуди 1,2,3 та 4-ї гармонік колекторного струму та середньої складової:

$$I_{1m}=\frac{(I_{max}-I_{min}+I_1-I_2)}{3}; \qquad (3.26)$$

$$I_{1m}=\frac{(57-0,5+35-10)}{3}=27,16\,(мА);$$

$$I_{2m}=\frac{(I_{max}+I_{min}-2I_0)}{4}; \qquad (3.27)$$

$$I_{2m} = \frac{(57 + 0{,}5 - 2 \cdot 20)}{4} = 4{,}125\,(мА);$$

$$I_{3m} = \frac{(I_{max} - I_{min} - 2(I_1 - I_2))}{6}; \qquad (3.28)$$

$$I_{3m} = \frac{(57 - 0{,}5 - 2(35 - 10))}{6} = 1{,}5\,(мА);$$

$$I_{4m} = \frac{(I_{max} + I_{min} - 4(I_1 + I_2) + 6I_0)}{12}; \qquad (3.29)$$

$$I_{4m} = \frac{(57 + 0{,}5 - 4(35 + 10) + 6 \cdot 20)}{12} = 2{,}5\,(мА).$$

д) Розраховуємо коефіцієнт нелінійних спотворень:

$$Кг_{се} = \sqrt{\frac{(I_{2mb})^2 + (I_{3m})^2 + (I_{4mb})^2}{I_{1m}}}, \qquad (3.30)$$

де: b=0,1…0,15-коефіцієнт асиметрії.

$$Кг_{се} = \sqrt{\frac{(4{,}125 \cdot 0{,}1)^2 + (1{,}5)^2 + (2{,}5 \cdot 0{,}1)^2}{27{,}16}} = 0{,}058.$$

Дійсна величина коефіцієнта нелінійних спотворень:

$$Кг_{се(Т1,\ Т2)} = Кг_{се}(1 - Ku_{еп}); \qquad (3.31)$$

де:

$$Ku_{еп(T1,T2)} = \frac{U_{км(T1,T2}}{U_{км(T1,T2)} + U_{бм(T1,T2)}};$$

$$Ku_{еп(T1,T2)} = \frac{3,5}{3,5+0,9} = 0,81;$$

Звідси:

$$Кг_{се(T1,T2)}=0,058(1-0,81)=0,01\%.$$

Визначаємо величини розділової ємності $C_р$ та її тип:

$$C_р = \frac{1}{2}\pi F_н R_н \sqrt{(M_н^2 - 1)}; \qquad (3.32)$$

$$C_д = \frac{1}{2}\cdot 3,14\cdot 400\cdot 240\sqrt{(1,059^2-1)} = 4,7(ìêÔ).$$

По ряду Е-24 $C_р$=К-50-6-4,7 мкФ×63В.

Уточнюємо величину частотних спотворень в області вищих частот:

$$Мв_{ск} = \sqrt{1+(2\pi F_в)^2 \tau_{еп(T1,T2)}^2}; \qquad (3.33)$$

$$Мв_{ск} = \sqrt{1+(2\cdot 3,14\cdot 3500)^2 (1,84\cdot 10^{-9})^2} = 1(0дБ);$$

$$C_0=C_к\cdot h_{21emin}+C_м,$$

$$C_0=6\cdot 10^{-12}\cdot 400+20\cdot 10^{-12}=2,42\cdot 10^{-9}(Ф).$$

Постійна часу емітерного повторювача дорівнює:

$$\tau_{еп} = \frac{C_0 R_н}{1} + S_0 R_н; \qquad (3.34)$$

$$\tau_{en} = \frac{2{,}42 \cdot 10^{-9} \cdot 4}{1} + 1 \cdot 4 = 1{,}84 \cdot 10^{-9} (c);$$

$$Мв_{розр.} = Мв_{тр} + Мв_{ск} < Мв_{попер.розрах}.$$

Розраховуємо опори, що задають зміщення транзисторів:

$$I_{под} = 10 \cdot I_{б;}$$

$$I_{под} = 10 \cdot 0{,}1 = 1 \text{ (мА)};$$

$$R_{заг} = \frac{E_{ж}}{I_{под}}; \qquad (3.35)$$

$$R_{заг} = \frac{9}{1 \cdot 10^{-3}} = 9 (кОм);$$

$$R_{1,4} = \frac{E_{ж} - U_{бVT1,VT2}}{I_{под} + I_{б}}; \qquad (3.36)$$

$$R_{1,4} = \frac{9 - 4{,}3}{1 \cdot 10^{-3} + 0{,}1 \cdot 10^{-3}} = 4{,}27 (кОм);$$

$$R_2 = R_3 = R_{\Sigma} - 2R_{1,2};$$

$$R_2 = R_3 = 9 - 8{,}54 = 230 \text{ (Ом)};$$

Вибираються номінали опорів із стандартного ряду Е24:

$R_1 = R_4 = 4{,}3$ кОм±5% типу С2-23-0,125

$R_2 = R_3 = 220$ Ом±5% типу С2-23-0,125

Для перевірки проведених електричних розрахунків можна використати комп’ютерне моделювання.

3.7 Комп’ютерне моделювання

Проведемо комп’ютерне моделювання смугових фільтрів. Для цього застосуємо схемний редактор Electronics Workbench.

Спочатку промоделюємо смуговий фільтр із смугою пропускання 300-1000 Гц. Схема фільтра в Electronics Workbench буде мати вигляд на рисунку3.11.

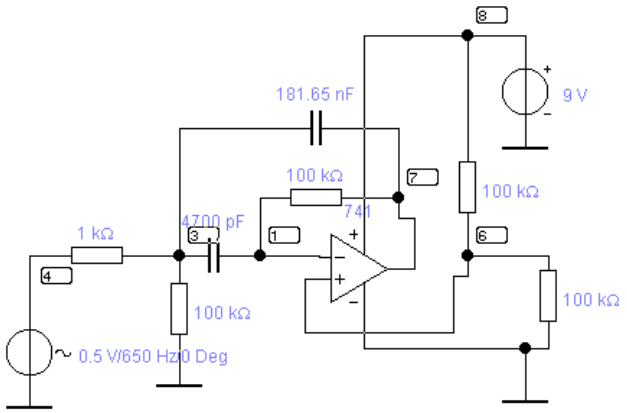


Рисунок 3.11 – Схема фільтра 1

АЧХ та ФЧХ цього фільтра яку ми отримали в схемному редакторі Electronics Workbench 5.0. буде мати вигляд на рисунку 3.12.

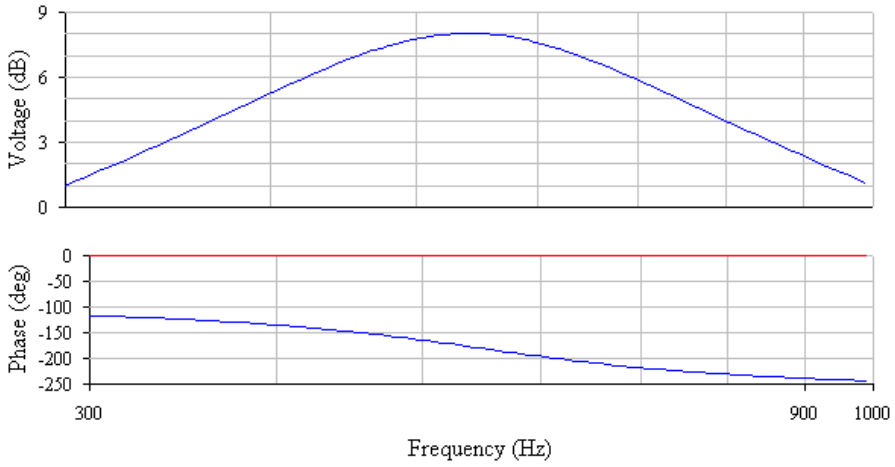


Рисунок 3.12 – АЧХ та ФЧХ фільтра 1

Промоделюємо смуговий фільтр із смугою пропускання 1000-3400 Гц. Схема фільтра в Electronics Workbench буде мати вигляд на рисунок 3.13.

