Міністерство освіти і науки України
Тернопільський національний економічний університет
Факультет комп’ютерних інформаційних технологій
Кафедра спеціалізованих комп’ютерних систем

Расевич Віктор Русланович

ВДОСКОНАЛЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ОХОРОННОЇ GSM СИСТЕМИ

напрям підготовки 151- Автоматизація та комп’ютерно інтегровані технологі
фахове спрямування - Комп’ютеризовані системи управління та автоматика

Дипломна робота за освітньо-кваліфікаційним рівнем "магістр"

Виконав студент групи АКІТм-21
В.Р. Расевич
_____

Науковий керівник:
к.т.н., Гуменний П.В.
_____

Дипломну роботу допущено до захисту:
"____"_____20___ р.

Завідувач кафедри
_____ Я.М. Николайчук

Тернопіль 2018

Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем
Освітній ступінь "магістр"
спеціальність: 151 – Автоматизація та комп'ютерно-інтегровані технології
магістерська програма – Автоматизація та комп'ютерно-інтегровані технології

"ЗАТВЕРДЖУЮ"
Завідувач кафедри СКС
_____ Я.М.Николайчук
"____" _____20__ р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ
Расевич Віктор Русланович
(прізвище, ім'я по-батькові)

1. Тема магістерської роботи
Вдосконалення автоматизованої системи охоронної GSM системи / Improvement of automated system of guarded GSM system

керівник роботи к.т.н.,Гуменний П.В.
затверджені наказом по університету від "14" листопада 2017 р. № 804

2. Строк подання студентом закінченої магістерської роботи 16 листопада 2018р.

3. Вихідні дані до роботи:
1. Схеми управління автомобілем
2. Автоматизовані схеми автосигналізацій
3. Електронних засоби для взлому автомобільних сигналізацій
4. Вимоги до технічної експлуатації системи

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)**:**
1. Аналіз видів охоронних автомобільних сигналізацій
2. Характеристика автоматизованих схем автосигналізації
3. Принципи автоматизованої системи керування автомобільної сигналізації з оповіщенням
4. Контроль параметрів технологічного процесу.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)**:**
_____
_____
_____

6. Консультанти розділів магістерської роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання 14 листопада 2017 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання етапів роботи	Примітка
1	АНАЛІЗ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ НА ОБ'ЄКТІ УПРАВЛІННЯ	11.2017р. – 01.2018р.	
2	ТЕХНІЧНІ ЗАСОБИ ПРИЗНАЧЕНІ ДЛЯ УПРАВЛІННЯ, КОНТРОЛЮ, РЕГУЛЮВАННЯ ПАРАМЕТРІВ ТА ЗАХИСТУ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ АВТОМОБІЛЬНОЇ СИГНАЛІЗАЦІЇ	02.2018р. – 04.2018р.	
3	РЕАЛІЗАЦІЯ АЛГОРИТМУ ТА РОЗРАХУНОК СИСТЕМИ УПРАВЛІННЯ АВТОМОБІЛЬНОЮ СИГНАЛІЗАЦІЄЮ	05.2018р. –07.2018р.	
4.	РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ ДЛЯ КОНТРОЛЮ ТЕХНОЛОГІЧНИХ ПАРАМЕТРІВ АВТОМОБІЛЬНОЇ GSM СИГНАЛІЗАЦІЇ	08.2018р. – 11.2018р.	

Студент _____ Расевич В.Р.
(підпис)

Керівник роботи _____ к.т.н., Гуменний П.В.
(підпис)

РЕФЕРАТ

Робота виконана на 95 сторінках та містить 85 рисунків, 5 таблиць, 45 джерел за переліком посилань.

Мета роботи. Метою роботи є розробка автоматизованої система управління автомобільною охоронною GSM сигналізацією з оповіщенням.

Методи дослідження. Методи, методики та технології створення САУ процесами та комплексами різного призначення. Інструментальні засоби моделювання, планування, математичного, алгоритмічного і програмного забезпечення задач аналізу та синтезу складних розподілених у просторі гнучких комп'ютерно-інтегрованих систем.

Результати роботи та їх наукова новизна полягають у розробці автоматизованої системи управління автомобільною сигналізацією з використанням шифрованих біт-орієнтованих кодових сигналів у базисі Галуа з ознаками переривання на основі використання комбінації незвідних поліномів.

Рекомендації по використанню результатів роботи. Розроблені принципи керування автомобільною сигналізацією дозволяє використовувати їх в автоматизованих системах охорони різної складності.

Можливі напрямки розвитку полягають у розширенні функціональних можливостей систем автоматизованого управління охоронними автомобільними сигналізаціями, а також вдосконалення ПІД-регулятора контролерів.

Ключові слова: АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ, ДАТЧИК РУХУ, УЛЬТРАСОНІК, ЦЕНТРАЛЬНИЙ БЛОК КЕРУВАННЯ.

ABSTRACT

Work carried out on 95 pages and contains 84 figures, 5 tables, 45 sources for references.

The purpose of the work. The aim is to develop an automated GSM system of automotive security alarm alerts.

Research methods Methods, methods and technologies for creating SAU processes and complexes of different purposes. Instrumental means of modeling, planning, mathematical, algorithmic and software problems of analysis and synthesis of complex distributed computer-integrated systems in space..

Job performances. and their scientific novelty consist in the development of an automated control system for automobile signaling using encrypted bit-oriented code signals in the Galois basis with signs of interruption based on the use of a combination of irreducible polynomials.

Recommendations for the use of the results. Principles of management automobile car alarm allow their use in automated systems of protection of varying complexity.

Possible areas of development is to extend the functionality of automated enforcement car alarm management, and improving PID-regulator controllers.

Keywords: AUTOMATED CONTROL SYSTEM, MOTION SENSOR, ULTRASONIK, CENTRAL CONTROL UNIT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

АСУ –автоматизована система управління

МК – мікроконтролер

ЕБК –електронний блок керування

АЛБ- арифметико-логічний блок

ОЗП-оперативний запам’ятовуючий пристрій

ВСТУП

Актуальність теми. В наш час автомобілі перестали виконувати тільки транспортні функції, а стали складними дороговартісними системами, спроектованими за останніми тенденціями техніки, використовуючи складне електронне обладнання у всіх своїх функціональних блоках. Нещодавно мікропроцесорні системи запалювання, електронні системи управління гідравлічними гальмами, системи впорскування бензину, бортова самодіагностика, глобальна система позиціонування автомобіля вважалися останніми досягненнями у сфері автомобільного апарато- і приладобудування. Тепер їх відносять до класичних систем і встановлюють на кожен серійний автомобіль.

На сьогодні наново розроблювані моделі автомобілів додатково починають встановлювати цілком нетрадиційні бортові автоматичні системи, до яких належать[1]:

- інформаційна система водія з мікропроцесорним забезпеченням;
- супутникова навігаційно-пошукова система;
- системи підвищення безпеки і комфорту людей салоні;
- система круїз-контролю;
- система «електронна карта»;
- мультиплексний електропровід.

Інформаційної система водія з мікропроцесорним забезпеченням покращує ефективність роботи автомобіля та контроль за ним. Відповідно вартість автомобілів, що використовують інформаційні системи – зростає, а звідси є небезпека викрадення такого автомобіля або взлом його електронних модулів, тому необхідно використовувати нові електронні системи захисту автомобіля від викрадення та пошкодження його програмного забезпечення через хакерські атаки.

Актуальність впровадження охоронних систем для автомобіля полягає в забезпеченні захисту транспортного засобу, життя та здоров'я водія та

пасажирів, а також вантажів, що транспортуються у ньому, включаючи і джерела інформації.

Оскільки технології охоронних систем постійно розвиваються і змінюються, надзвичайно актуальною є розробка дешевих і надійних систем, які зможуть забезпечити безпечність автомобіля, а також зможуть здійснювати постійний моніторинг положення автомобіля через глобальні системи позиціонування і присилати оповіщення власнику при можливому викрадення транспорту та блокувати його роботу повністю або окремих вузлів, щоб запобігти викраденню.

Мета і задачі дослідження. Мета роботи полягає у розробці автоматизованої системи охоронної сигналізації автомобіля з оповіщенням, що зможе забезпечити захист від викрадення та унеможливить здійснення стороннього втручання у роботу електронних вузлів за допомогою хакерських атак.

Об’єкт дослідження – процес автоматизованого керування охоронною сигналізацією автомобіля з оповіщенням.

Предмет дослідження – система автоматизованого регулювання інерційних датчиків, що здійснює захист автомобіля, блокування роботи двигуна, захист периметрів та здійснення двостороннього зв’язку через системи оповіщення.

Методи дослідження. У роботі використовувались теоретичні основи автоматичного управління та автоматизації, методи ідентифікації, метод оптимального параметричного синтезу, методи дослідження стійкості і якості, а також методи імітаційного комп’ютерного моделювання. Для створення комп'ютерних моделей застосовано теорію імітаційного моделювання та використано програмне середовище Matlab.

Наукова новизна одержаних результатів полягає в тому, що запропоновано у системі автоматизованого керування автомобільною сигналізацією використовувати шифровані біт-орієнтовані кодові сигнали у базисі Галуа з ознаками переривання на основі використання комбінації

незвідних поліномів що у порівнянні з двійковими кодами дозволить покращити систему захисту автомобіля.

Практичне значення одержаних результатів. Розроблені структурні рішення, алгоритми керування та їх реалізація на контролерній техніці використані при реалізації автоматизованої системи охоронної сигналізації автомобіля.

Публікації. Гуменний П.В. Автоматизована система керування на основі вертикально-інформаційної технології у кодовому базисі Галуа /П.В. Гуменний, Б.Ю. Гуменюк , В.Р. Расевич , І.М Хомишин//Збірник матеріалів проблемно-наукової міжгалузевої конференції “Юриспруденція та проблеми інформаційного суспільства (ЮПІС-2018)” – Тернопіль – 2018 – с.79-84.

1. АНАЛІЗ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ НА ОБ'ЄКТІ УПРАВЛІННЯ

1.1. Аналіз систем автоматизованого управління автомобілем

Крім дисплея та елементів керування в сучасних автомобілях застосовується набір засобів забезпечення інформацією, зв'язком і комфортом руху, який постійно розширюється. Радіозв'язок, телефон, система навігації (рисунок 1.1) поступово стають стандартним оснащенням автомобілів. Кожен з цих засобів потребує наявності дисплея, спеціальних схем керування та різних процедур для їх роботи.

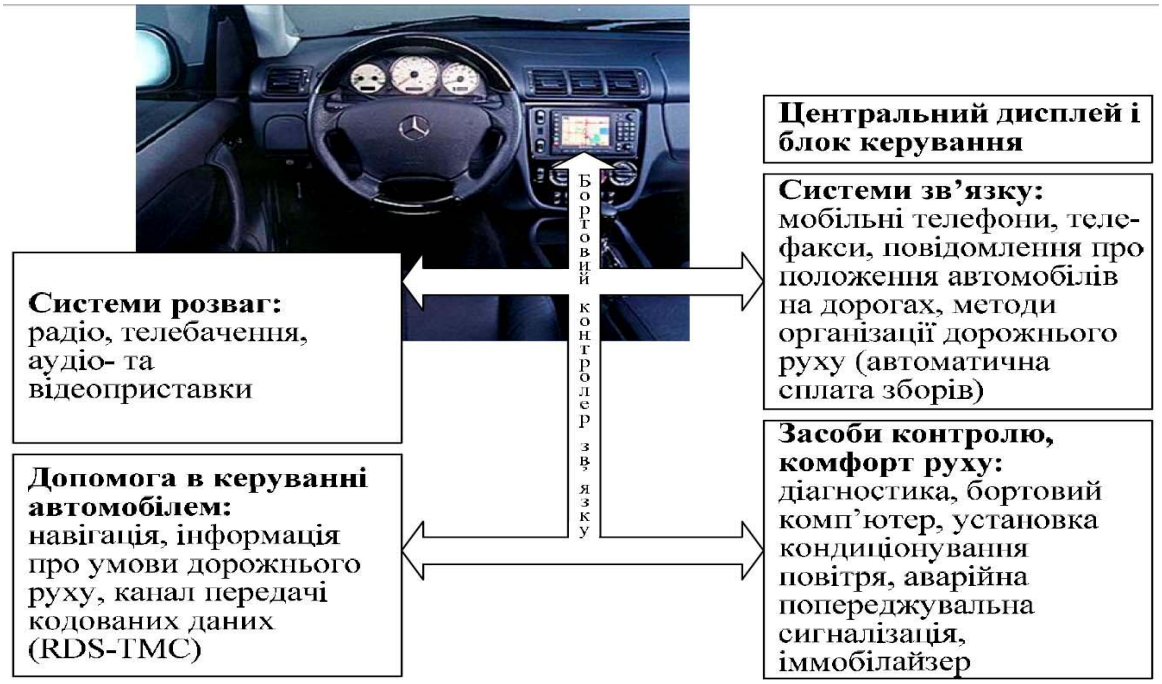


Рисунок 1.1- Центральний блок управління автоматизованою системою автомобіля

Для повного задоволення вимог щодо забезпечення комфорту і безпеки руху, інформаційна система автомобіля повинна мати стандартизований «інтерфейс користувача» для вибору водієм різних засобів забезпечення інформацією, зв'язком і комфортом руху. Застосування робочих елементів повинно бути обмежене рамками одного дисплея та одного робочого пристрою. Істотне зменшення числа елементів введення/виведення інформації полегшує впровадження ергономічних схем керування. Через

підвищення складності, інформаційні системи потребують розробки легко читаної та зручної контрольно-вимірювальної апаратури автомобіля, головною умовою застосування якої є забезпечення безпеки дорожнього руху. Дисплей і робочий блок підтримують взаємний зв'язок з усіма під'єднаними компонентами через шинну систему, наприклад, через бортовий контролер зв'язку (controller area network (CAN)), для керування і відображення інформації на дисплеї [2].

Основні функції більшості комбінацій приладів є однаковими (рисунок 1.2), хоча функціональні блоки, які включають мікроконтролери, інтегральні схеми запам'ятовуючих пристроїв з програмами (applicationspecific integrated circuit (ASIC)) [3] і стандартні зовнішні пристрої інколи значно відрізняються (за асортиментом, характеристиками і типом дисплеїв). Електронні комбінації приладів показують вимірювані параметри з високою точністю завдяки технології крокових двигунів, а також застосовуваних «інтелектуальних» функцій, таких як попередження про зміну тиску мастила в залежності від частоти обертання колінчатого вала двигуна, індикація відмов або необхідності технічного обслуговування і ремонту на матричному дисплеї.

Рисунок 1.2 – Блок-схема функціонування комбінації приладів з використанням
бортового контролера зв'язку CAN

Навіть оперативні діагностичні функції є стандартними і займають важливу частину запам'ятовуючого пристрою програми. Застосовувані в сучасних комбінаціях приладів системи шин (каналів передачі інформації)

використовуються як інтерфейси між різними системами автомобіля (наприклад, контролер зв’язку з двигуном, бортовим контролером зв’язку і шиною діагностування).

Завданням мікропроцесорних вбудованих засобів [3] є контроль за технічним станом агрегатів, вузлів, систем та автомобіля в цілому. В результаті формуються рекомендації із продовження роботи автомобіля на лінії або поставлення його на технічне обслуговування (ТО) і поточний ремонт (ПР), чи виконання дрібного ремонту самим водієм у межах щоденного обслуговування (ЩО).

Вбудовані засоби підрозділяються на:

– системи датчиків і контрольних точок, що забезпечують виведення сигналів на зовнішні засоби діагностування;

– бортові системи контролю параметрів функціонування та технічного стану з виведенням результатів тільки на дисплеї в кабіні водія;

– вбудовані системи діагностування – автономні або функціонуючі комплексно зі стаціонарними інформаційно-керуючими центрами. Ці системи призначені для непрямого узагальненого контролювання роботоздатності вузлів і агрегатів з видачею результатів на дисплей водієві та у бортовий накопичувач для подальшого прогнозування і обліку ресурсу та напрацювання вузлів, коректування режимів ТО стаціонарними комп’ютерами .

Найбільше поширення одержали вбудовані системи з мікропроцесорною обробкою, нагромадженням і видачею інформації водієві, у бортовий накопичувач і на штекерний вивід, що несуть функції всіх трьох зазначених різновидів. Такі системи призначені для використання водієм або механіком АТП і видачі даних в комп’ютер стаціонарного комплексу автоматичних систем контролю (АСК) роботою і технічним станом парку.

Найбільш перспективною можливістю зняти зазначені обмеження, забезпечивши практично безперервним контролем найменш надійні вузли, служить впровадження вбудованих засобів діагностування. Провідні

автомобілебудівні фірми застосовують на автомобілях розгалужені мікропроцесорні бортові системи контролю (БСК), які забезпечують контроль стану зчеплення, амортизаторів, акумуляторної батареї, системи запалювання, компресії в циліндрах та ін. (рисунок 1.3).

Рисунок 1.3 – Можливості й сфера контролю технічного стану вмонтованими засобами

Різноманіття функціональних можливостей, апаратної побудови та форм видачі результатів відображає класифікація вбудованих засобів діагностування за функціональними і структурними ознаками (рисунок 1.4).

Рисунок 1.4 – Класифікація вбудованих засобів діагностування

Вбудовані системи діагностики (ВСД) [4] автоматизують процедуру узагальненої оцінки стану автомобіля, звичайно виконувану водієм і механіком суб'єктивно навіть при оснащенні бортовими системами контролю. Конструювання ВСД ведеться за двома основними напрямками:

створення автономних цілком орієнтованих на водіїв систем для узагальненої оцінки стану автомобіля і систем у комплексі зі стаціонарними засобами ІКЦ, адресованих насамперед механікам, майстрам і керівникам АТП.

На сучасному етапі найбільш характерним є об'єднання різних автомобільних систем контролю і діагностування на структурному та алгоритмічному рівнях у єдину інформаційну систему автомобіля із загальною мережею датчиків і мікропроцесорним блоком з накопичувачем у комплексі зі стаціонарними ІКЦ АТП. Цим забезпечується не тільки раціональна побудова бортового комплексу, але й новий, якісно більш високий рівень оптимізації оперативного керування в технічній і комерційній експлуатації.

Сучасні транспортні засоби оснащуються великим числом електронних блоків керування (ЕБК), які виконують обмін великої кількості даних. Традиційний метод розв’язання цієї задачі шляхом використання ліній передачі даних, закріплених за кожним каналом, на даний час досягає меж своїх можливостей і стає стримуючим фактором розвитку ЕБК. Тому вирішення проблеми слід шукати у використанні спеціалізованих, сумісних з автомобільною проводкою, послідовних систем шин, серед яких бортовий контролер зв’язку (CAN) уже прийнято як стандарт.

Існує чотири основних види застосування CAN [5]:

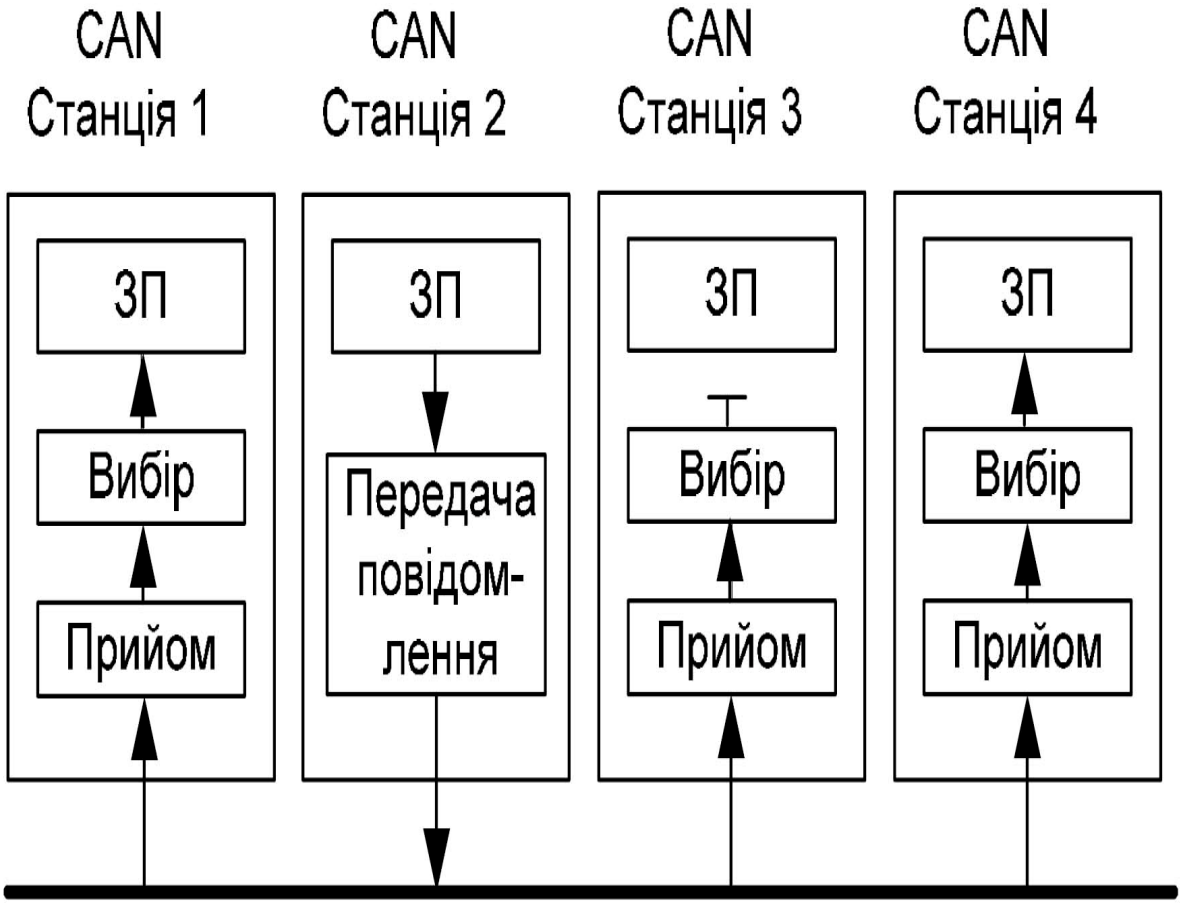
– зв’язок між ЕБК;

– рухомі засоби зв’язку;

– діагностування;

– мультиплексна проводка для елементів електрообладнання.

Зв'язок між окремими ЕБК стає необхідним, коли повинні з’єднуватись такі електронні системи, як Motronic, електронне перемикання коробки передач, електронне керування потужністю двигуна, керування силою тяги (ASR). Звичайно швидкість передачі даних знаходиться в діапазоні від 125 кбіт/с до 1 Мбіт/с і повинна бути достатньо високою для забезпечення реагування системи у реальному масштабі часу. Послідовне передавання даних (рисунок 1.5) забезпечує більш високу швидкість їх передавання, ніж в стандартних інтерфейсах, без створення додаткових перешкод для центрального процесора. Число штирьових контактів для ЕБК також зменшується



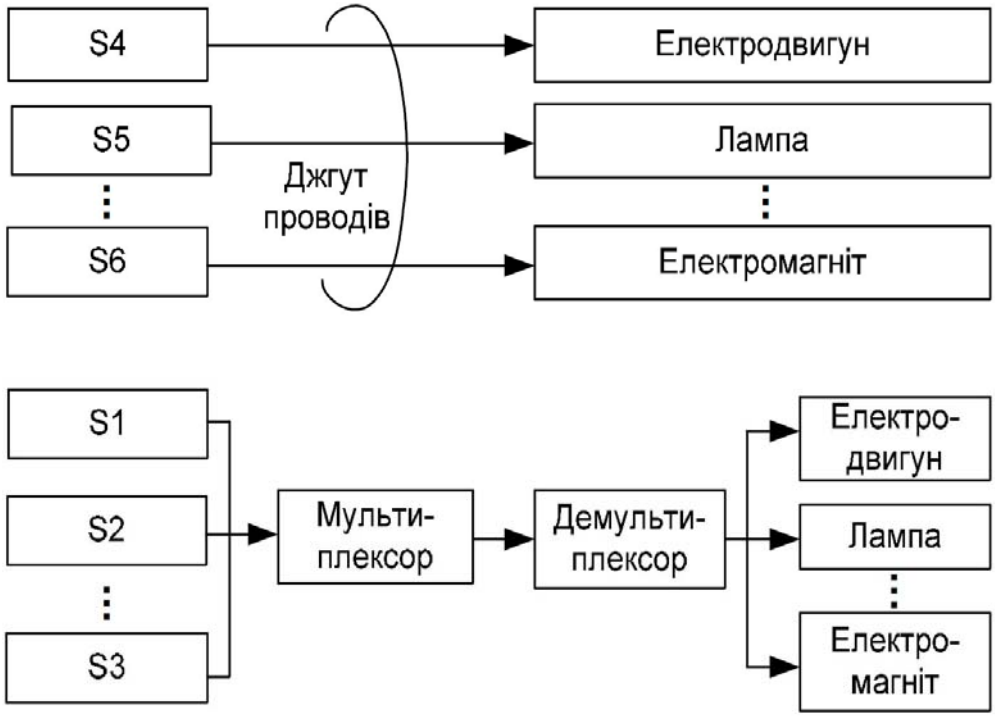
ЗП- запам’ятовуючий пристрій

Рисунок 1.5 – Послідовна передача даних з використанням контролера CAN

Мультиплексна система зв'язку в автомобілі [6] використовується для передачі декількох сигналів по одному сигнальному проводу, з’єднуючи

електронні компоненти з інтерфейсом водія. Ця система не тільки скорочує число джгутів і знижує масу з’єднувальних проводів, але й дозволяє істотно спростити конструкцію монтажу каналів у кузові та вузлів з'єднання дверей з кузовом. Сигнали, які керують виконавчими пристроями – електродвигунами, соленоїдами, електромагнітними клапанами, лампами, обробляються мультиплексором (пристроєм, що поєднує кілька сигналів), передаються по одному сигнальному проводу і за допомогою демультиплексора надходять до виконавчих пристроїв. Колись ці сигнали передавалися по численних проводах.

Приклад мультиплексної системи зв'язку [7] наведений на рисунку 1.6 Вимикачі систем керування в ній розташовані на дверях, а зв'язок з ЕБК забезпечується за допомогою світлодіодів. ЕБК системи виконують такі функції керування: блокування і розблокування дверей, поворот дзеркал, регулювання положення скла у вікнах, регулювання сидінь, підігрів сидінь, підсвічування попільниці та вимикачів, освітлення під передньою панеллю та освітлення гнізда ключа запалювання.



S1-S6- вимикачі

Рисунок 1.6 – Традиційна та мультиплексна системи зв'язку

Передача даних між ЕБК здійснюється стартостопним способом. При цьому способі на початку і в кінці даних додаються сигнали (так звані стартовий біт і біт зупинки), які синхронізують роботу приймальних і передавальних пристроїв. Швидкість передачі даних при такому способі невисока. Проте стартостопний спосіб одержав найбільш широке поширення, оскільки він забезпечує досить надійну синхронізацію даних. Швидкість передачі даних становить від 10 до 125 кбіт/с (низько швидкісні CAN). Формат даних поданий на рисунок 8.10. Тип сигналу вказується в зоні керуючого коду, а зміст обробки і стан вимикачів – у зоні даних. ЕБК 2,розташований в передніх правих дверях, є провідним елементом мультиплексного зв'язку. Він генерує 32-бітові послідовності керуючих імпульсів (первинні сигнали), які через ЕБК кузова 1 передаються на ЕБК в інших дверях. ЕБК записують у зоні даних цих сигналів стан вимикачів і потім передають сигнали в ЕБК кузова, що обробляє їх і передає вихідні сигнали на виконавчі пристрої кузова.

1.2 Аналіз видів автоматизованих охоронних систем автомобіля

З кожним роком автомобільна промисловість створює нові електронні пристрої для своїх автомобілів плавно рухаючись до створення автоматизованих робото технічних систем управління транспортними засобами. Над розробкою автоматичних систем курування автомобіля працює велика кількість автовиробників спільно з провідними виробниками мікропроцесорної та мікроелектронної техніки. Згідно наукових розробок корпорації Tesla [8] спроектувала автоматичну систему управління електромобілем Tesla Model S, що здійснює авто пілотне керування при швидкості 8 - 16 км / год, за допомогою панелі управління (рисунок 1.7) оскільки в разі потреби транспортний засіб може бути зупинено в чітко визначеному ультразвуковими датчиками місці.

Рисунок 1.7- Панель управління електромобілем Tesla Model S

Системи автономного водіння також можуть впоратися з автомобілем на автомобільних дорогах на швидкості 80 км / год, тоді як пересуватися на автострадах без участі водія ненабагато складніше. Проте, в діапазоні 16 - 80 км / год все набагато складніше. Для пересування в міських умовах дуже важливе значення має швидке прискорення при розгоні з місця після неминучих зупинок біля світлофорів, перед рухомими пішоходами та іншими об'єктами.

Функції автопілота для Tesla Model S включають автоматичне керування, зміна смуги руху, активований сигнал повороту і авто-паркування в паралельних просторах. У моделі електромобіля Tesla використання автопілота відбувається з підтримкою апаратних засобів, яка включає в себе відеокамери камери, радари і 360 датчиків ступеня ехолота Використання смарт-програмного забезпечення у моделі S дозволяє розпізнавати знаки швидкості, розпізнавати тварин і об'єкти в передній частині автомобіля, а також розпізнавати смуги і провулки,система через камери може бачити набагато краще, ніж людина може через туман, дощ і пилові бурі.

З впровадженням у транспортні засоби дороговартісних електронних пристроїв збільшує вартість автомобіля до 20-35 %. Звідси виникає небезпека у захисті автомобіля від викрадення та його взлому чи виведення зі строю

шляхом хакерських атак окремих вузлів, що може спричинити загибель водія чи викрадення автомобіля. Згідно статистичних даних [9] в Україні в середньому відбувається одне викрадення автомобіля за годину. Також у столиці України протягом 2013-2015 років кількість викрадень автомобілів зросла в середньому у 4-ри рази (рисунок 1.8).

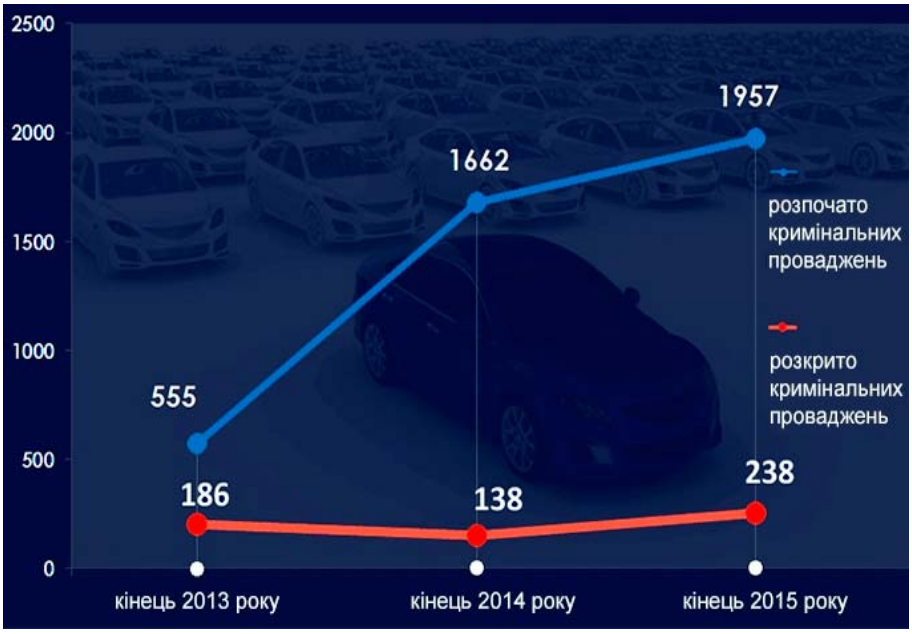


Рисунок 1.8- Динаміка росту викрадень автомобілів у м. Києві

Звідси виникає актуальність у розробці інтелектуальних автомобільних сигналізацій, які б унеможливити викрадення транспорту, а також могли б через систему глобального позиціонування моніторити знаходження автомобіля та здійснювати віддалене управління окремими вузлами.