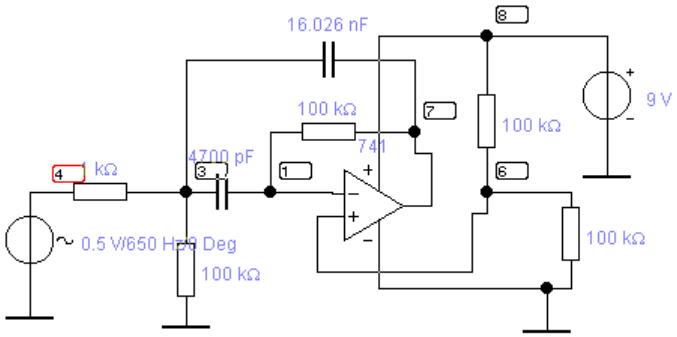


Рисунок 3.13 – Схема фільтра 2

АЧХ та ФЧХ цього фільтра яку ми отримали в схемному редакторі Electronics Workbench 5.0. буде мати вигляд на рисунку 3.14.

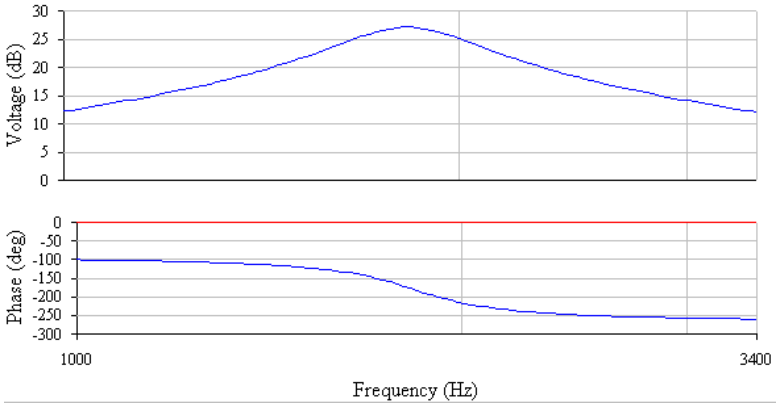


Рисунок 3.14 – АЧХ та ФЧХ фільтра 2

Отримані результати комп'ютерного моделювання співпадають з очікуваними та з результатами чисельного розрахунку який ми проводили в електричних розрахунках для смугових фільтрів. Фільтри влаштовують нас своєю вибірністю та формою АЧХ.

3.8 Висновки до третього розділу

Результат дослідження АЧХ свідчить про запас по частоті, що впливає на перехідну характеристику. Схема має менші спотворення по вищим частотам ніж по нижчим, що видно з АЧХ, але значення нерівномірності АЧХ лежить в межах 3 дБ. Фазовий зсув лежить в межах від'ємних значень кутів спостерігається зміна кута в -160 дБ. На частоті 1,25 ГГц. Схема забезпечує струм зміщення і накачування.

Сучасні мікроконтролери та мікросхеми вміщують вище приведені схеми, тому схема електрична принципова буде певним чином відрізнятись. Схема електрична принципова приведена в додатках.

ВИСНОВКИ

Системи обмеження доступу є складним комплексом апаратного та програмного забезпечення. Системи обмеження мають взаємодіяти як з проводовими так і безпровідними мережами.

В сучасних системах використовуються величезна кількість засобів охорони. Це різноманітні датчики виявлення руху на охороняємо му обкті, датчики відкривання, датчики розбивання скла.

Для охоронних систем великою проблемою є реалізація передачі сповіщень від охоронних систем до центру моніторингу, або до власника об’єкту за умови відсутності дротяної телефонної мережі, яка часто використовувалась для цих цілей.

Стільникові системи зв’язку надають величезні можливості для створення систем нового зразка. Перевагою таких систем є моніторинг охороняємого об’єкту безпосередньо власником зі свого стільникового телефону, а канал передачі даних надає унікальну можливіст створення систем з передачою швидкісних кодованих протоколів обміну для реалізації пультової охорони.

В роботі проаналізовано принцип реалізації стандарту GSM та загальні принципи побудови стільникової мережі. Проведено електричні розрахунки вхідного лінійного підсилювача, попереднього лінійного підсилювача, буферного підсилювача, мікрофонного підсилювача, а також виконано комп’ютерне моделювання.

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. ДСТУ 3008-95. Документація, звіти у сфері науки і техники.Структура і правила оформления.- Київ.: Держстандарт України, 1995.

2. Банкет В, Л. Современные и перспективные системы спутниковой связи. Уч. пособие, Одесса УГАС им. А.С. Попова, 1996.

3. Кветний Р.Н. Основи техніки передачі інформації / Р.Н. Кветний та ін. – Вінниця. ВДТУ 2002. – 220 с.

4. http://www.pricemaster.kiev.ua // ціни Online.

5. Терещук Р.М. и др. Полупроводниковые приёмно-усилительные устройства. Справочник радиолюбителя. – Киев.: Наукова думка, 1989, 273с.

6. Одинцов Б.В. Системи космічного зв'язку / Б.В. Одинцов, Е.А. Сукачев, А.К. Гуцалюк, – навч. посібник, Одеса. – ОНАС ім О.С. Попова, 2008.

7. Банкет В. Л., Иващенко П. В., Геер А. Э., Цифровые методы передачи информации в спутниковых системах связи. Уч. пособие, Одесса, УГАС им. А.С. Попова, 1996.

8. Брагин А.С. Радиотелекоммуникационные системы. Часть 1. Тракты радиопередачи. – Киев.: НТУУ "КПИ", 2005. – 244 с.

9. Системы связи передвижной службы: Учебное пособие / Л. С. Чайников. – Київ. Світ знань, 2001.

10. Авдєєнко Г. Л. Методичні рекомендації до виконання лабораторних робіт, практичних та семінарських занять з дисциплін «Передавальні та приймальні пристрої», «Телекомунікаційні тракти прийому та передачі сигналів» (електронна версія).

11. Бойко Ю. М. Генерування та формування сигналів : метод. вказівки / Ю. М. Бойко, В. В. Мишан. – Хмельницький : ХНУ, 2011 – 85 с.

12. Гершунский Б.С. Расчет основных электронных и полупроводниковых схем в примерах. – Издательство Киевского университета, 1986, 136с.

13. Ткачук В.М. Радіопередавальні пристрої : навчальний посібник / В.М. Ткачук, С.М. Цирульник, Т.А. Петренко. – Вінниця : Т. П. Барановська, 2015. – 188 с.

14. Методи і засоби обробки небезпечних сигналів / [Азаров О. Д. Максименко Г .О., Хорошко В. О., Яремчук Ю. Є.]. – Вінниця: ВНТУ, 2005. – 282 с.

15. Хаізмон І. Я. Техніка передачі інформації. Функціональні вузли та схеми. Ч.1. / І. Я. Хаізмон. – Вінниця.: ВДТУ, 2000 р. – 143с.

16. Бойко Ю. М. Основи функціонування багатоканальних систем передачі інформації : навч. посіб. для ВНЗ / О. М. Шинкарук, Ю. М. Бойко, І. І. Чесановський. – Хмельницький : ХНУ, 2011. – 231 с.

17. Ткачук В. М. Радіопередавальні пристрої: навч. посібник / В. М. Ткачук, С. М. Цирульник, Т. А. Петренко. – Вінниця : Т.П. Барановська, 2015. – 188 с.