Промисловість випускає багато різних протиугінних систем, зазвичай, ціна корелюється відповідно до запропонованого рівня захисту. Протиугінні системи мають бути ефективними, надійними, мати тривалий термін служби, стійкими до зовнішніх впливів, наприклад, до радіоперешкоди.

Протиугінні системи реалізують захист автомобіля умовно за трьома рівнями [10]:

- Захист по периметру. Система периметричного захисту використовує вимикачі контролю за які відкриваються панелями автомобіля (двері, капот, багажник). При спробі несанкціонованого відкриття панелі включаються

звуковий та світловий сигнали. Іноді система доповнюється датчиками, здатними виявляти рух тіла.

- Захист за об’ємом. Система з допомогою інфрачервоних, ультразвукових чи мікрохвильових датчиків виявляє несанкціоноване рух в салоні автомобіля. Ультразвукові датчики використовують ефект Допплера, коли будь-який рух в салоні змінює частоту сигналу ультразвукового випромінювача (40 кГц), який приймається відповідним приймачем. Мікрохвильова радіосистема працює на тому самому принципі, але радіосигнал випромінюється на частоті 10 ГГц. Мікрохвильові датчики рідше помилково реагують на рух повітря, тому частіше встановлюються в кабріолетах. Інфрачервоні датчики влаштований як комплект «приймач — випромінювач» і монтуються до стелі салону. Вони утворюють невидиму інфрачервону завісу до підлоги салону. Приймач постійно контролює відбитий сигнал і його зміни (хтось з’явився у салоні) включається сигнал тривоги. На рисунку 1.9. приведена стандартна схема автомобільної сигналізації, що забезпечує захист по периметру та захист по об’єму [11] .

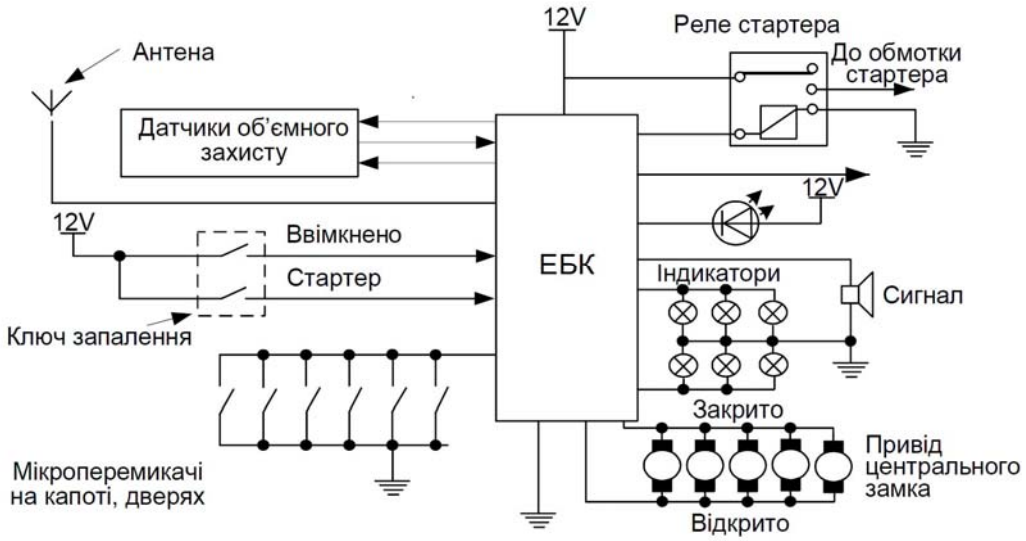


Рисунок.1.9 – Блок-схема базової протиугінної системи

- Іммобілізація двигуна [12] здійснюється спеціальним датчиком, який забороняє запуск двигуна, якщо отримано сигнал тривоги. Це може бути здійснене двома шляхами:

а) апаратною іммобілізацією, коли деякі електричні ланцюга системи пуску двигуна розриваються спеціальними реле чи напівпровідниковими перемикачами. Ефективність апаратних систем іммобілізації залежить від прихованості реле, що розривають і відсутність маркувань на дротах у джгутах. Прихованість потрібна для того, щоб не можна було шпунтувати розриви у ланцюзі, які створюють ці пристрої;

б) програмною іммобілізацією, коли за командою протиугінної системи двигуна забороняє його запуск, наприклад, робить недоступними калібровані діаграми подачі палива й запалювання. Після цього двигун хоч і буде провертатися стартером, але не запуститься. Такі системи дуже ефективні, потрібно лише не допустити можливість запуску шляхом заміни датчика двигуна в інший працездатний блок.

На даний час відсутня єдина класифікація для усіх типів охоронних систем автомобіля. Спеціалісти класифікують їх за співвідношенням охоронних і сервісних функцій. Зокрема розрізняють три основних класи [13]:

1. Системи класу «Стандарт» забезпечують такі охоронні функції:

- дистанційне керування радіо брелоком (один канал керування, декілька десятків тисяч кодів);

- охорона дверей, капота, багажника за допомогою кнопкових вимикачів;

- захист від ударів;

- режим «Паніка»;

- блокування двигуна по одному ланцюгу (ланцюг запалювання або живлення стартера);

- світлова і звукова сигналізація (в режимі тривоги);

- антисканерний захист.

Стандартними сервісними функціями є такі:

- світлове і звукове підтвердження поставлення і зняття режиму охорони;

- світлодіодна індикація режимів роботи;

- світлова і (або) звукова індикація факту спрацьовування сигналізації;

- службовий режим з відключеними охоронними функціями.

2. Системи класу «Екстра» забезпечують такі охоронні функції:

- дистанційне керування з кількістю кодових комбінацій від сотень до тисяч і вище;

- захист об'єму салону;

- блокування двигуна, яке зберігається навіть при демонтажі системи;

- автоматичне повернення в режим охорони, яке забезпечує захист від випадкового вимкнення системи (повернення режиму охорони через 15-30 с);

- пасивне ввімкнення охорони (автоматичне ввімкнення режиму охорони через 15-30 с після закриття останньої дверці);

- захист від угону, який дозволяє дистанційно зупинити автомобіль і заглушити двигун (функція Anti-Hi-Jack);

- роздільний захист дверей, капота і багажника автомобіля;

- захист від ударів;

- розгалужена діагностика системи, яка дозволяє визначити несправний датчик і завчасно прийняти відповідні заходи.

3. Системи класу «Супер» забезпечують такі охоронні функції:

- дистанційне керування з динамічним кодом, завдяки якому усі спроби запам'ятати його або розшифрувати за допомогою сканера чи іншого електронного пристрою стають безрезультатними;

- резервне джерело живлення блока керування системою;

- використання не менше трьох ланцюгів блокування двигуна: блокування запалювання, стартера і системи подачі палива;

- досконала автоматична система захисту від нападу – активного, пасивного чи комбінованого типу, яка потребує від водія мінімальних керованих впливів.

На даний момент в охоронній системі більшості відомих імпортних автомобілів (BMW, Renault, Audi, Volkswagen, Saab, Volvo та інші, кількість

яких постійно зростає) встановлюють цифрові автомобільні сигналізації класу «Супер» та «Екстра» у яких використовується CAN шина[14]. Вона являє собою виту пару спеціальних проводів (специфічна комп'ютерна мережа), яка одночасно поєднує всі деталі автомобіля і здатна передавати дані на високій швидкості по швидкому каналу (500 кбіт/с - 1 Мбіт/с). Завдяки цьому за допомогою CAN шини [14] можна швидко зв'язуватися з брелоком управління автосигналізацією навіть на відстані. Особливістю автосигналізації на основі цифрової шини по відношенню до аналогових сигналізацій класу «Стандарт» є те, що не потрібне підключення додаткових проводів і суттєвого розбирання салону (рисунок1.10), так як число підключень до ланцюгів автомобіля складає всього до п'яти точок (проти 20-30 в інших видах автосигналізацій (рисунок 1.11), з'являється також можливість добре заховати елементи охоронної системи.

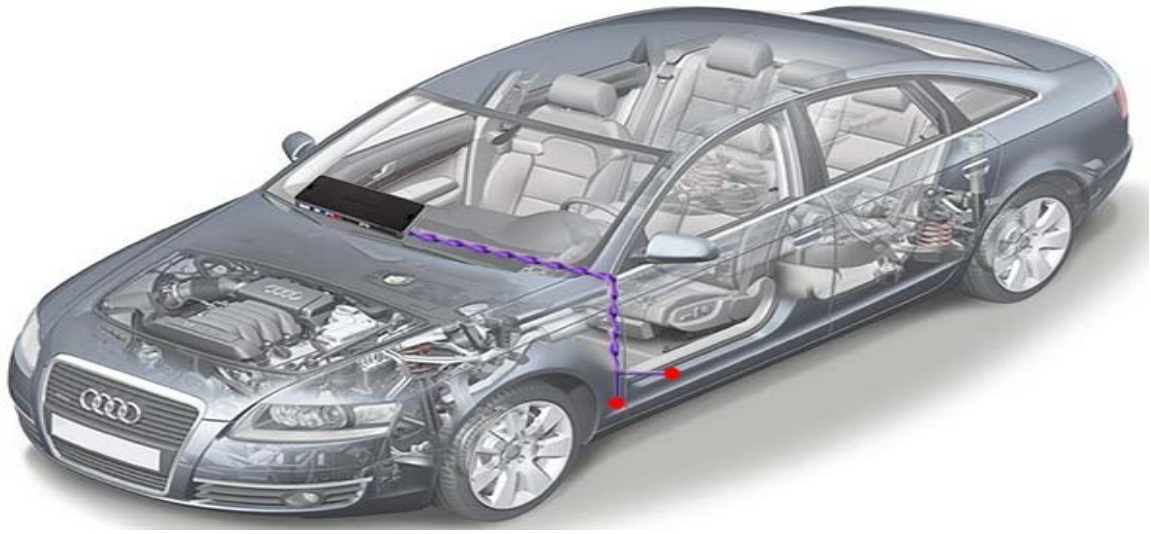


Рисунок 1.10- Точки підключення авто сигналізації по цифровій шині CAN

Завдяки своїм конструктивним особливостям шина істотно знижує рівень впливу електромагнітних полів, поява яких прямо пропорційно пов'язано з роботою автомобіля (двигун і інші системи). Шина використовується не тільки в охоронних системах, а й для підключення інших зовнішніх пристроїв. При цьому кілька пристроїв можуть використовуватися одночасно і швидкість передачі даних не зменшується.

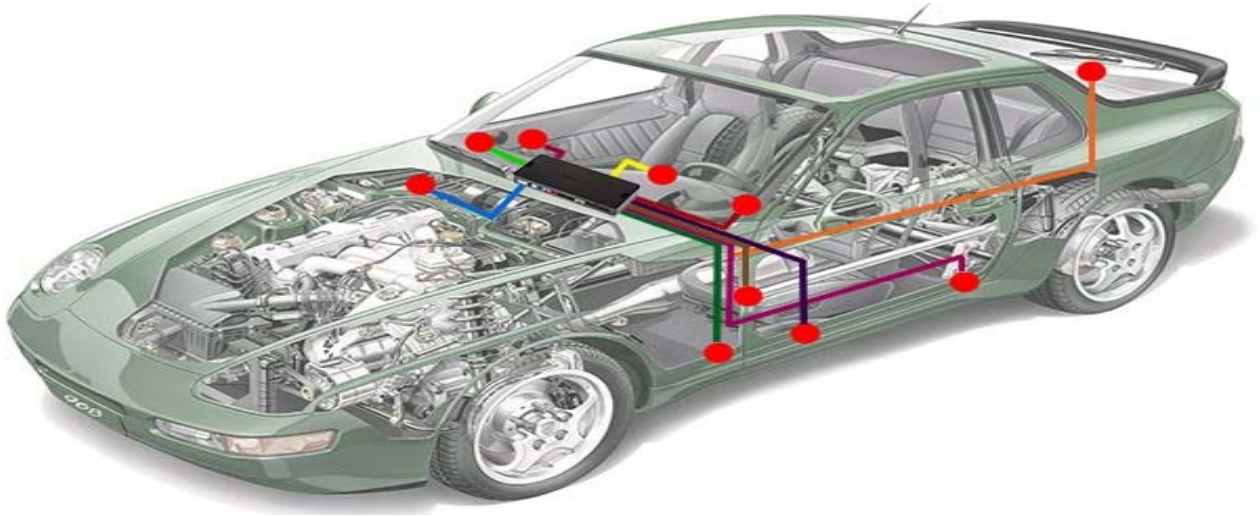


Рисунок 1.11- Точки підключення авто сигналізації по аналогових шинах

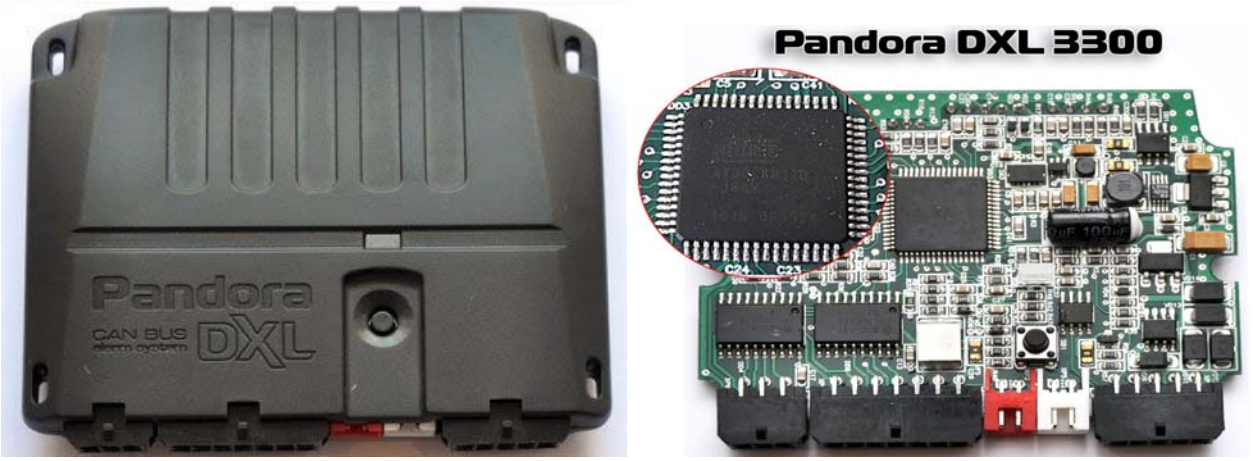
Адаптер цифрового типу CAN шини, гарантує стабільну роботу охоронної системи. Суть дії полягає у зчитуванні інформації з CAN шини і перетворенні її в цифрові аналогові сигнали, що необхідні для відправки на брелок авто сигналізації. З'являється також можливість керування пристроями автомобіля (відкриття / закриття дверей (вікон), отримання інформація від спідометра, що представлено на рисунок 1.12).

Рисунок 1.12- Приклад підключенну функціональних модулів автомобіля до CAN шини

Кожен CAN модуль має індивідуальну програму, яка призначена виключно під певний автомобіль. Особливістю CAN-шини є відсутність єдиного загальноприйнятого стандарту протоколу передачі даних, що

дозволяє конструкторам автомобіля гнучко підстроювати систему під конкретні завдання.

Розглянемо системи автоматизованої охоронної сигналізації на основі CAN шини. На рисунку 1.13 представлений центральний блок управління (а) та плата цього блоку (б) автомобільної сигналізації Pandora DXL 3300 [15].



а) б)

Рисунок 1.13- Центральний блок (а) та плата (б) автомобільної сигналізації Pandora DXL 3300

Система Pandora DXL 3300 [15] має багатоканальний радіотракт, що працює в діалоговому режимі і забезпечує високу стійкість перед перешкодами в сучасних індустріальних містах. Персональний ключ шифрування кожного брелка. що входять в комплект та мають діалоговий код. Вбудовані датчики удару, нахилу і руху, реалізовані на високочутливому трикоординатному інтегральному акселерометрі. Радіотракт , який використовуються в охоронній системі Pandora DXL 3300, дозволяє у дозволеному діапазоні навколо частоти 433,92 МГц «вирізати» 10 вузьких каналів і працювати на одному з них. Щоб домогтися від системи максимальної завадозахищеності, потрібно відокремитись від центральної частоти системи за містом.

Стійкою роботою каналу управління можна вважається дальність до 1700 метрів від автомобіля. На наступних ста метрах стійкість управління падає, після чого зв'язок відновлюється практично ідеально на віддаленні

2300 метрів від машини. Повідомлення господаря про те, що відбувається з автомобілем є стабільним на дистанціях до 2600 м. В системі застосовується восьмизарядний мікропроцесор AT90CAN128 виробництва компанії Atmel. Його максимальна тактова частота 16 МГц. Процесор має на борту 128 Кб вбудованої флеш-пам'яті і забезпечує апаратну підтримку обробки CAN-протоколів. Для реалізації авто запуску двигуна до сигналізацію додатково можна підключити зовнішній блок автозапуску, уякий входять п'ять реле для комутації силових ланцюгів.

Модель автомобільного охоронного комплексу Scher-Khan MAGICAR 9[16] (рисунок 1.14) позиціонується як елітна двостороння автомобільна охоронна система з автоматичним запуском двигуна.

Рисунок 1.14- Система автомобільного охоронного комплексу Scher-Khan MAGICAR 9

Система володіє функцією підключення до шини CAN з контролем стану акумуляторної батареї. У системі відбувається синхронізація брелоків запуску з автоматичною передачею даних на всі брелоки. Заявлена дальність зв'язку до 2000 м. При роботі каналу управління стабільний зв'язок відбувається на відстані до 1100 м. В умовах високих перешкод Scher-Khan MAGICAR 9 має можливість управління системою на відстані 210 і 220 м. При цьому система досить стабільно сповіщає користувача про події, що сталися з автомобілем, практично у всіх тестових точках, крім найвіддаленішої точки у 360 м. Scher-Khan MAGICAR 9 при підключення по CAN-шині автомобіля додає 15-20 мА до споживання. Якщо з відключеним

CAN-модулем без охорони система споживає 35 мА і 40 мА в режимі охорони, то при активізованою цифровій шині споживання зростає до 50 мА і 60 мА.

На рисунок 1.15. представлена система охоронної GSM сигналізації автомобіля StarLine M30 [17]. Система StarLine M30 немає зовнішньої антени, як немає і роз'єму для її підключення, тому основний блок потрібно розташовувати в зоні радіодоступності сигналів стільникового зв'язку.

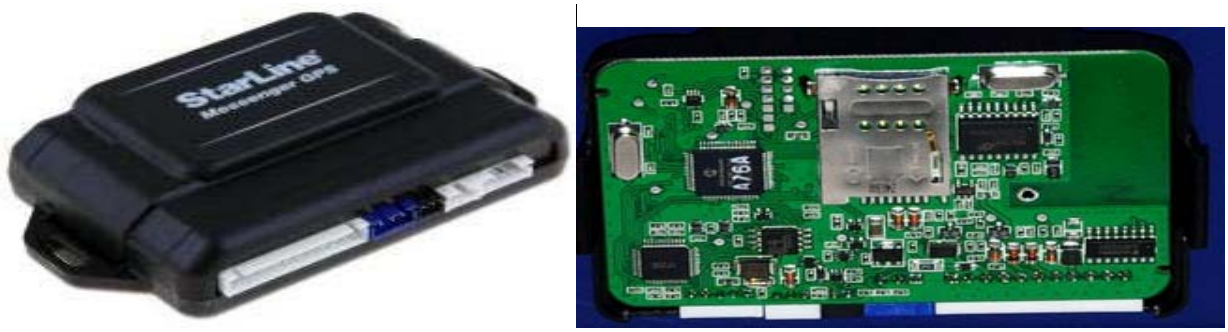


Рисунок 1.15- Система автомобільного охоронного комплексу StarLine M30

Проте система комплектується зовнішнім GPS-приймачем, і автономним NiMH-акумулятор на 750 мА/год, розташований в корпусі пристрою. На відміну від попередніх систем управління модулем йде по цифровій шині SL-Data. Крім цього є шлейф для аналогового підключення системи.

Головне управління режимами роботи систем сигналізації відбувається за допомогою тонових DTMF-команд, які набираються з телефонної клавіатури. Команди всі двозначні, без додаткового підтвердження. При дзвінку на систему лунає вітання, після чого StarLine M30 чекає набору команди, а також пропонує прослухати список команд. Якщо дзвінок здійснюється не з основного номера власника, то потрібно ввести пін-код. Пін-коди задаються при первинній інсталяції системи і, отже, будуть відомі установнику, тому їх краще перезаписати після отримання автомобіля.

Крім управління охороною з мобільного телефону можна включити або відключити датчик удару, активувати режим відвідування сервісного центру,

завести або заглушити двигун. Є можливість управління чотирма додатковими каналами. Також система за запитом видає інформацію про місцезнаходження автомобіля у вигляді SMS-повідомлення і про стан сигналізації, режим роботи та стан датчиків і входів. Є можливість прослухати салон машини. Великий блок команд настройки системи StarLine M30 передається за допомогою SMS-команд, в тому числі для зміни основних і додаткових телефонних номерів, паролів, трекерного режиму. Система дозволяє встановити періодично висилається звіт про місцезнаходження автомобіля, задати зону контролю авто, а також відправляти повідомлення про перевищення швидкості руху автомобіля.

Система дозволяє отримати координати розташування автомобіля у вигляді дійсних значень або у вигляді посилання на картографічний сервіс. Якщо підключений GPS-приймач, то дані беруться з нього, при його відсутності наводяться дані LBC-моніторингу по стільникових вишок операторів стільникового зв'язку.

На рисунку 1.16 представлена система автомобільної сигналізації X-Keeper Drive V3 [18] особливістю даної системи є відсутність в системі звичного всім брелка управління сигналізацією. Розробники вирішили відмовитися від радіоканалу для управління системою на користь режиму автоматичного впізнання власника з використанням високочастотної мітки і сповіщення за допомогою SMS-повідомлень.

Рисунок 1.16- Системна плата автомобільної сигналізації X-Keeper Drive V3

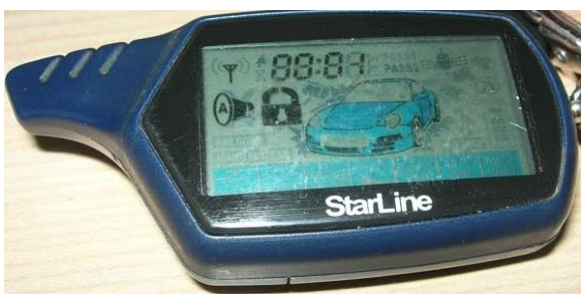
Управління сигналізацією проводиться з стільникового телефону з використанням Java-додатка, яке завантажується з сайту виробника. У комплект крім основного блоку входить GPS-приймач, зовнішня GSM-антена і блок ідентифікації мітки. Також додається резервний свинцево-кислотний

акумулятор типу AMG на 1,3 А/год, 6 В. Для роботи з CAN-шиною система укомплектовується додатковим модулем CAN-PRO. У системі X-Keeper Drive V3 використовується GSM-трансівер Telit Ce868 DUAL. За задумом розробників, в штатному режимі стільниковий телефон служить для сповіщення власника, оскільки при щоденній експлуатації система автоматично розпізнає мітку і знімається з охорони, не вимагаючи від власника ніяких додаткових дій. У зворотній послідовності відбувається постановка на охорону. Мітка працює на частоті 2,4 ГГц, сигнал має діалогове кодування. Управління з телефону власника має пріоритет над міткою. Якщо систему X-Keeper Drive V3 поставити на охорону із стільникового телефону, мітка автомобіль не розблокує. Все управління відбувається за допомогою Java-додатка, що формує команди і висилає їх в SMS-повідомленні, в якому крім команди міститься ідентифікаційний код власника. Якщо керуюча SMS приходить без такого коду, система розглядає це як спробу злому. Також система може сповіщати власника про спроби глушіння свого GSM-каналу.У системі відсутнє DTMF-управління, але можна запрограмувати X-Keeper Drive V3 так, щоб по дзвінку з телефону власника виконувалися або автозапуск двигуна, або зняття з охорони. Система також інтегрується в власний web-інтерфейс для відображення місця розташування автомобіля і його треку. Сервіс дозволяє контролювати автомобіль, відстежувати треки його переміщення і події, що відбуваються з автосигналізацією.

1.3. Аналіз електронних засобів для взлому автомобільних сигналізацій

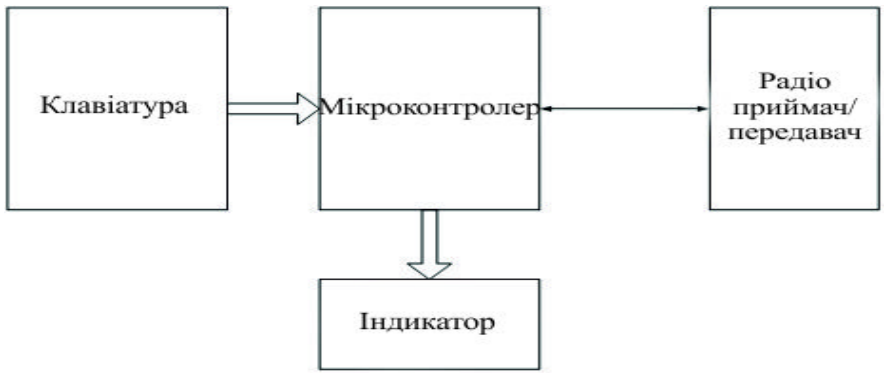
Сучасні охоронні сигналізації це складні електронні пристрої, які мають дистанційне керування, деякі функції іммобілайзера, а також виконують безліч сервісних функцій. Включена сигналізація контролює ряд точок в автомобілі, і, в разі вторгнення, включає звукові і світлові сигнали для залучення уваги та виконує ряд інших функції. Кількість контрольованих

точок залежить від комплекту поставки і кількості додаткових датчиків, що підключаються до сигналізації. З розвитком засобів зв'язку більш широко почали використовувати радіоканал. З його ж допомогою виконується дистанційне керування апаратурою автомобіля. В якості електронного ключа і пульта управління застосовують кодові брелоки. Кодовий брелок (рисунок 1.17) - мініатюрний передавач, що працює, як правило, в діапазоні дециметрових хвиль (200-500 МГц). Найбільш слабка ланка автосигналізації - радіосигнал, який передається від брелока до основного блоку.



А)

б)



в)

Рисунок 1.17. Радіо брелок автомобільної сигналізації (а) та його системна плата (б) та принцип роботи (в)

Набір нулів і одиниць буде представляти із себе набір викидів напруги (імпульсів), що з'являються на виході пристрою під час передачі якого-небудь числа в двійковому коді. Цей код передається у вигляді імпульсів. Такий спосіб передачі називається послідовним кодом, тому що імпульси передаються послідовно, один за одним. Цей спосіб застосовується практично у всіх передавальних пристроях автосигналізацій. Приймач

пересилає прийнятий сигнал (код) в перетворювач, який перетворює послідовний код в паралельний (рисунок 1.17). Потім з перетворювача код надходить в дешифратор, який визначає правильність коду, і, якщо він правильний - видає сигнал постановки / зняття з охорони на елементи управління, а якщо код неправильний - просто ігнорує його.

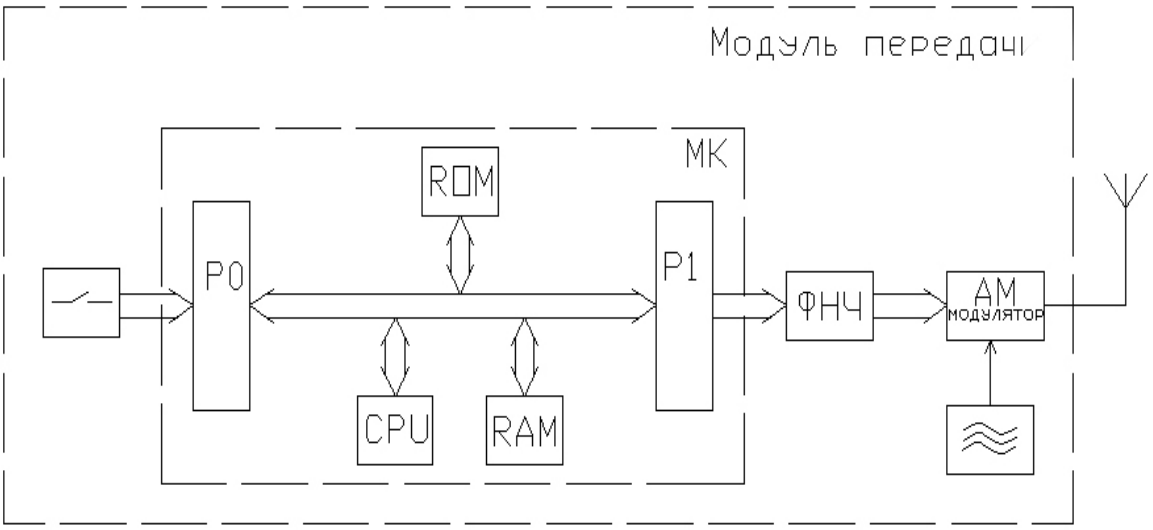


Рисунок 1.17- Модуль передачі коду з брелока автомобільної сигналізації

Найперші брелоки мали 5-й і 10-й значний постійний код, який виставлявся за допомогою перемикачів на брелоку і в центральному блоці автосигналізації. Як тільки стало зрозуміло, що примітивний код брелока не має майбутнього, з'явився антисканер. Так, наприклад, фірми пішли на збільшення розрядності кодів, що передаються брелоками. Код став мати таку кількість комбінацій, що стало неможливо займатися його перебором, так як на це пішли б століття. Тоді викрадачі виготовили прилад, здатний встановлювати частоту, на якій відбувається передача коду, пристрій записує сам код, а потім передає його, знімаючи автомобіль з охорони. Антісканер проти цього пристрою був безсилий. Новий прилад стали називати код-граббер (рисунок 1.18). Кодграббер - це пристрій для відключення сигналізації автомобіля, тобто засобів охорони автомобіля. При застосуванні даного пристрою повністю вимикається охоронна система автомобіля, відкривається центральний замок , а також вимикаються всі блокування, які перешкоджають запуску двигуна. В основі роботи цей прилад використовує

оригінальні алгоритми фірм, що виготовляють автосигналізацію. Тобто він працює як рідний брелок.