18. Калінін В.І. Математичні моделі та методика оцінки експлуатаційної надійності елементів і виробів електронної техніки Частина II / В.І. Калінін, О.А. Костюк, А.А. Грудин. – Вінниця ВДТУ, 1999,

ДОДАТКИ

Завідувачу кафедри автоматизації та
комп'ютерно-інтегрованих технологій
Валерію МАРТИНЮКУ
здобувача вищої студента, студента
Ярослава Шаламая,
4 курсу, гр. ТР1с-19-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

13.06.2022р.
дата

Ярослав Шаламай

Tue Jun 14 13:38:48 EEST 2022, Федула Микола Васильович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 2.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 8%**

ID: 105262 Назва: Бакалаврська кваліфікаційна робота Додано в БД: 2022-06-14 Автора: Шаламай Я. Керівники: Яновицький О.К. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	77133	660	4177 (5%)	46 (7%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK

Ім'я користувача:
Кафедра АКІТіТК

ID перевірки:
1011576534

Дата перевірки:
14.06.2022 14:19:43 EEST

Тип перевірки:
Doc vs Internet

Дата звіту:
14.06.2022 14:26:00 EEST

ID користувача:
100005862

Назва документа: **ШАЛАМАЙ_доступ (2)**

Кількість сторінок: **70** Кількість слів: **12160** Кількість символів: **89242** Розмір файлу: **596.00 KB** ID файлу: **1011446637**

15.5%
Схожість

Найбільша схожість: **5.83%** з Інтернет-джерелом (https://studopedia.ru/19_341275_tehnichni-zasobi-ohoroni.html)

15.5% Джерела з Інтернету	87	..... Сторінка 72

Пошук збігів з Бібліотекою не проводився

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	80

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРИ

АВТОМАТИЗАЦІЇ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Пристрій обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж

Автор: Ярослав Шаламай

Спеціальність: 172 Телекомунікації та радіотехніка

Освітня програма Телекомунікації та інформаційно-комунікаційні технології

Науковий керівник к.т.н., доц. Олександр ЯНОВИЦЬКИЙ

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнуті. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: Запозичення у розмірі 15,5%, що виявлені в роботі, містять посилання на відповідні джерела літератури, що використані в роботі. Результати конструкторського розділу не містять запозичень. Розроблена схема електрична та її опис є унікальними та також не містять запозичень. Робота приймається до захисту.

14.06.2022р.

Науковий керівник роботи: Олександр ЯНОВИЦЬКИЙ

Зав. каф. АКІТ Валерій МАРТИНЮК

МІНІСТЕРСТВО ОВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Ярослав Шаламай

Тема: Пристрій обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж

Спеціальність: 172 «Телекомунікації та радіотехніка»

Обсяг кваліфікаційної роботи

Кількість листів креслень 2 Кількість сторінок записки 72

1. Короткий зміст роботи та прийнятих рішень проведено розгляд тематики та економічне обґрунтування доцільності розробки блоку системи обмеження доступу, виконано розробку структурної схеми пристрою та його електричний розрахунок

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота повністю відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки та техніки і передових методів роботи: У першому розділі обґрунтовано доцільність розробки пристрою обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж.

4. Позитивні сторони роботи: в роботі розглянуто питання щодо використання стандарту 5G /4G в розрізі використання елементів тестування з вже існуючими мережами. В другому розділі показано взаємозв'язок між стандартом та існуючими мережами. В третьому розділі виконано розрахунки окремих складових пристрою. Оскільки блоку керування радіоохоронної системи стандарту GSM призначено в тому числі і для передачі голосових повідомлень на пульт поліції чи безпосередньо на телефон власника приміщення, що охороняється, тому були виконані розрахунки для окремих елементів аналогового каналу пристрою.

5. Негативні сторони роботи: в роботі присутні незначні стилістичні помилки, але наявні недоліки не зменшують важливість та повноту роботи

6. Оцінка графічного оформлення та пояснювальної записки роботи: -

7. Відгук про роботу в цілому: Робота виконана на достатньому рівні

8. Інші зауваження: -

9. Оцінка дипломної роботи: Розглянувши представлену роботу, вважаю, що робота заслуговує оцінки "відмінно" (4,50 , "B")

10. Рецензент (прізвище, ім'я, по батькові, місце роботи)
к.т.н., доцент каф. ТМІТ Костянтин ГОРЯЩЕНКО

«10» 06 2022р.

підпис

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ПРИСТРІЙ ОБМЕЖЕННЯ ДОСТУПУ ДО ОБ’ЄКТІВ ІНФРАСТРУКТУРИ ІЗ ЗАСТОСУВАННЯМ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Виконав:

студент 4 курсу, група ТР1с-19-1 Ярослав Шаламай

Керівник:

к.т.н., доцент Олександр ЯНОВИЦЬКИЙ

ЗАГАЛЬНІ ПОНЯТТЯ І ЗАВДАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Останнім часом широко розповсюджуються системи стільникового зв’язку. Охоронні системи також не залишились в стороні. Адже завжди було великою проблемою реалізації передачі сповіщень від охоронних систем до центру моніторингу, або до власника об’єкту за умови відсутності дротяної телефонної мережі, яка часто використовувалась для цих цілей. Тому розробники охоронних систем просто немогли не використати принцип стільникового зв’язку в своїх розробках.

Стільникові системи зв’язку надають величезні можливості для створення систем нового зразка. Перевагою таких систем є моніторинг охороняємого об’єкту безпосередньо власником зі свого стільникового телефону, а канал передачі даних надає унікальну можливіст створення систем з передачою швидкісних кодованих протоколів обміну для реалізації пультової охорони.

Система контролю та управління доступом зазвичай складається із серверів системи обмеження доступу (СКУД) – звичайних комп'ютерів, які управляють підключеними до них контролерами СКУД. Контролер (контрольна панель) – це спеціалізований високонадійний комп'ютер. У ньому зберігається інформація про конфігурацію, режими роботи системи, список людей, які мають право доступу до ресурсу, а також їх привілеї доступу до цього ресурсу. У найпростіших випадках мінімальний варіант контролера може бути вбудований у зчитувач, турнікет, замок або інший виконавчий пристрій.

СПОСОБИ ІДЕНТИФІКАЦІЇ

Існує два різні напрями в способах ідентифікації. Це ідентифікація з використанням електронних карт, і ідентифікація, що використовує біометричні параметри людини. Застосовуються наступні типи карт, кожному з яких відповідає певний тип зчтувача:

магнітні карти - прочитуються, при проведенні в певному напрямі і з певною швидкістю по щілині зчитувача. Магнітна смуга із записаною на ній інформацією нанесена на одну із сторін пластикової картки. Сучасні магнітні смуги виготовлені з матеріалів, що вимагають сильних магнітних полів для запису інформації і, відповідно, для її знищення, тому можна не боятися випадкового розмагнічування.

безконтактні радіочастотні (PROXIMITY) карти - найбільш перспективний на сьогодні тип карт. Безконтактні картки діють на відстані і не вимагають чіткого позиціонування, що забезпечує їх стійку роботу і зручність використання, високу пропускну спроможність. Для прочитування інформації з безконтактної картки її досить просто піднести до зчитувача.

карти Виганда - названі по імені вченого, такого, що відкрило сплав, що має прямокутну петлю гістерезису. Усередині карти розміщені відрізки дроти з цього сплаву, які при переміщенні повз прочитуючу голівку дозволяють рахувати інформацію.

штрих-кодові карти - на карту наноситься штриховий код. Існує складніший варіант - штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, прочитування відбувається в інфрачервоній області.

Touch - memory - металева пігулка, усередині якої розташований чіп. При торканні пігулки зчитувача, з пам'яті пігулки в контроллер пересилається унікальний код ідентифікатора. Досить дешеві і зручні.

КЛАСИФІКАЦІЯ СКУД ЗА СПОСОБОМ УПРАВЛІННЯ :

автономні - для управління одним або декількома пристроями, що перегороджують, без передачі інформації на центральний пульт і без контролю з боку оператора. Звичайно це прості СКУД, точніше електронні замки, які обмежують доступ в приміщення. До переваг таких систем можна також віднести можливість легкого видалення номера ключа з енергозалежної пам'яті системи при його втраті, таким чином, ключ, що знайшов, ніколи не зможе їм скористатися. Автономні системи знайшли застосування, як правило, на невеликих об'єктах (входи до житлових будинків, котеджі і тому подібне). Існують і автономні системи контролю доступу з функціями охорони.

централізовані (мережеві) - для управління пристроями, що перегороджують, за рахунок обміну інформацією з центральним пультом, для контролю (управління) з боку оператора. Мережеві системи контролю застосовуються там, де потрібно постійний контроль стану об'єкту, можливість оперативного втручання в роботу системи і отримання різних статистичних даних про рух персоналу.

універсальні - включаючі функції як автономних, так і мережевих систем, працюючі в мережевому режимі під управлінням центрального облаштування управління і що переходять в автономний режим при виникненні відмов в мережевому устаткуванні, в центральному пристрої або обриві зв'язку.

По кількості контрольованих точок доступу розрізняють:

- системи малої місткості (менше 16 точок);
- системи середньої місткості (не менше 16 і не більше 64 точок);
- системи великої місткості (64 точки і більше).

Класифікація по виду об'єктів контролю :

- для контролю доступу до фізичних об'єктів;
- для контролю доступу до інформації.

СУТЬ ТЕХНІЧНОЇ ПРОБЛЕМИ, ЯКА ВИНИКЛА НА СУЧАСНОМУ ЕТАПІ РОЗВИТКУ НАУКИ І ТЕХНІКИ

В кожній галузі народного господарства бувають етапи розвитку, при яких потрібен перехід на якісно новий підхід до вирішення проблем, наприклад перехід на нових технологічний процес, запровадження нових систем, станків тощо. Предметом дослідження став блок керування радіоохоронної системи стандарту GSM, що встановлюється на будь-якому охороняємому об’єкті і є серцем усієї системи.

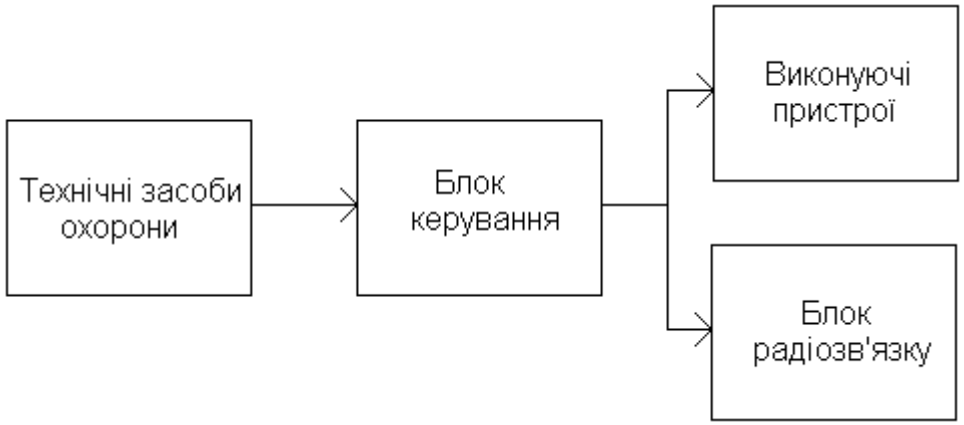


Рисунок 1 – Структура класичної побудови радіоохоронної системи

Класична побудова радіоохоронної системи (рисунок 1.1) в загальному вигляді складається з чотирьох частин:

1) Технічні засоби охорони;
2) Блок керування системою;
3) Виконуючі пристрої.
4) Блок радіозв’язку

ПРИНЦИП РЕАЛІЗАЦІЇ СТАНДАРТУ GSM

Загальноєвропейський стандарт GSM - перший у світі стандарт на цифрові ССРЗ, що передбачає їхнє створення в діапазоні 900 МГц і є основою стандарту **DCS1800** (діапазон 1800 МГц) з мікростільниковою структурою, прийнятого в даний час у Європі. Стандарт GSM реалізується в даний час і в Північній Америці в діапазоні 1900 МГц (**PCS-1900**).

В даний час популярність стандарту GSM настільки велика, що тепер він розуміється як глобальна система рухомого зв'язку. GSM і його варіанти - **DCS-1800** (Digital Cellular Systems 1800) і **PCS-1900** (Personal Communication Service), прийняті і розвиваються в Європі, Азії, Африці, Австралії і Північній Америці (по стану на лютий 1998 року цей стандарт прийнятий у 105 країнах). З огляду на цю обставину, абревіатура GSM, спочатку утворена з перших букв назви спеціальної групи (Group Special/Mobile), у даний час розшифровується як Global System for Mobile Communications (глобальна система для рухомого зв'язку).

Стосовно інших цифрових стандартів GSM забезпечує кращі енергетичні і якісні характеристики зв'язку, найвищі характеристики безпеки і конфіденційності зв'язку. Цей стандарт передбачає роботу передавачів у двох діапазонах частот: 890-915 МГц (для передавачів рухливих станцій), 935-960 МГц (для передавачів базових станцій). У цьому стандарті використовується вузькосмуговий багатостанційний доступ з тимчасовим поділом каналів (**NB TDMA**), що дозволяє організувати 8 фізичних каналів на кожній з 124 несучих частот.

ХАРАКТЕРИСТИКА ЦИФРОВОГО СТАНДАРТУ СТІЛЬНИКОВОЇ СИСТЕМ ЗВ'ЯЗКУ GSM

Характеристики стандарту	GSM (DCS1800, PCS1900)
Метод доступу	TDMA
Рознос частот, кГц	200
Кількість мовних каналів на несучу	8(16)
Швидкість перетворення мови, Кбіт/с	13 (6,5)
Алгоритм перетворення мови	RPE-LTP
Загальна швидкість передачі. Кбіт/с	270
Еквівалентна смуга частот на мовний канал, кГц	25 (12,5)
Необхідне відношення сигнал/шум, дБ	9
Метод рознесення	перемеження, стрибки по частоті
Радіус стільника, км	0,5-35
Робочий діапазон частот, МГц	935-960 (GSM) 890-915 (GSM) 1710-1785 (DCS) 1805-1880 (DCS)

ЕФІРНИЙ ІНТЕРФЕЙС GSM

Протокол обміну між мережею і опонентом по радіоканалу отримав назву ефірного інтерфейсу (U_m). Частотний канал - це смуга частот, яка відводиться для передачі інформації одного каналу зв'язку. При використанні методу TDMA (Time Division Multiple Access) в одному частотному каналі передається інформація декількох каналів зв'язку, тобто в одному частотному каналі розміщуються декілька фізичних каналів (ФК).

Канали трафіку TCH (Traffic Channels) поділяються на повношвидкісні (22,8 Кбіт/с - TCH/FS (із повношвидкісним кодуванням; F - Full - повний; S Speech - мова) і напівшвидкісні (11,4 Кбіт/с) - TCH/HS (H - Half- половина). Також передбачені канали трафіка для передачі даних зі швидкістю від 2,4 Кбіт/с до 9,6 Кбіт/с (TCH/F9.6, TCH/F4.8, TCH/H4.8 і т.п.).

Канали керування CCH (Control Channels) поділяються на 4 типи: віщальні BCCH (Broadcast Control Channels); загальні CCCH (Common Control Channels); виділені закріплені SDCCH (Standalone Dedicated Control Channels); суміщені (асоційовані) ACCH (Associated Control Channels).