Розглянемо основні різновиди подібних комплексів [19]:

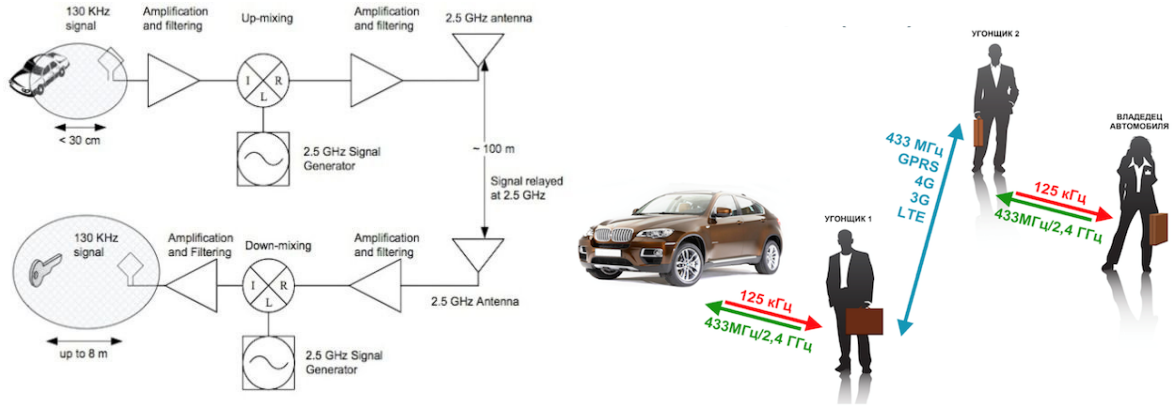
- Алгоритмічний (мануфактурний) кодграббер. Це прилад для відключення охорони автомобіля. При його застосуванні вимикається охоронна система авто, відкриваються двері і багажник, а також знімаються всі блокування на старт двигуна. В основі роботи - заводські алгоритми виробників автосигналізацій. Працює як рідний брелок. Він відкриває сигналізації без створення перешкод у радіоефірі і непотрібних блокувань рідного брелка. Кодграббер перехоплює всього один запит коду з рідного брелка, навіть при відсутності самого авто поруч. Після перехоплення пакету, Алгоритмічний кодграббер створює цифровий аналог брелка і зберігає його у внутрішній енергонезалежний EEPROM процесора. Мануфактурний код-граббер зазвичай зроблений у вигляді звичайного брелока від сигналізації.

Рисунок 1.18- Мануфактурний кодграббер

Багато виробників використовують єдиний ключ шифрування для кодування сигналу для всього модельного ряду автосигналізацій. Маючи в пам'яті цей ключ шифрування, код-граббер розпізнає сигналізацію в ефірі, зазначає код і в подальшому може управляти пристроєм несанкціоновано;

- Кодграббер з ретрансляцією виконує прийом сигналів на проміжному пункті, їх посилення і передача в колишньому або іншому напрямку.

Ретрансляція призначена для збільшення дальності зв'язку. Подібний пристрій застосовується для систем автосигналізацій і іммобілайзерів, обладнаних складними системами кодування, такими як діалоговий код. У цій ситуації відбувається передача сигналу до об'єкту на великій відстані через допоміжні електронні пристрої. Злому за допомогою ретранслятора схильні до системи, які мають пасивний принцип дії брелока (мітки). У таких системах реалізований алгоритм автоматичного зняття з охорони (відкриття центрального замка і вимикання блокувань) при наближенні до автомобіля з брелоком (міткою).



а) б)

Рисунок 1.19- Принцип взлому сигналізації кодграбером з ретранслятором

Код-граббер з ретрансляцією може бути використаний проти систем, в яких відсутній постійний або періодичний контроль наявності радіопозначки (штатної або додаткової) після зняття з охорони, коли сигнал треба "доставити" тільки на момент запуску двигуна;

- Код-граббер заміщувач застосовується для комплексів автосигналізацій і іммобілайзерів[18], обладнаних складними системами кодування. У момент передачі сигналу такий прилад випромінює перешкоду, не даючи охоронній системі зреагувати на посилку, і одночасно перехоплює код. Власник автомобіля натискає кнопку брелока вдруге. В ефірі знову виникає перешкода, і системі надсилається перша перехоплена команда. Автомобіль слухняно встає на охорону, а в пам'яті граббера залишається

друга, придатна для відключення сигналізації кодова посилка. За допомогою цього алгоритму викрадачі навчилися обманювати систему KeeLoq [20] - алгоритм динамічного захисту радіоканалу, розроблений південноафриканської фірмою Nanoteq. Цей алгоритм шифрування досі є своєрідною крипто-графічної іконою, оскільки математичних способів підбору його ключових комбінації не існує (на комп'ютерний перебір всіх 18446744073709551616 варіантів піде 29247 років). Нинішній власник прав на технологію KeeLoq - американська компанія Microchip. На рисунку 1.20 представлена схема взлому автомобіля кодграббером заміщувачем.

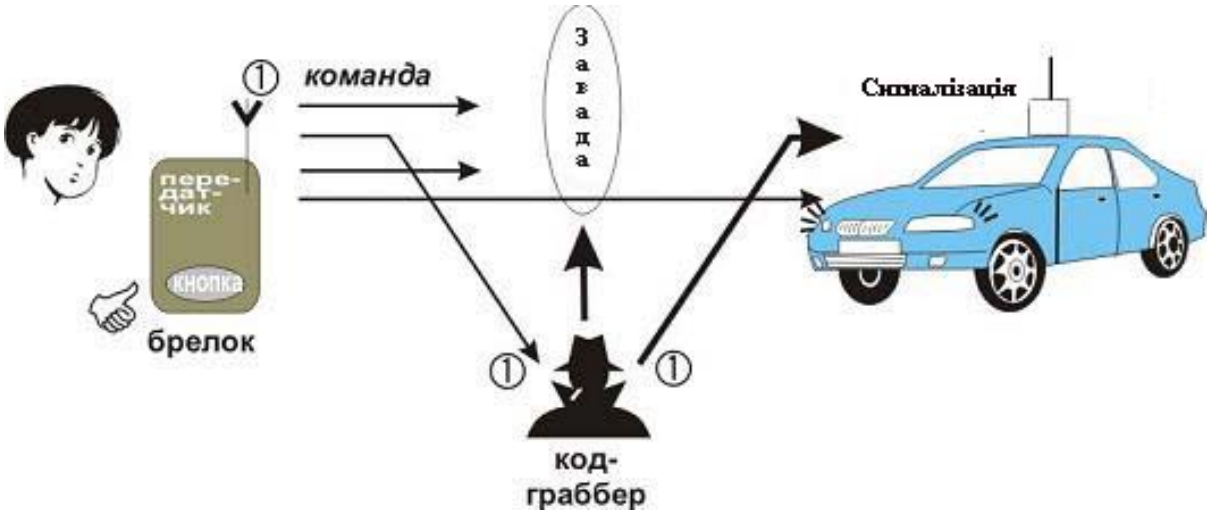


Рисунок 1.20- Схема взлому авто сигналізації кодграбером заміщувачем

Якщо є діалоговий код, то відбувається передача сигналу від об'єкта до об'єкта на великій відстані через допоміжні електронні пристрої, і в даному випадку код-граббер перехоплює сигнал. Принцип діалоговий коду полягає в наступному. Отримавши сигнал, система переконується, що він посланий з "свого" брелка, причому це відбувається не одноразово, а в діалозі. У відповідь на перший сигнал система посилає на брелок запит у вигляді випадкового числа, який обробляється брелоком за спеціальним алгоритмом і відсилається назад. Автосигналізація обробляє свою посилку за тим же алгоритмом, порівнюючи отриману відповідь зі своїми даними. Якщо вони збігаються, команда виконується, а на пульт відправляється підтвердження.

2. ТЕХНІЧНІ ЗАСОБИ ПРИЗНАЧЕНІ ДЛЯ УПРАВЛІННЯ, КОНТРОЛЮ, РЕГУЛЮВАННЯ ПАРАМЕТРІВ ТА ЗАХИСТУ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ АВТОМОБІЛЬНОЇ СИГНАЛІЗАЦІЇ

2.1 Дослідження пристроїв криптографічного захисту автомобільної сигналізації та характеристика їх роботи

Одним з додаткових пристроїв захисту автомобіля від несанкціонованого викрадення є імобілайзери, які можуть як складовими окремо взятої системи захисту так і бути автономними пристроями. Іммобілайзер (immobilizer) - захисний пристрій проти викрадення автомобіля, який перешкодить роботі основних вузлів автомобіля при спробі привести його в рух без відома власника. Пристрій включає в себе цілий електронний комплекс, завдання якого виключити можливість запуску двигуна без участі власника ключа, тобто - господаря авто. Іммобілайзер перешкоджає нормальному функціонуванню однієї або відразу декількох "життєво важливих" систем автомобіля, без яких він не зрушить з місця, як правило це - система подачі палива і система запалювання автомобіля. На рисунку 2.1 представлена плата контактного імобілайзера та ключ його відключення [18].

Рисунок 2.1- Системна плата контактного імобілайзера та ключ його деактивації

На рисунку 2.2 продемонстрована схема підключення контактного імобілайзера до то стартера двигуна автомобіля. На схемі провід від іммобілайзера (2) підключений до системи запалювання автомобіля за допомогою роз'єму (1). В даному випадку блокується можливість появи іскри запалювання.

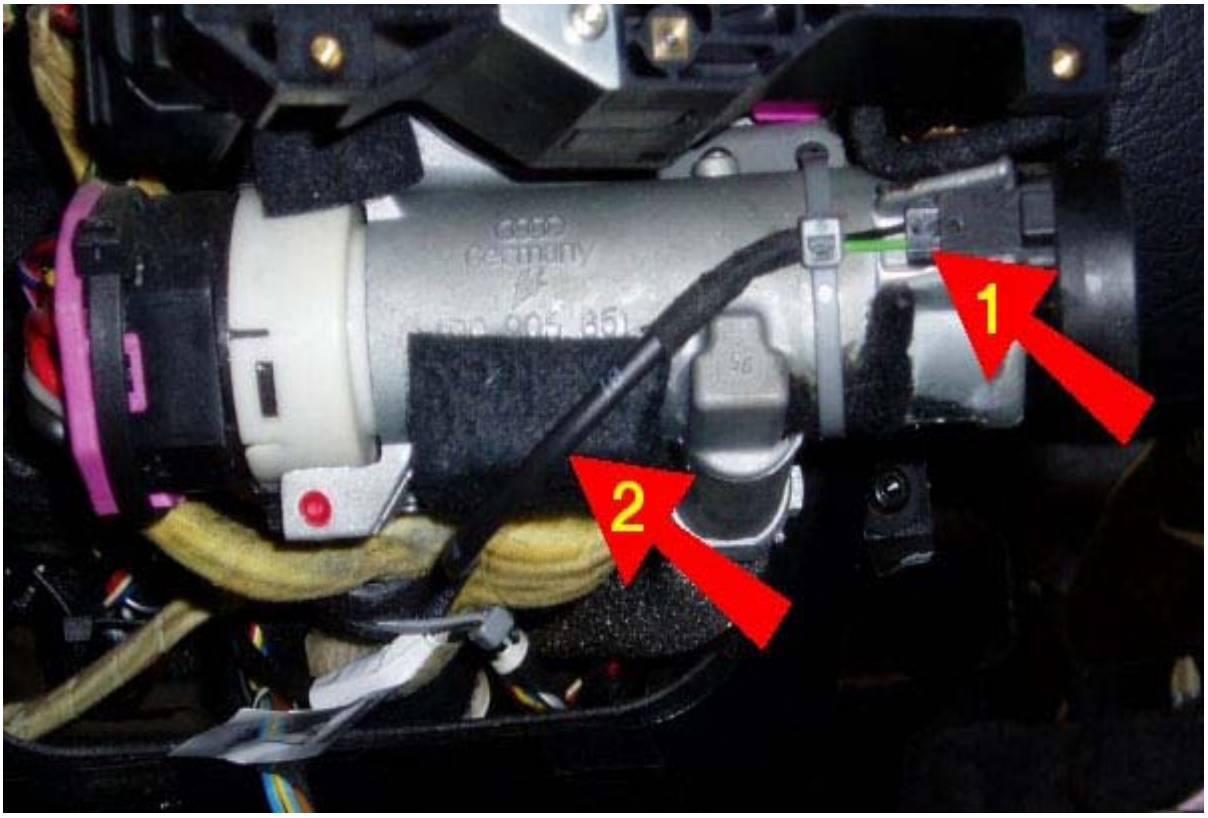


Рисунок 2.2- Схема блокування контактним імобилайзером іскри запалювання автомобіля

Принцип роботи імобілайзера відбувається шляхом розриву електричного кола або навпаки, шляхом подачі живлення на спеціальні механізми, які вже виробляють блокування двигуна. Іммобилайзером неможливо деактивувати шляхом "обриву проводів", чи спробою розібрати сам пристрій, якщо система зафіксує спробу злому або розтину елементів імобілайзера, вона автоматично блокується і блокує всі доступні системи автомобіля. Імобілайзери, як правило, оснащені системою автоматичної активації, тобто якщо протягом певного часу (встановленого виробником) автомобіль ніяк не використовувалася, то система захисту автоматично ставить авто під охорону.

На рисунку 2.3 представлено пристрій у виді ключа з транспондером який знімає імобілайзер з блокування запуска двигуна та системи вприскування палива у бензонасос.

Рисунок 2.3- Плата ключа деактивації імобілайзера з чіпом зчитування коду запуску

На рисунку 2.4 представлена схема роботи ключа з транспондером при запуску автомобіля. Іммобілайзер, використовує ключ запалювання, складається з чотирьох основних компонентів. Ядром системи є транспондер, пристрій без джерела живлення, яке може бути різного виконання і з різною функціональністю. Для приведення в робочий стан транспондер повинен отримувати енергію від зовнішнього джерела. Для цього потрібний прийомо-передатчик. Антенна-котушки випромінює магнітне поле щодо високої частоти, і енергія поля включає транспондер. Він передає пакет даних у формі модульованого радіосигналу. Цей сигнал демодулюється приймачем і потім направляється в контролер для подальшої обробки.

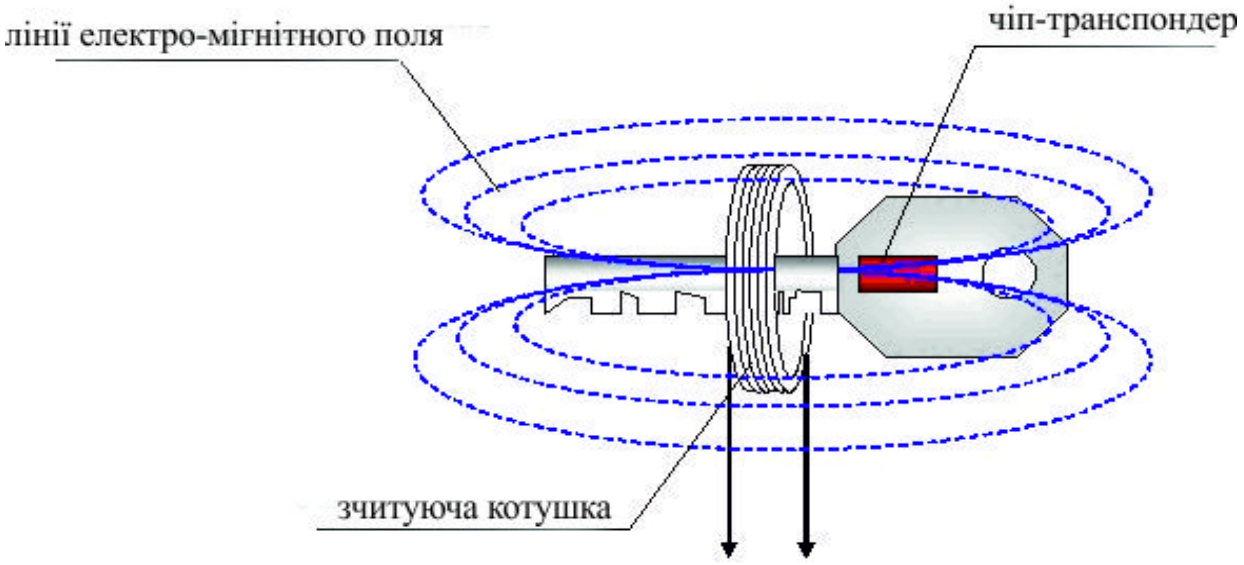


Рисунок 2.4- Схема зчитування коду активації імобілайзера з транспондера

Імобілайзер використовує шифрування в процесі передачі даних по радіоканалу. Ці системи, по суті, виконують процес бездротової ідентифікації власника ключа. При цьому секретний ключ, що зберігається в транспондері, не передається в ефір в будь-якому вигляді, а використовувався для криптографічного «підписування» запиту, отриманого від іммобілайзера. Структуру такої системи розробили інженери корпорації Texas Instruments[21]. Розроблений ними транспондер отримав назву Digital Signature Transponder (DST). Використання у алгоритмі DST схеми хешування зробило процес радіосніффінга абсолютно марним (до певного моменту), тому що через ефір передавалися настільки різні блоки даних, що логічно простежити хоч якусь залежність викликало велику складність. На рисунку 2.5. представлена схема реалізації криптошифрування алгоритму DST40.

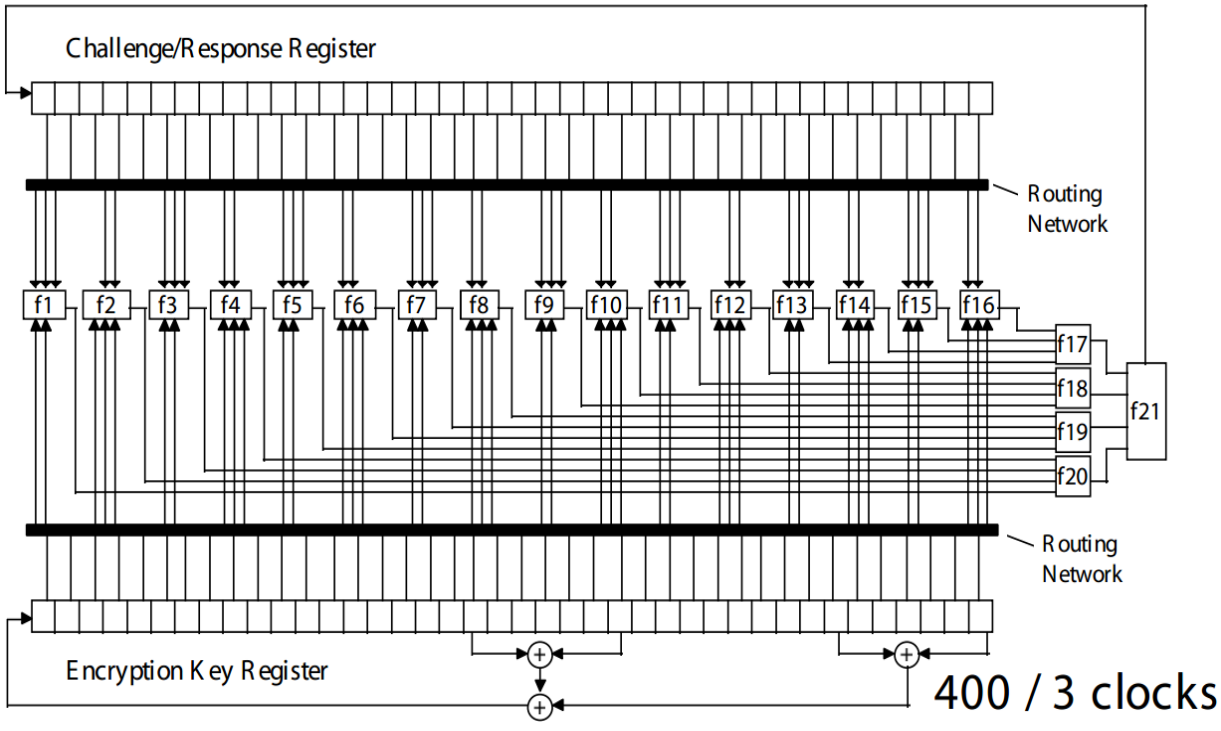


Рисунок 2.5- Схема реалізації криптошифрування алгоритму DST40

При типовому застосуванні іммобілайзер формує випадкове (random) слово-запит довжиною 40 біт і відправляє його в транспондер, використовуючи широтно-імпульсну модуляцію. У транспондері це слово фіксується шляхом зсуву в регістрі запиту. Слідом за цим спеціальна логічна

схема шифрування формує, використовуючи раніше отриману енергію накачування, відгук довжиною 24 біт (підпис). Як уже зазначалося, автори для спрощення викладу ототожнюють відгук з цифровим підписом і ігнорують блок фіксованих даних та інші доповнення у вихідному повідомленні, яке насправді, звичайно, набагато довше 24 біт.

Центральний блок іммобілайзера обчислює очікуваний відгук, використовуючи той же самий алгоритм і той же самий ключ шифрування, і порівнює результат розрахунку з відгуком, який приходить від транспондера в дійсності. Розрахунок виконується одночасно з встановленням зв'язку між транспондером і приймачем, після отримання відгуку транспондера. Якщо прийнятий і розрахунковий відгуки однакові, інформація направляється в центральний блок двигуна. Для додатків, що вимагають швидкої реакції, такі запит і відгук можуть бути сформовані під час чергового розблокування заздалегідь, і відгук буде зберігатися для наступного циклу (в регістрі відгуку).

Проте даний алгоритм шифрування має ряд функціональних недоліків:

-по-перше, по кожному такту регістри ключа шифрування і запиту/відповіді піддавалися мінімальним модифікаціям - всього лише в один біт;

по-друге, присутня наявність «слабкого» ключа шифрування, що складається з одних нулів - в процесі хешування він так і залишається обнуленим до самого кінця. Це відкривало можливість проведення над транспондером різних криптоаналітичних дослідів, здатних розкрити його внутрішню структуру;

по-третє, довжина ключа становила всього 40 біт, що зовсім недостатньо, щоб протистояти брутфорсним атакам [22], що виконується за допомогою апаратних засобів.

Транспондер є з'єднанням механічної мікро-конструкції з логічною схемою, яка працює при досить низькому енергоспоживанні [23]. В процесі накачування транспондера його мікросхема (IC) споживає струм менш 1мкА.

Це дозволяє конденсатору (capacitor) заряджатися навіть на значній відстані за розумний час, яке зазвичай становить менше 50 мс. Протягом процесу шифрування споживання струму становить менше 16мкА. Проте типовий діапазон зчитування порівняємо зі стандартною системою фіксованого коду (Read Only).

Для стійкої роботи крипто-транспондера в ньому застосовується кілька вбудованих схем контролю. Перш ніж транспондер вийде з режиму прийому вхідного повідомлення (Write) і виконає команди програмування відгуку (Program), буде проведено ряд перевірок (Check) (рисунок2.6).

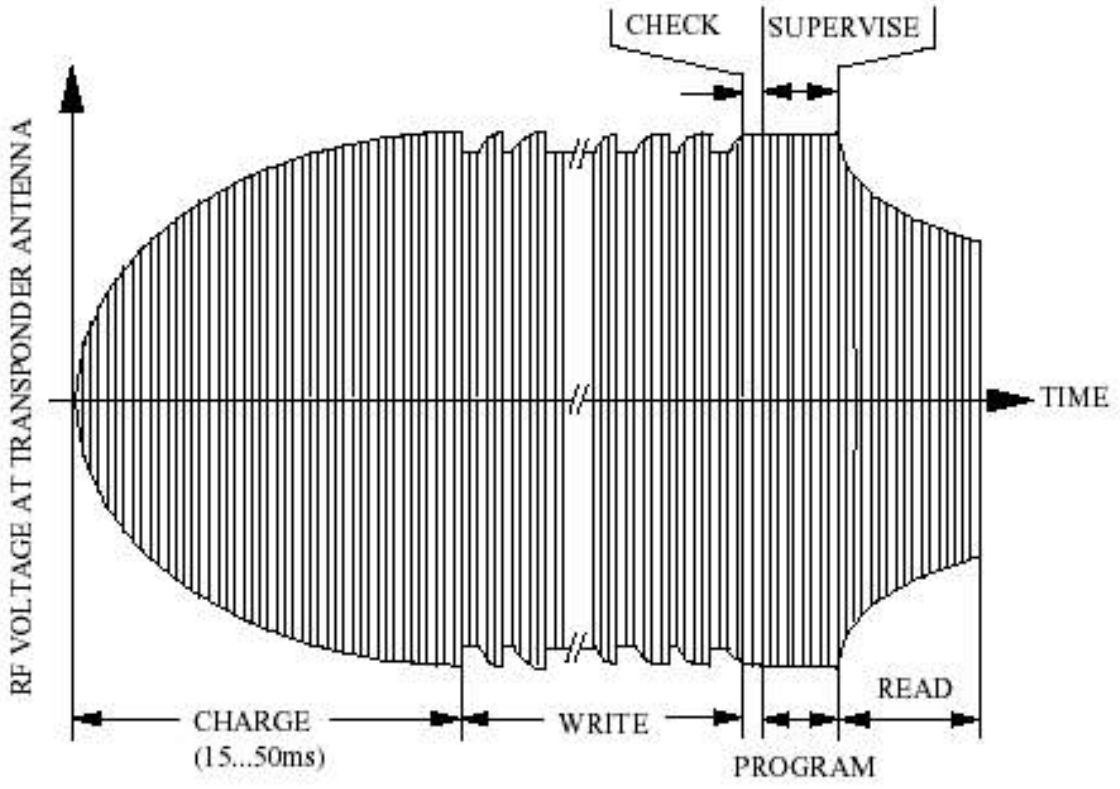


Рисунок 2.6- Часова діаграма прийомо-передачі секретного коду транспондером

Особливо важливим є контроль зупинки прийому, тому що, якщо ненавмисно заблокувати сторінку пам'яті транспондера, відгук не буде сформований. У штатному режимі роботи, згідно блок-схеми (рисунок 2.7) поточний сеанс прийому переривається сторожовим таймером, що є типовим рішенням захисту від перешкод в ефірі. До завантажування на стадії Write командам, даними і адресами застосовується обчислення 16-бітного

контрольного коду CRC відповідно со стандартом CCITT (Consultative Committee of International Telegraphy and Telephony)[24]. Cyclic Redundancy Check (CRC) контроль циклічним надлишковим кодом; зазвичай обчислюється по більш складним правилам, ніж підрахунок контрольної суми, але в даному випадку CRC може вважатися контрольною сумою. Підрахунок числа прийнятих біт контролює правильність закінчення сеансу прийому. Певні перевірки передують записи EEPROM-осередків пам'яті по включенню напруги програмування від внутрішнього акумулятора накачування (Charge Pump) (рисунок 2.7)

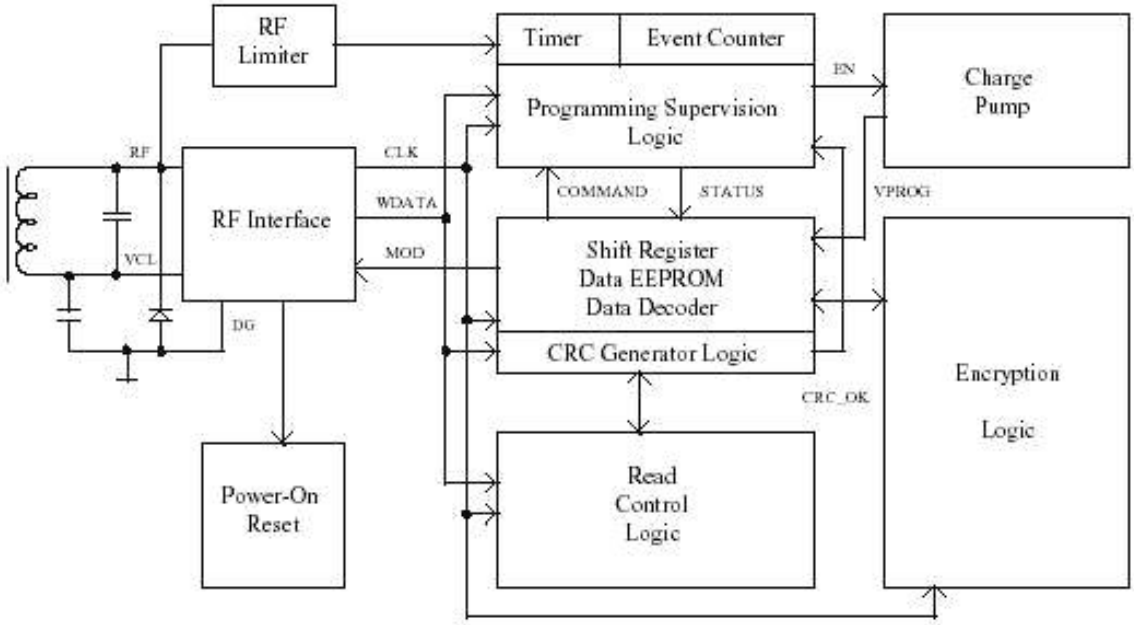


Рисунок 2.7 –Блок-схема крипто-транспондера

Програмування EEPROM зазвичай відбувається за стандартною системною шиною мікропроцесорного пристрою.. Запис кожного осередку EEPROM автоматично стирає стару інформацію в ній, тобто можна змінювати дані в будь-якому осередку, не зачіпаючи інші.

В процесі запису EEPROM напруга програмування має бути досить високою протягом відомого проміжку часу, щоб запис було виконано надійно.

Вбудована схема обмеження (RF Limiter) амплітуди радіосигналу несучої частоти захищає внутрішню мікросхему транспондера від

перевантаження в разі надмірної напруженості магнітного поля антени. Такий же обмежувач також використовується і в пристрої стеження за записом (Programming Supervision). Якщо схема входить в режим обмеження, це означає, що енергія для досягнення досить високої напруги програмування виконана. Режим роботи схеми обмеження відстежується кожні 800 мкс лічильником подій (Event Counter), поки акумулятор накопичує енергію (Charge). Як тільки режим обмеження реалізується, і буде зберігатися протягом зазначеного тимчасового вікна, акумулятор накачування готовий до роботи. Після цього стан схеми обмеження починає відслідковуватися лічильником подій безперервно, який оцінює величину сигналу на її виході. Якщо цей вихідний сигнал впаде внаслідок зовнішнього впливу, такого, наприклад, як метал або переміщення в поле антени, певний параметр завантаження не досягне потрібної величини за час сеансу прийому (фактична контрольна сума не співпаде з вкладеною у вихідне повідомлення). Цей стан фіксується як ознака подальшого формування недостовірного відгуку. Якщо виявлена подібна помилка, інформація про неї включається в вихідне повідомлення для реакції центрального блоку іммобілайзера. Крім того, вихідне повідомлення, що містить статус, адреси та дані, завжди захищене контрольною сумою CRC, щоб центральний блок міг перевірити відсутність внесення спотворення в інформацію при її передачі в ефірі.

В обох випадках вказівка на помилку CRC дозволяє шляхом автоматичної відправки нового запиту уникнути помилкового заблокування блоку управління двигуном, що логічно поєднується з затримкою обчислення зразковою підпису в ECU іммобілайзера до тих пір, поки зв'язок з транспондером не буде стійким.

Розглянемо принцип роботи імобілайзера на базі мікроконтролера PIC12F629 компании Microchip и RFID модуля ID-12 компании ID Innovation (рисунок2.8) [25].