Таблиця 1 – Класифікація і типові позначення каналів

Ознака	**Позначення**	**Назва каналу**
Напрямок зв'язку	F	Прямий (Forward)
	R	Зворотній (Reverse)
Тип каналу	L	Логічний (Logical)
	P	Фізичний (Physical)
Призначення каналу	A	Доступ (Access)
	P	Виклик (Paging)
	S	Сигналізація (Signaling)
	T	Трафік (Traffic)
	C	Керування (Control)
Спосіб організація зв'язку	A	Суміщений (Associated)
	B	Широкомовний (Broadcast)
	C	Загальний (Common)
	D	Виділений (Dedicated)
	SD	Автономний (Stand-alone)
Допоміжні канали	A	Допоміжний (Auxiliary)
	PL	Пілот-сигнал (Pilot)
	S або SYNC	Синхроканал (Synchronization)

СТРУКТУРНА СХЕМА СИСТЕМИ ОХОРОНИ

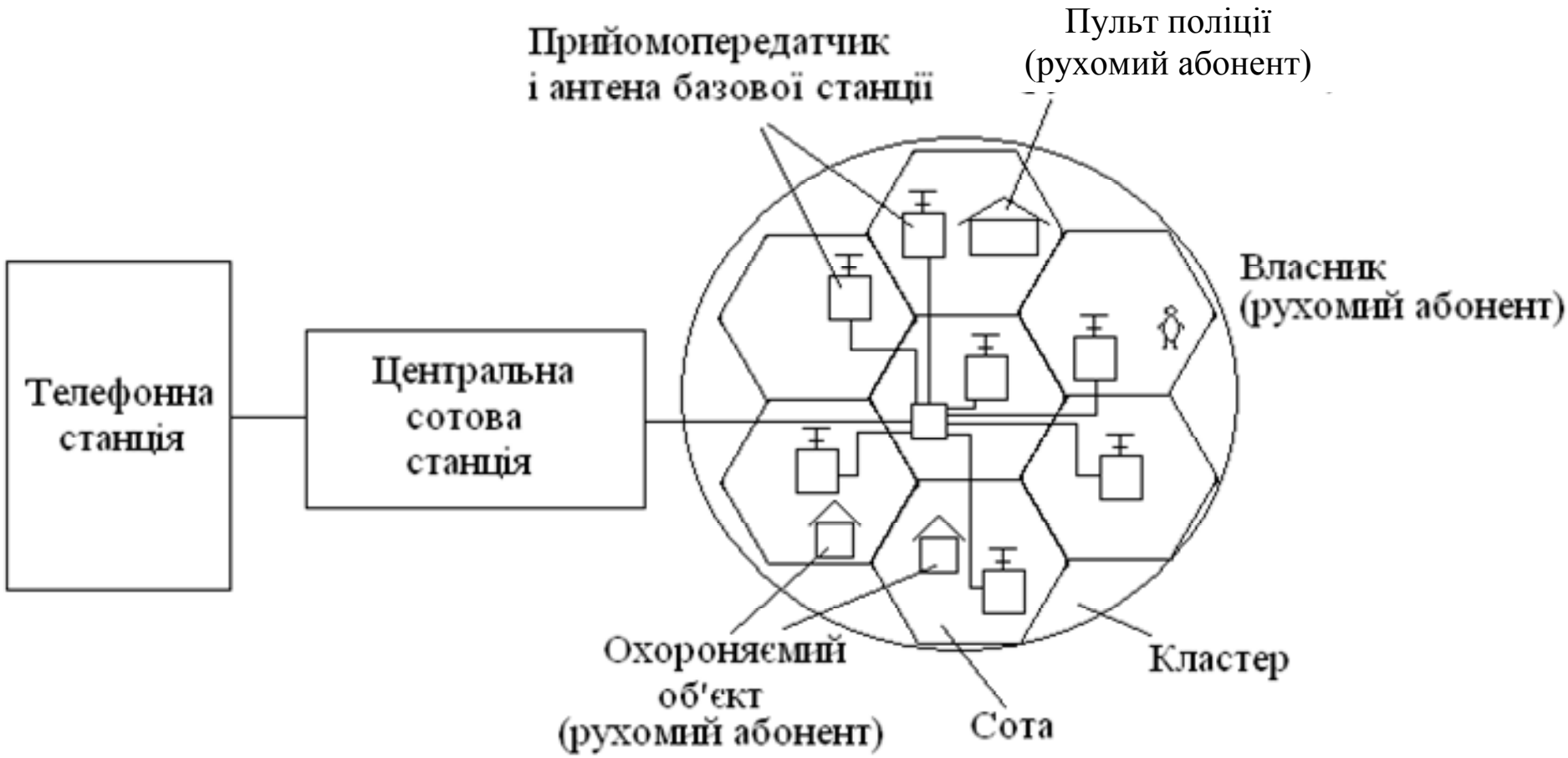


Рисунок 2 – Структурна схема системи охорони з використанням стільникової мережі

СТРУКТУРНА СХЕМА БЛОКУ КЕРУВАННЯ

Структурна схема блоку керування радіоохоронної системи, яка використовує стільникову мережу стандарту GSM для передачі сповіщень на пульт міліції чи власнику об’єкта, що охороняється, приведена на рис. 3.

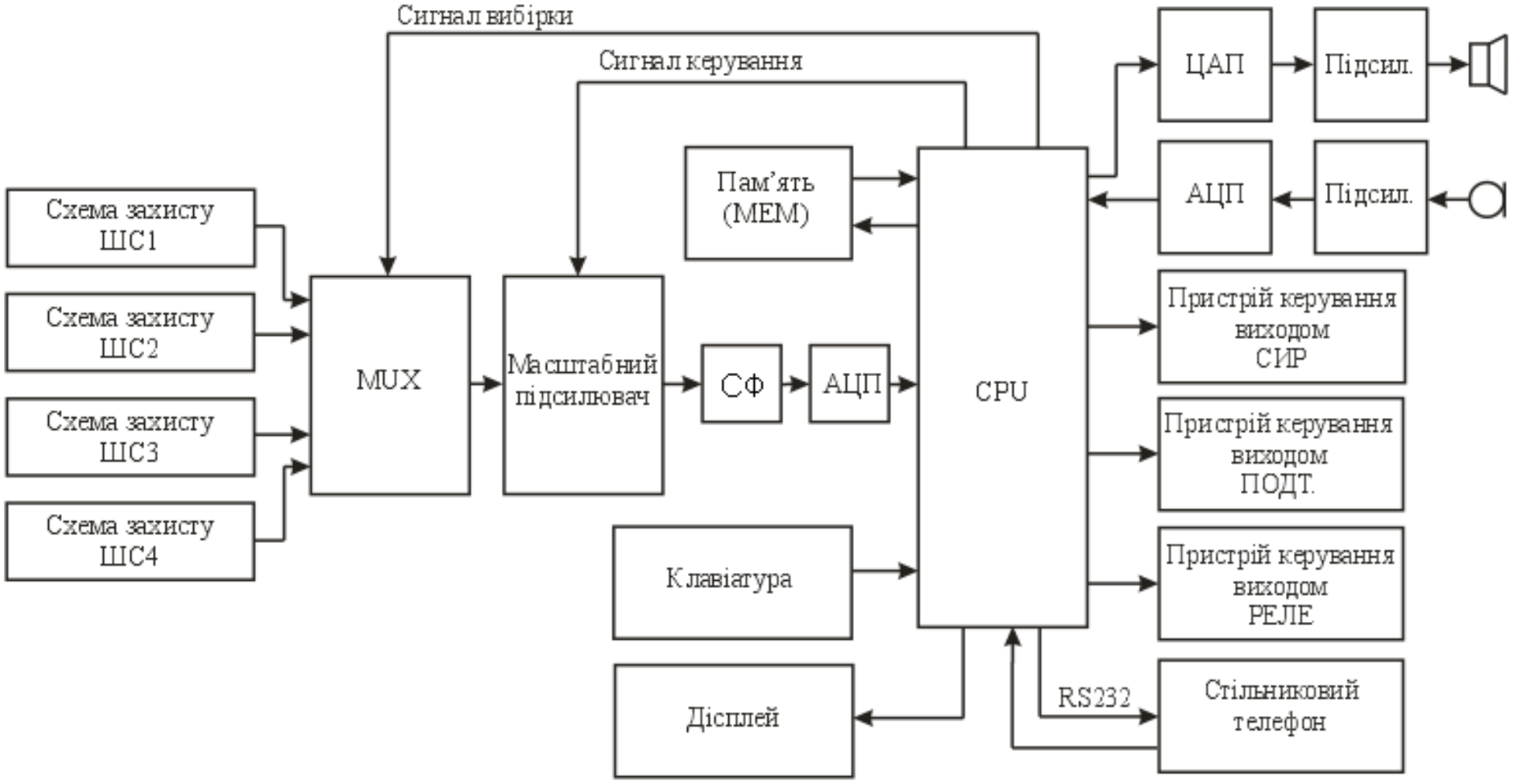


Рисунок 3 – Структурна схема радіоохоронної системи

ЕЛЕКТРИЧНИЙ РОЗРАХУНОК

Однією із функцій розробляємого блоку керування радіоохоронної системи стандарту GSM є передача голосових повідомлень на пульт поліції чи безпосередньо на телефон власника приміщення, що охороняється. Тому для зберігання та передачі цих повідомлень потрібні сигнали (повідомлення) достатнього рівня. Для забезпечення рівня таких сигналів можна використати звичайні підсилювачі на ОП.

Останнім часом в зарубіжній літературі з'явилися статті з описами ППЗЧ, побудованих на основі схеми ОП із струмовим входом (мається на увазі ОП з низькоомним інвертуючим входом, наприклад, серій AD8001, КМ1432УД1). Ці підсилювачі більш широкосмугові і мають високу швидкість наростання вихідної напруги. Така побудова підсилювача звукової частоти дозволяє значно знизити нелінійні спотворення в цілому і повністю позбавитися динамічних, що у результаті приводить до підвищення якості звуковідтворення.

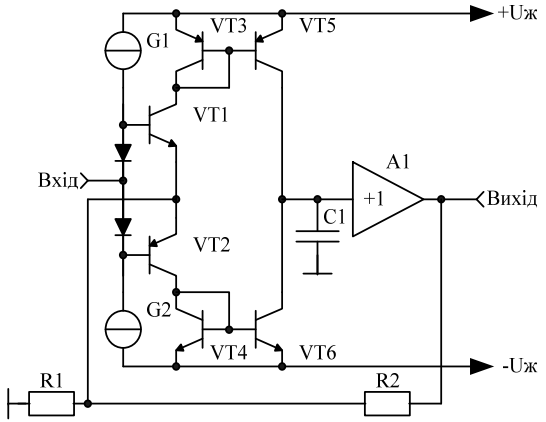


Рисунок 4 – Схема типового ОП з послідовним ВЗЗ на струмовий вхід

Структурна схема типового ОП з оберненим зв’язком на струмовий вхід показана на рисунку 4.

Він має вхідний підсилювач на транзисторах VT1, VT2 з ланцюгами зсуву G1, G2, VD1, VD2, два струмові дзеркала VT3-VT6 і вихідний неінвертуючий підсилювач A1 (резистори R1, R2 є елементами зовнішнього ВЗЗ).

Коефіцієнт підсилення можна знайти з наближеного співвідношення:

$$U_{BX} \Big/ U_{ВИХ} = \frac{1 + R2/R1}{1 + j\omega C1R2}. \qquad (1)$$

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ЕЛЕМЕНТІВ СХЕМИ

Проведемо комп'ютерне моделювання смугових фільтрів. Для цього застосуємо схемний редактор Electronics Workbench.

Спочатку промоделюємо смуговий фільтр із смугою пропускання 300-1000 Гц. Схема фільтра в Electronics Workbench буде мати вигляд на рис. 5.

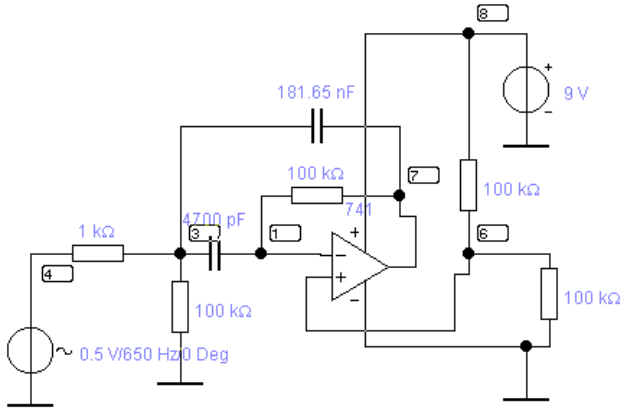


Рисунок 5 – Схема фільтра 1

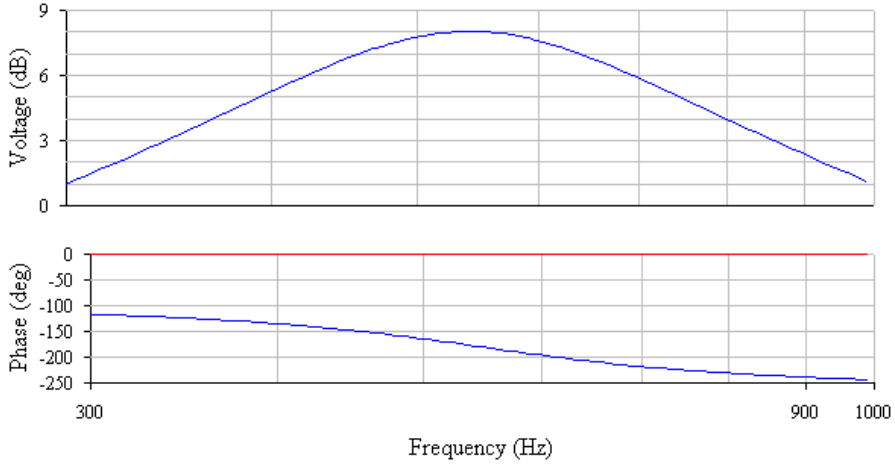


Рисунок 6 – АЧХ та ФЧХ фільтра 1

Промоделюємо смуговий фільтр із смугою пропускання 1000-3400 Гц. Схема фільтра в Electronics Workbench буде мати вигляд на рис. 7.

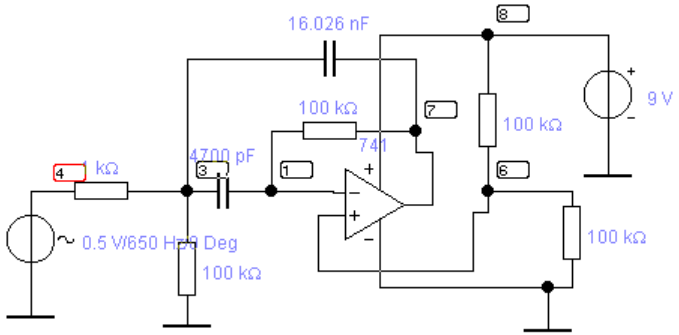


Рисунок 7 – Схема фільтра 2

АЧХ та ФЧХ цього фільтра яку ми отримали в схемному редакторі Electronics Workbench 5.0. буде мати вигляд на рис.8.

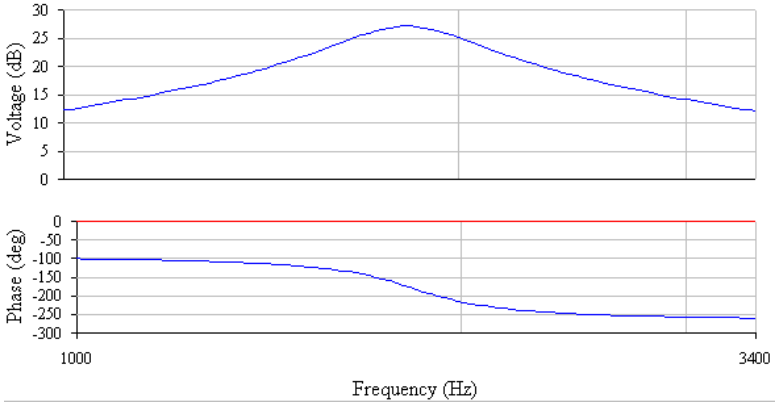


Рисунок 8 – АЧХ та ФЧХ фільтра 2

ВИСНОВКИ

Системи обмеження доступу є складним комплексом апаратного та програмного забезпечення. Системи обмеження мають взаємодіяти як з проводовими так і безпровідними мережами.