Основні характеристики іммобілайзера:

- модуль ID-12 може бути встановлений в будь-якому місці і далеко від основної друкованої плати, для нього не потрібно зовнішніх елементів.

- якщо зловмисник викраде автомобіль (наприклад, коли двигун автомобіля вже працює), то коли зловмисник вимкне запалювання - завести автомобіль знову він вже не зможе.

Основні характеристики модуля ID-12:

- модуль має вбудовану антену, що дозволяє зчитувати ключі на відстані більше 12 см;

- підтримує роботу з форматами даних: ASCII, Wiegand26, Magnetic ABA Track2;

- алгоритм кодування Manchester 64-bit;

- робоча частота 125 кГц;

- напруга живлення 4.6 В - 5.4 В;

- розміри: 26 мм × 25 мм × 7 мм.

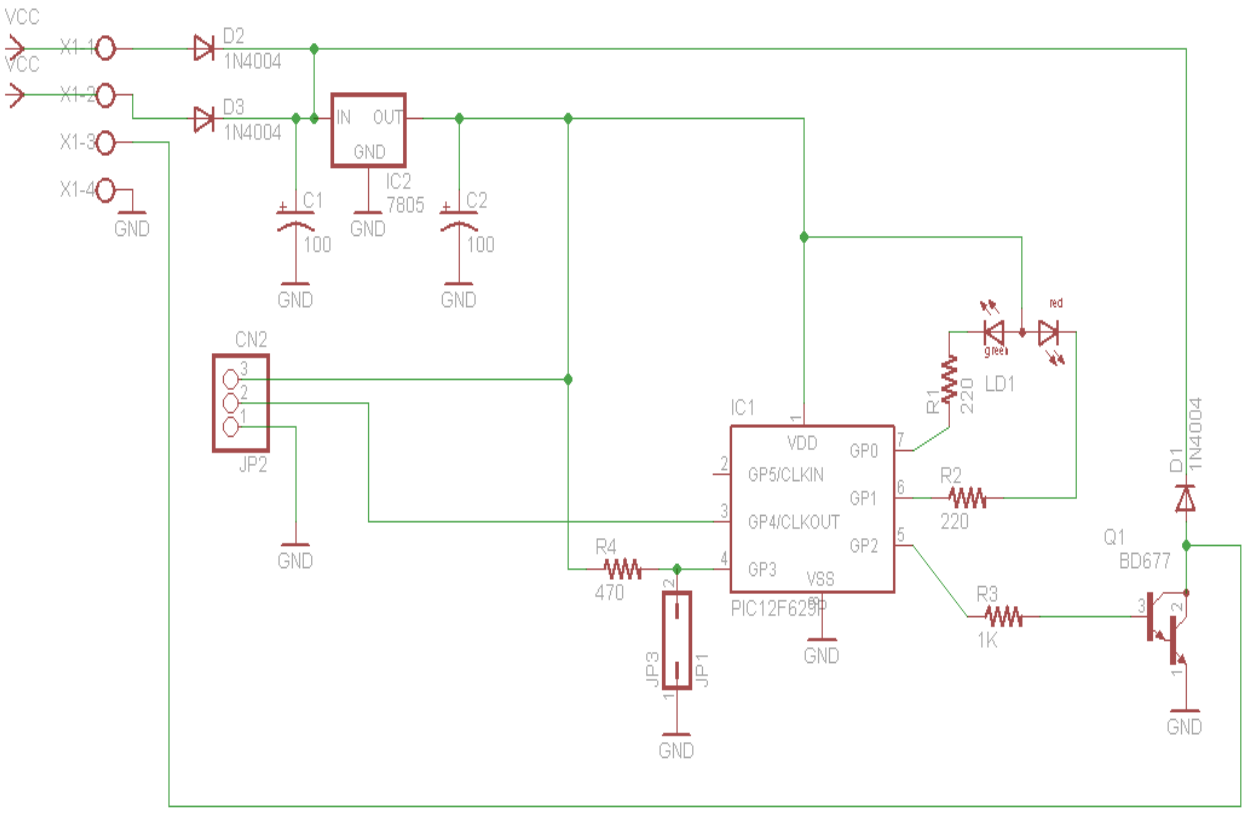


Рисунок 2.8- Схема імобілайзера на базі мікроконтролера PIC12F629 компанії Microchip

Живлення мікроконтролера PIC12F629F і модуля ID-12 +5.0 В подається від регулятора напруги IC2 7805, з використанням базових фільтруючих конденсаторів. Мікроконтролер постійно зчитує доступні дані від модуля ID-12. Як тільки карта (ключ) прочитаний, мікроконтролер порівнює дані з тими, що зберігаються в EEPROM, всього збережено може бути до 10 ключів. Якщо встановлений ключ збігається зі збереженим, то активується реле через керуючий транзистор Q1BD677 і виконання програми мікроконтролера припиняється. Якщо збігу немає, мікроконтролер знаходиться в режимі очікування даних. Двоколірний світлодіод служить для індикації стану.

Налаштування іммобілайзера зводиться до запису 10 ключів у пам'ять мікроконтролера шляхом включення перемички JP1. При програмуванні ключів необхідно подати живлення на пристрій при включеній перемичці. Двоколірний світлодіод загориться зеленим кольором, а потім загориться червоним. Тоді користувач може записати до 10 ключів. Помаранчеве свічення індикатора відповідає вдалому читання і запису ключа. Після програмування всіх 10 ключів, перемичку потрібно зняти, через деякий час апарат перейде в робочий режим і світлодіод буде світитися червоним кольором.

При читанні картки (ключа) світіння індикатора змінюється на помаранчевий і, якщо ключ вірний, світлодіод на півсекунди загоряється зеленим кольором і гасне, активується реле. Якщо ключ не вірний, то світлодіод загоряється знову червоним кольором і пристрій переходить в режим очікування наступного ключа.

Для можливості налагодження користувач може підключити вихід 2 мікроконтролера (GPIO5) і вивід GND до послідовного порту комп'ютера до сигналів Rx і GND відповідно. Це з'єднання не завжди працездатне, тому краще використовувати перетворювач логічних рівнів MAX232. Для налагодження потрібно лише програма HyperTerminal, швидкість обміну необхідно встановити 9600 кбіт/с.

2.2 Дослідження пристроїв глобального моніторингу та позиціонування для автомобільних сигналізацій

Пристрій позиціонування являє собою стаціонарний прилад, який стає частиною бортового навігаційного обладнання. Він призначений для прийому і передачі інформації про місцезнаходження, швидкості і маршруту руху об'єкта в режимі реального часу. Застосування GPS [23] трекера актуально для будь-яких видів стеження об'єктів і суб'єктів. Наявність трекера в авто дає можливість відстежити його місцезнаходження в разі викрадення, а також виявити неналежне використання автомобіля.

Основою роботи GPS-маячка[27] є використання двох різних модулів зв'язку - GPS і GPRS. Система GPS покриває близько 99% поверхні земної кулі, що дає можливість відстежувати місце розташування трекера практично в будь-якому місці планети. Дані про знаходження і переміщення передаються на приймальний пристрій через канал GPRS. Приймальним пристроєм може бути комунікатор, планшетний або персональний комп'ютер, ноутбук, або віддалений сервер. Трекер оснащений резервним живленням, що дозволяє йому працювати тривалий час в автономному режимі. Крім того, він може поєднувати в собі функції комутаційного пристрою і портативного маяка. Вибрані трекери використовують супутникову систему навігації - GPS (Global Positioning System - система глобального позиціонування). GPS дозволяє в будь-якому місці Землі (не включаючи приполярні області), майже при будь-якій погоді визначити місце розташування і швидкість об'єктів.

Принцип визначення координат об'єкту в системі GPS заснований на обчисленні відстані від нього до декількох супутників, точні координати яких відомі [28]. Інформація про відстані мінімум до 3 супутників дозволяє однозначно визначити координати об'єкта як точку перетину сфер, центр яких супутники, а радіус вимірювання відстаней (рисунок 2.9).

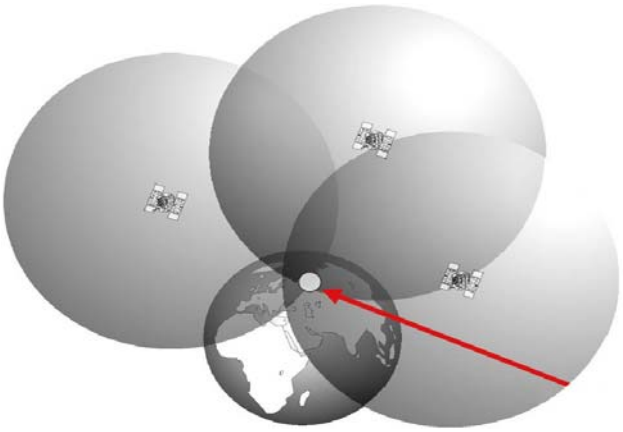


Рисунок 2.9- Визначення місцеположення за допомогою 3-ох супутників

Відстань до кожного з супутників визначається як час проходження радіосигналу від супутника до приймача помножене на швидкість світла. Визначення часу проходження радіосигналу вирішується за рахунок генерації і передачі з супутника сигналу, модульованого за допомогою спеціальної послідовності. Точно такий же сигнал генерується в GPS приймачі, а аналіз відставання прийнятого сигналу від внутрішнього дозволяє визначити час його проходження (рисунок 2.10).

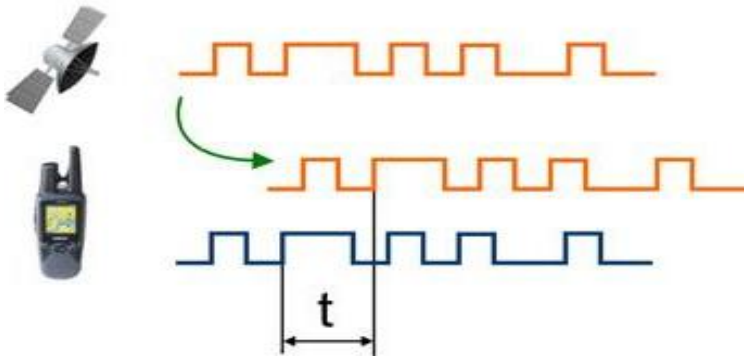


Рисунок 2.10- Час проходження сигнала з супутника.

Для точного визначення часу проходження сигналу годинник GPS приймача і супутника повинні бути максимально синхронізовані, відхилення навіть на кілька мікросекунд призводить до похибки вимірювання в десятки кілометрів. На супутнику для цих цілей є високоточні атомні годинники. Встановити аналогічні годинники в GPS приймач неможливо (використовуються звичайні кварцові годинники), тому для синхронізації часу використовуються додаткові сигнали, як мінімум з ще одного супутника.

На практиці при хорошій видимості небосхилу GPS приймачі отримують сигнали відразу від безлічі супутників (до 10-12), що дозволяє їм синхронізувати годинник і визначати координати з досить високою точністю (рисунок 2.11).

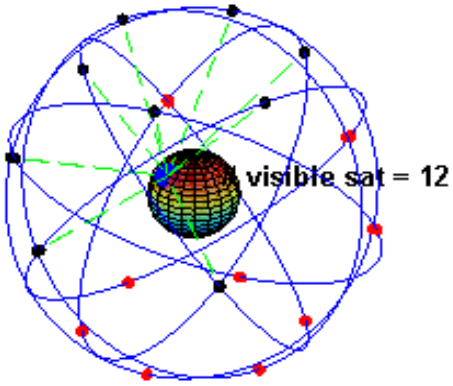


Рисунок 2.11-Принцип роботи системи GPS

Поряд з послідовністю, по якій визначається час поширення сигналу, кожен супутник передає двійкову інформацію - альманах і ефемериди [28]. Альманах містить інформацію про поточний стан і розрахункову орбіту всіх супутників (отримавши інформацію від одного супутника, з'являється можливість звузити сектори пошуку сигналів інших супутників).

Ефемериди - уточнену інформацію про орбіті конкретного супутника, передає сигнал (реальна орбіта супутника може відрізнятися від розрахункової). Саме точні дані про поточний стан супутників дозволяють GPS приймачу розраховувати щодо них власне місце розташування.

Система GSM [28] складається з безлічі підсистем, але для передачі інформації по GPRS використовується 2 з них: підсистема базових станцій і підсистема GPRS станцій розставлених таким чином, що області їх покриття утворюють соти контролерів базових станцій.

Підсистема GPRS складається з пакетного комутатора і GPRS шлюзу. Як тільки трекер запросить обмін даними через GPRS, GSM-модуль посилає запит на базову станцію, яка в свою чергу передає інформацію на контролер базових станцій. Контролер базових станцій з'єднується з пакетним комутатором. Пакетний комутатор виконує функції обробки пакетної

інформації і перетворення кадрів GSM у формати, які використовуються протоколами TCP/IP глобальної комп'ютерної мережі Internet. Виконавши перетворення він відсилає дані на GPRS шлюз. Шлюз забезпечує зв'язок системи GPRS з пакетними мережами передачі даних: Internet. Він містить всю необхідну інформацію про мережі, куди абоненти GPRS можуть отримувати доступ, а також параметри з'єднання.

GPS модулі трекера відсилають інформацію керуючому пристрою в форматі протоколу NMEA 0183[29]. NMEA 0183 - текстовий протокол зв'язку морського (як правило, навігаційного) обладнання (або обладнання, що використовується в поїздах) між собою. GPS модуль відсилає безліч рядків у форматі даного протоколу, але в даному проекті мене цікавить лише RMC рядок, яка представляє собою «рекомендований мінімум навігаційних даних».

Трекер складається з 3-х блоків:

1) GPS приймач. Завдання приймача - як описано вище, прийняти сигнали з супутників, визначати своє поточне місцезнаходження супутників, визначити відстань до супутників, визначити своє місце розташування, швидкість, напрямок руху і відправити ці дані на керуючий пристрій. Як приймача в «GPS трекер» виступає GPS модуль Quectel L10. Як приймач в комунікаторі виступає вбудований в комунікатор GPS модуль.

2)Передавач. Завдання передавача - передати отримані дані з приймача на віддалений сервер в заданому форматі. Як передавача в «GPS трекер» виступає GSM модуль SIM 900D [30]. Як передавача в комунікаторі виступає вбудований телефонний модуль.

3)Керуючий пристрій. Завдання керуючого пристрою - зв'язати в єдину систему (трекер) приймач і передавач, тобто прийняти даний з приймача і відправити через передавач на віддалений сервер. В якості керуючого пристрою в «GPS трекер» виступає мікроконтролер STM32F100. В якості керуючого пристрою в комунікаторі виступає мікроконтролер виробника пристрою (рисунок 2.12).