В сучасних системах використовуються величезна кількість засобів охорони. Це різноманітні датчики виявлення руху на охороняємо му обкті, датчики відкривання, датчики розбивання скла.

Для охоронних систем великою проблемою є реалізація передачі сповіщень від охоронних систем до центру моніторингу, або до власника об’єкту за умови відсутності дротяної телефонної мережі, яка часто використовувалась для цих цілей.

Стільникові системи зв’язку надають величезні можливості для створення систем нового зразка. Перевагою таких систем є моніторинг охороняємого об’єкту безпосередньо власником зі свого стільникового телефону, а канал передачі даних надає унікальну можливіст створення систем з передачою швидкісних кодованих протоколів обміну для реалізації пультової охорони.

В роботі проаналізовано принцип реалізації стандарту GSM та загальні принципи побудови стільникової мережі. Проведено електричні розрахунки вхідного лінійного підсилювача, попереднього лінійного підсилювача, буферного підсилювача, мікрофонного підсилювача, а також виконано комп’ютерне моделювання.

Поз. познач.	Найменування	Кіл.	Примітка
	КОНДЕНСАТОРИ		
C1	K50-35-35В-2200мкФ+-20%	1	
C2 C5	K50-35-63В-10мкФ±20%	7	
C16,C19			
C26,C32			
C35			
C3	SMD-0805-Z5V-50V-0,1мкФ	15	
C11-C14			
C15,C18			
C21,C22			
C23,C25			
C37,C33			
C36, C44			
C4, C6	K50-35-25В-100мкФ+-20%	3	
C34			
C7,C8	SMD-0805-NP0-63V-22пФ +-5%	2	
C38,C39	SMD-0805-NP0-63V-33пФ +-5%	2	
C17	K50-35-25В-47мкФ+-20%	1	
C20	K53-19-16В-4.7мкФ+-20%	1	
C24	K50-35-16В-220мкФ+-20%	1	
C28,C29	SMD-0805-Z5V-50V-0.01мкФ	2	
C30,C31	SMD-1206-Z5V-50V-1мкФ	6	
C37,C41			
C42,C43			
C40	K50-35-10В-2200мкФ+-20%(<50mOm)	1	

Зм.	Лист	№ докум.	Підпис	Дата	КВРТР.2019032.01.11 ПЕ		
Розроб.		Я.О.Шаламай			Пристрій обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж Перелік елементів	Літ.	Лист 1 / Листів 5
Перевір.		О.К.Яновицький					
Реценз.						ТР1С-19, ФІТ, ХНУ	
Н. Контр.							
Затверд.		В.В.Мартинюк					

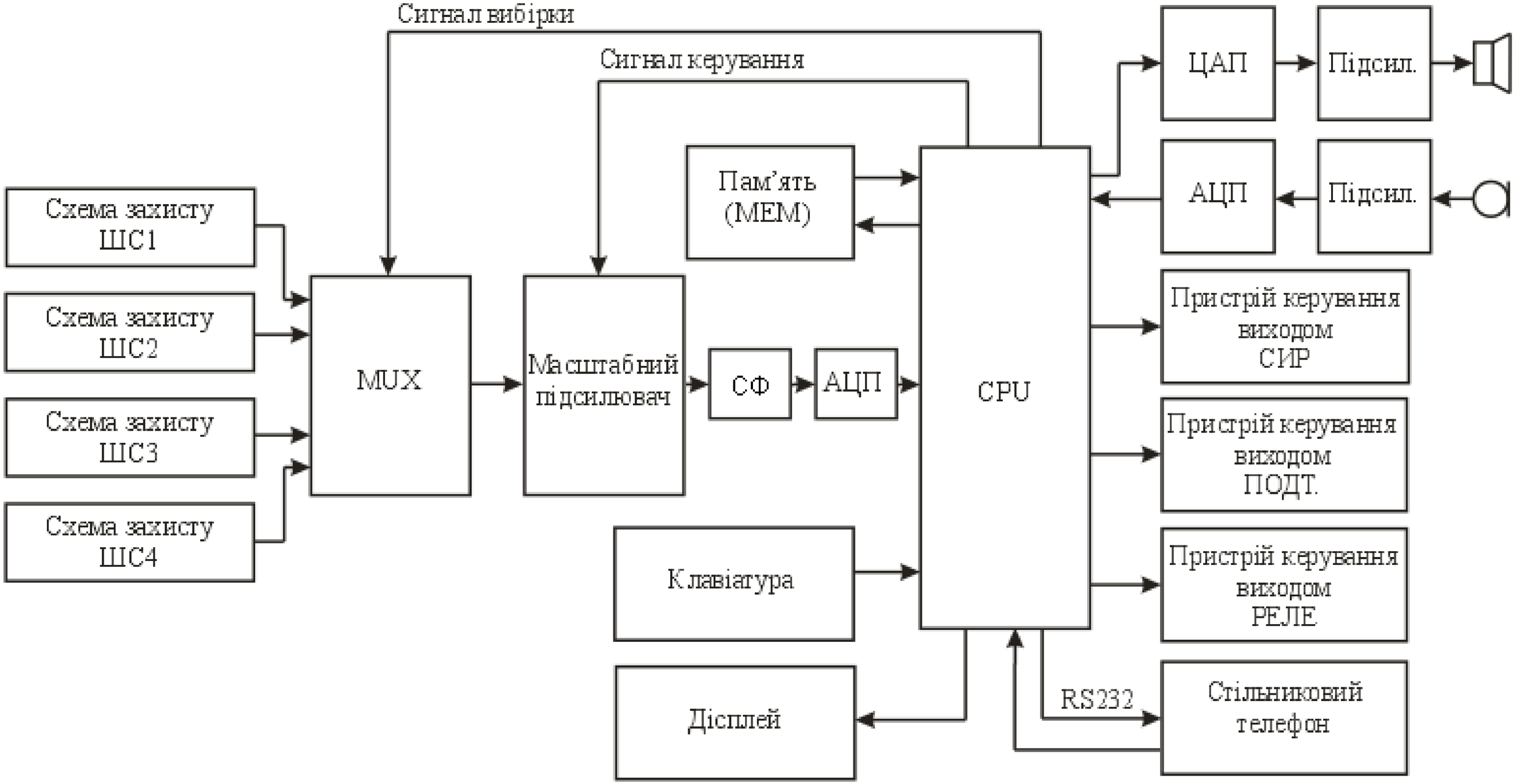
Поз. познач.	Найменування	Кіл.	Примітка
	МІКРОСХЕМИ		
DA1	LM317T National Semiconductor	1	
DA2	MC7805CT (MOTOROLA)	1	
DA3	PC817 (DIP4)	1	
DA4	LM350T National Semiconductor	1	
DD1	PIC16F877A-20/P	1	
DD2	ISD2560P (DIP28)	1	
DD3	MT8870DS (SOIC18)	1	
	РЕЗИСТОРИ		
R54	Резистори 595 – 0,5 Ом±10%	1	
	РЕЗИСТОРИ SMD-1206		
R17,R19	750 Ом±1%	6	
R21,R23			
R28,R36			
R40	220 Ом ± 5%	1	
R42	0 Ом	1	
	РЕЗИСТОРИ SMD-0805		
R1	75 Ом ±1%	1	
R2	100 Ом ±1%	1	
R3	120 Ом ±1%	1	
R4	2,2 кОм ±1%	1	
R5, R65	240 Ом ±1%	4	
R66, R76			
R6,R53	510 Ом ±5%	2	
R7,R11	10 кОм ±5%	18	
R16,R18			
R20,R22			

Поз. познач.	Найменування	Кіл.	Примітка
R29,R44			
R59,R67			
R68,R70			
R71,R72			
R75,R78			
R79,R84			
R8	39 кОм±5%	1	
R9,R10	3 кОм±1%	13	
R12,R27			
R32,R35			
R45,R48			
R49,R50			
R51,R52			
R83			
R14,R31	20 кОм±5%	7	
R34,R46			
R57,R58			
R61			
R30, R47	2 кОм±5%	2	
R39,R43	5,1 кОм ±5%	5	
R55,R60			
R63			
R56	51 кОм ±5%	1	
R62	470 кОм ±5%	1	
R64,R37	1 кОм ±5%	2	
R69	470 Ом ±5%	1	
R77,R80	100 кОм ±5%	2	
R33,R38	330 Ом ±5%	3	
R81			
R73, R74	220 Ом ±1%	2	
R82	300 кОм±5%	1	

Поз. обозн.	Наименование	Кол.	Примечание
	РЕЗИСТОРИ ПІДСТРОЄЧНІ		
RP2	3323P-1 кОм±5%	1	
	ТРАНЗИСТОРИ		
VT1-VT2	BC817 (Philips)	11	
VT4-VT6			
VT8, VT9			
VT10, VT12			
VT14, VT15			
VT7, VT11	IRF7204	3	
VT13			
	ДІОДИ		
VD2	Діодний місток 2KBB80R (KBL4005)	1	2A
VD3, VD4	Диод КД708А	10	
VD5, VD7			
VD8, VD21			
VD22, VD24			
VD25, VD26			
VD6	Діод LL4448	1	SMD
VD9	Супрессор SMAJ 15A	1	
VD19	Супрессор SMAJ 5A	1	
VD20	Стабілітрон SMD 6V2	1	
VD23	Стабілітрон SMD 9V1	1	
VD27	Супрессор 3V9	1	
HL1	Світлодіод L934 YD	1	
VD10, VD11	Супрессор SMAJ 28	5	
VD12, VD13			
VD1			

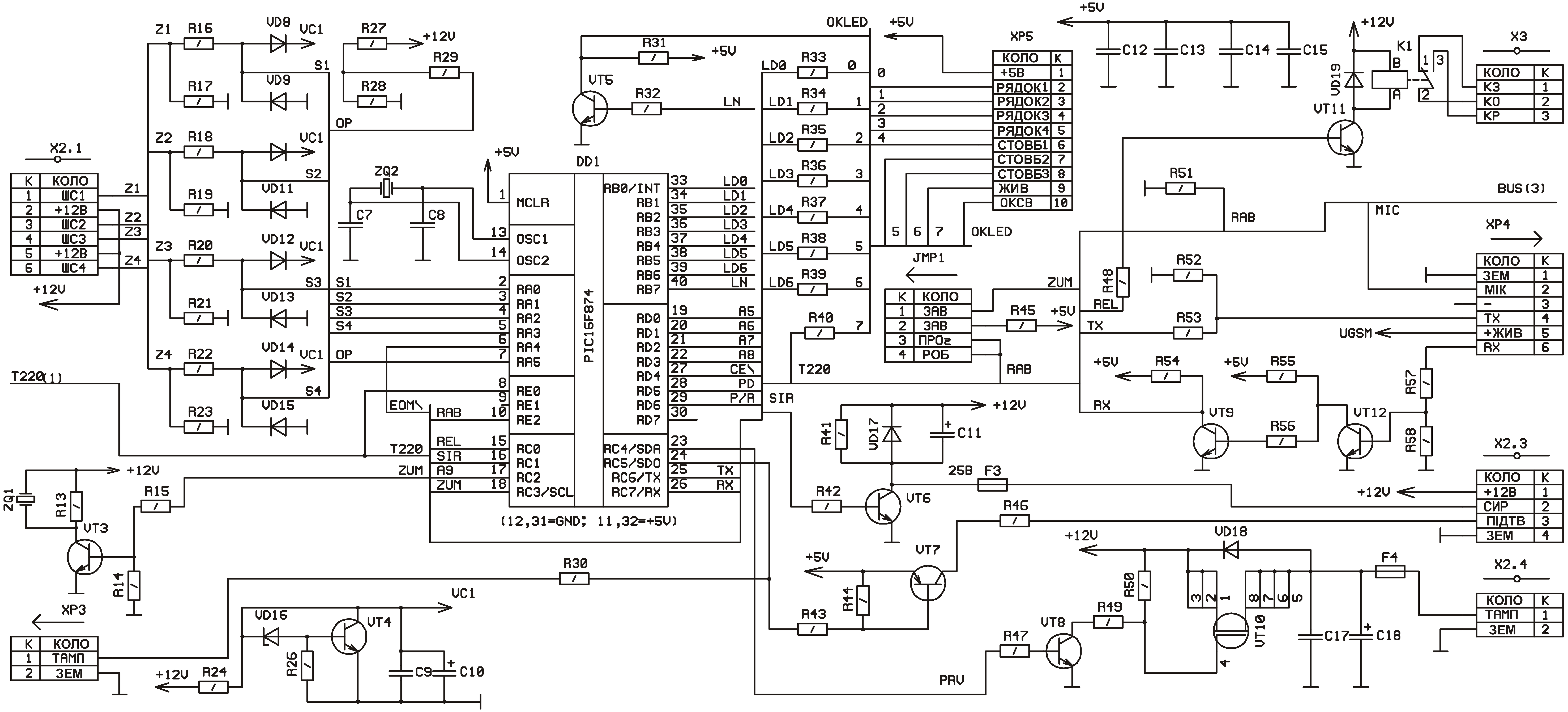
Поз. познач.	Найменування	Кіл.	Примітка
	РОЗ'ЭМИ		
X1,X2	Клемний роз'єм TL203V-2P	9	
X4			
X3	Клемний роз'єм TL203V-3P	1	
XP3,XP7	Штирьовий з'єднувач PLS2	2	
	Джампер MJO	1	
JMP1	Штирьовий з'єднувач PLS4	1	
	Джампер MJO	1	
XS8	Роз'єм FLE-130-01-G-DV	1	
XS9	Тримач SIM 91228-0002	1	
XP4	Штирьовий з'єднувач PLS5 (2)	1	
ZQ1	Кварцевий резонатор 16 МГц	1	
ZQ2	Кварцевий резонатор 3,579545 МГц	1	
RT1,RT2	Термістор FRX 185-60	2	
RT3,RT4	Термістор FRX 110-60	2	
K1	Реле MP3-2001210	1	
SB1	Мікрокнопка SWT - 2/9,5	1	
RU1	Варістор 331	1	
MIC1	Електретний мікрофон MKE338 (MKE333)	1	

					КВРТР.2019032.01.11 ПЕ	Лист
Зм.	Лист	№ докум.	Підпис	Дата		5



					КВРТР.2019032.01.11 Е1	
Зм.	Арк.	№ докум.	Підпис	Дата		
Виконав		Я.О. Шкляний			Пристрій обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж Схема структурна	Літ. / Аркуш / Аркушів
Перевір.		О.К.Яновицький				
Т.Контр.						Лист 1
Реценз.						
Н.Контр.						ТР1с-19, ФІТ, ХНУ
Затв.		В.В.Мартинюк				

Інв. № орига. | Підпис і дата | Взам. інв. № | Інв. № дубл. | Підпис і дата



Зм.	Арк.	№ докум.	Підпис	Дата
Виконав		Я.О. Шаламай		
Перевір.		О.К.Яновицький		
Т.Контр				
Реценз.				
Н.Контр				
Затв.		В.В.Мартинюк		

КВРТР.2019032.01.11 Е3

Пристрій обмеження доступу до об'єктів інфраструктури із застосуванням телекомунікаційних мереж
Схема електрична принципова

Літ.	Аркуш	Аркушів

Лист 1

ТР1с-19, ФІТ, ХНУ

Підпис і дата | Інв. № дубл. | Взам. інв. № | Підпис і дата | Інв. № ориг.