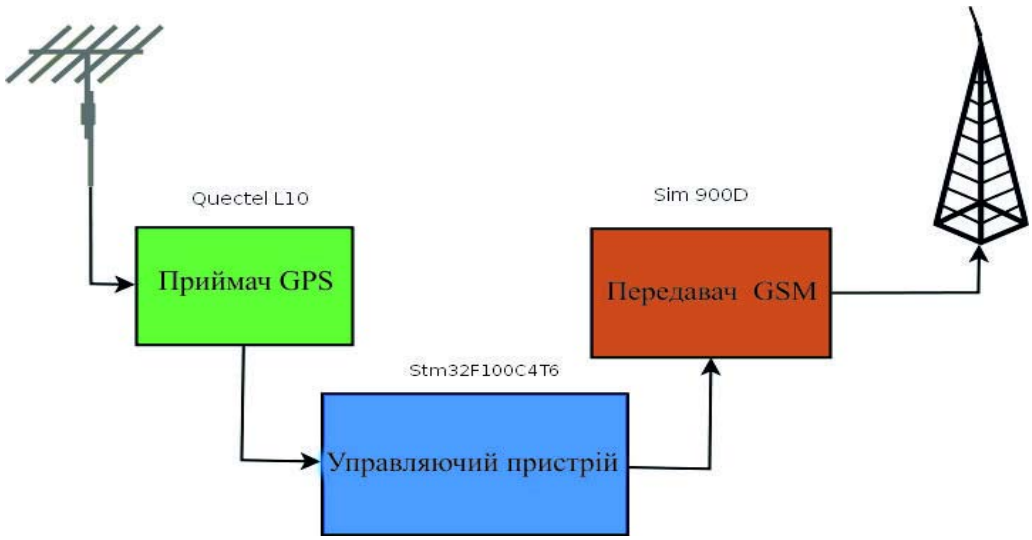


Рисунок 2.12-Схема GPS трекера

Розглянемо бюджетний GSM/ GPRS SIM900D модуль компанії SIMCOM. Даний модуль має наступні переваги: популярний форм-фактор з торцевими пайками, що дозволяє не використовувати дорогі технології монтажу та контролю пайки, зручний вбудований TCP / IP стек, низька ціна. Характеристики GSM модуля SIM900D (рисунок 2.13):

• чотири діапазони GSM 850/900/1800/1900 МГц;

• клас передачі даних GPRS multi-slot class 10/8;

• відповідність стандарту GSM фази 2/2 +;

• клас потужності 4 (2 Вт в діапазонах 850/900 МГц) ;

• клас потужності 1 (1 Вт в діапазонах 1800 / 1900MHz) ;

•управління AT командами (GSM 07.07, 07.05 і ф;

• фірмові AT команди SIMCOM) ;

• вбудований стек TCP / IP, UDP / IP;

• протоколи HTTP і FTP;

• embedded AT - робота з призначеним для користувача ПЗ;

• контролер заряду Li акумулятора;

• маса 4,2 г;

• температурний діапазон -40 °C ... +80 °C;

• напруга 3,2 ... 4,8 В.

а) б)

Рисунок 2.13- GSM/ GPRS модуль SIM900D

а) значення виходів; б) чіп пристрою

Розглянемо GPS модуль GPS Quectel L10 [31]модуль який задає новий стандарт продуктивності завдяки високоефективному набору системної логіки MTK. L10 має 210 каналів PRN і завдяки 66 каналам пошуку та 22-ом каналам одночасного спостереження, знаходить і відстежує супутники за дуже короткий час навіть в умовах слабкого сигналу. Цей універсальний, GPS приймач об'єднує в собі широкий набір функцій з гнучкими можливостями по підключенню. Простота його інтегрування у вироби дозволяє скоротити час розробки нових виробів для автомобільних, промислових і споживчих ринків. Пристрій GPS Quectel L10 має наступні характеристики:

• 210 PRN каналів з 66 каналами пошуку і 22 каналами стеження,

• -165dBm чутливість в режимі стеження,

• Найвища чутливість в режимі пошуку, -148dBm

• Низький рівень споживання енергії, 38mA (з пасивної антеною)

• Захист всіх входів від електростатичного напруги

• 4 Мбіт вбудованої флеш-пам'яті

• Більш досконала Перешкодостійка схема, що дозволяє інтегрувати модулі в інші бездротові рішення, такі як: WiFi, WiMax, CDMA і GSM

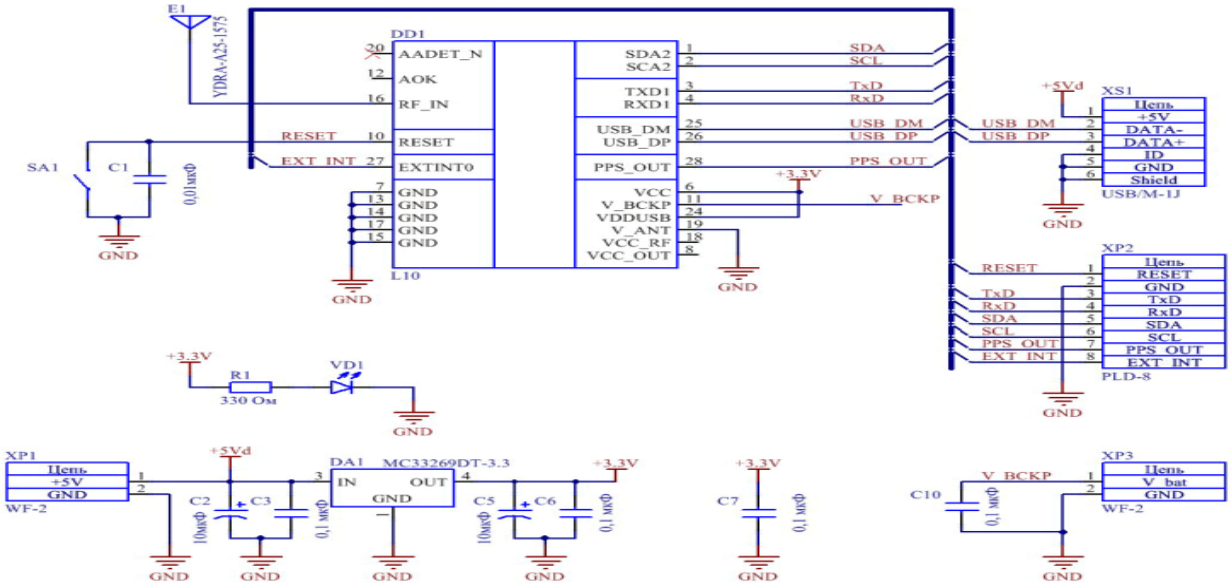
• Готовність до роботи з AGPS

• Більш точна навігація в умовах щільної міської висотної забудови завдяки компенсації сигналів, що відбиваються.

• Частота оновлення координат 5 Гц

• Повно-швидкісний сумісний з USB 2.0 інтерфейс

а)



б)

Рисунок 2.14- Модуль GPS Quectel L10 (а), схема розведення плати для підключення модуля GPS Quectel L10

Плата з підключеним модулем GPS Quectel L10 та представлена на рис 2.15.

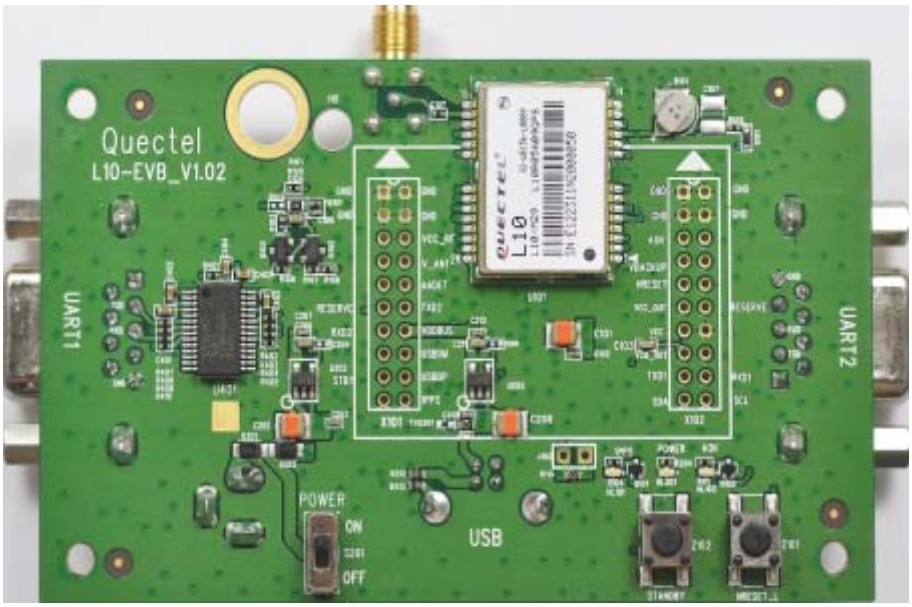


Рисунок 2.15- Системна плата з модулем GPS Quectel L10

У якості пристрою управління модулями GPS і GSM доцільно використати контролер STM32f100[32]. Перевагами цього модуля являється дешева ціна та малий розмір (LQFP48 7 × 7 мм) для більш щільного компонування, та зменшення розміру пристрою. Мікроконтролер STM32f100(рисунок2.16) має наступні особливості:

• до семи 16-бітних ШІМ-таймерів, зокрема таймер з розширеним управлінням: всього 26 каналів;

• три незалежна 16-бітна ШІМ-таймерів з комплементарними виходами і генератором пауза не перекриття;

• вбудований 12-бітний здвоєний ЦАП з підтримкою прямого доступу до пам'яті (DMA), і буферизованного виходами;

• пристрої введення-виведення для управління споживчою електронікою (CEC)

• ЦВК, I²C (400кГц), провідний і підлеглий SPI (до 12Мбіт / сек), УСАПП (до 3Мбіт / сек)

• 32-бітний набір інструкцій ARM Cortex-M3 Thumb-2 і 7-канальний DMA

• прискорювач CRC з підтримкою DMA

• Вбудована схема скидання при подачі живлення і при неприпустимому зниженні напруги живлення, сторожовий таймер, відкалібрований на фазі виробництво, RC-генератор частота 8 МГц і 40 кГц для синхронізації годин реального часу (RTC) і сторожового таймера.

Рисунок 2.16- Мікроконтролер STM32f100

До переваг мікроконтролера STM32f100 можна віднести:

• ідеально підходить для застосування в керуючих системах;

• ідеальні для виконання функцій управління в складі електрообладнання, та прилади індукційного нагріву;

• знижує загальна собівартість система;

• знижує складність проектування і мінімізує використання ЦП, пристрої введення-виведення і пам'яті;

• розширені комунікаційні можливості;

• хороша продуктивність, завдяки 16-бітній щільності коду;

• спрощує перевірку флеш-пам'яті на цілісність;

• знижує собівартість системи.

Параметри мікроконтролера STM32f100 наведено у табл.2.1.

Таблиця 2.1. Параметри мікроконтролера STM32f100

ЦПУ: Ядро	Cortex-M3
ЦПУ: F,МГц	от 0 до 24
Пам’ять: Flash,КБайт	16
Пам’ять: RAM,КБайт	4
I/O (макс.),шт.	37
Таймери: 16-бит,шт	6
Таймери: Канали ШІМ,шт	3
Таймери: RTC	так
Интерфейс: UART,шт	2
Интерфейс: SPI,шт	1
Интерфейс: I2C,шт	1
Интерфейс: DMA,шт	1
Аналогові входи: Разрядів АЦП,бит	12
Аналогові входи: Каналів АЦП,шт	10
Аналогові виходи: Разрядів ЦАП,бит	12
Аналоговые выходы: Каналів ЦАП,шт	2
VCC,В	от 2 до 3.6
TA,°C	от -40 до 105
Корпус	LQFP-48

Середовищем розробки програмного коду для мікроконтролерів ARM є програма CooCox CoIDE(рисунок 2.17) [33]. Програма заснована на базі Eclipse[34]h редактор коду включає в себе підсвічування синтаксису і спливаючі підказки. Присутні функції глобальної заміни змінної та

пропозиції варіантів закінчення коду. Середовище підтримує мікроконтролери серії ST, а також ряд інших сімейств: Atmel, Holtek, Freescale, Nuvoton, NXP, Energy Micro, Texas Instruments [35]. Вбудований дебагер ST-Link підтримує всі основні режими налагодження.

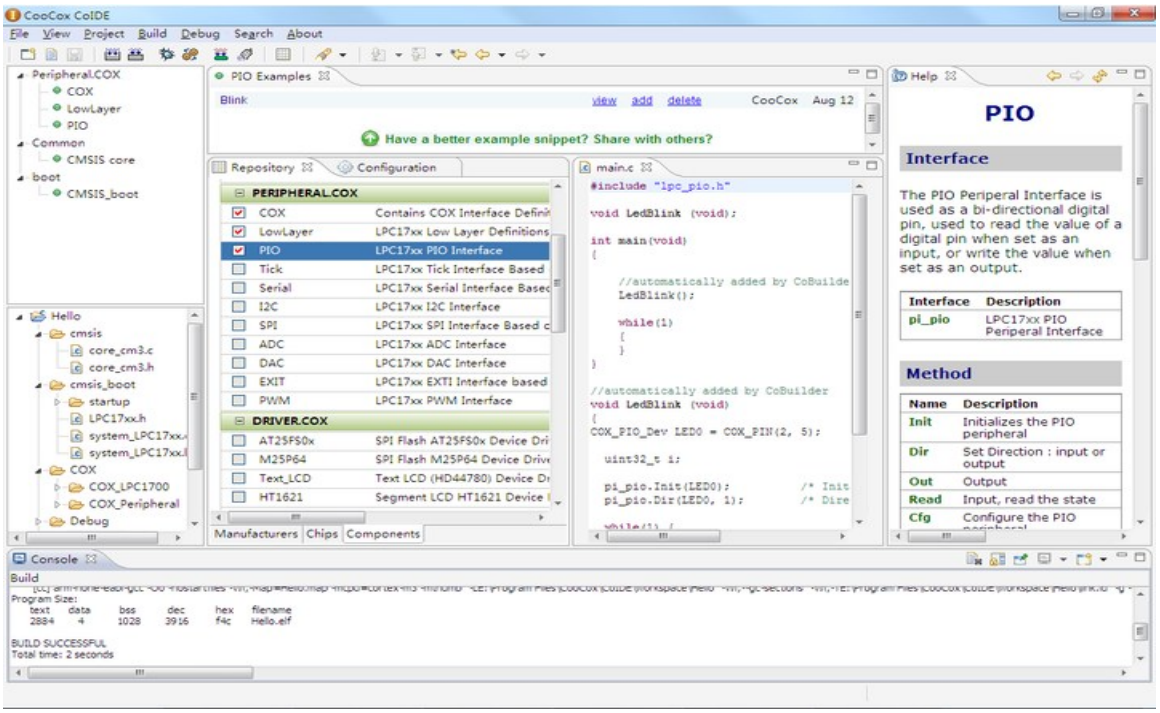


Рисунок 2.17- Вікно програми CooCox CoIDE для мікроконтролера STM32f100

При створенні нового проекту пропонується вибір використовуваної мікросхеми і бібліотек. Можливий перегляд коротких характеристик кожного чіпа. CoIDE автоматично створює всю структуру проекту, а також підключає всі інші необхідні для роботи бібліотеки. Кожна з них містить кілька готових прикладів, які можна використовувати в проекті. Присутня функція поповнення бібліотек власними прикладами. При підключенні нових бібліотек до проекту враховуються всі залежності між ними.

Розглянемо пристрій глобального моніторингу на основі GPS і GSM модулів Starline M32T[18] (рисунок 2.18). M32T можна використовувати і в якості самостійної охоронної системи, але з небагатим набором функцій. Сповіщення будуть реалізовані у вигляді SMS-повідомлень або дзвінків з вказівкою причини спрацювання.

а) б)

Рисунок 2.18- Пристрій глобального моніторингу на основі GPS і GSM модулів Starline M32T (а), та GSM модуль(б)

Передбачені виходи на датчики дверей, багажник, гальма і ручне гальмо. Для спрацьовування кожного можна вибрати спосіб оповіщення і текст, якщо використовується смс повідомлення. Для безпеки є такі функції:

-при спробі угону, користувач може відправити команду, яка зупинить двигун;

-якщо автомобіль покинув задану зону комфорту, то буде вироблено сповіщення власника. Програмна начинка модуля дозволяє проводити діагностику систем автомобіля на наявність помилок по OBD II. У разі виявлення будь-яких несправностей, M32T CAN відправить користувачеві звіт про проблеми на мобільний телефон.

2.3. Дослідження вимірювальних об'єктів автосигналізації і методи отримання від них вимірювальної інформації

Важливою частиною будь-якого автомобіля є датчики. Їх в своєму складі також має будь-яка автомобільна сигналізація. Під час будь-якого впливу на автомобіль, вони передають інформацію до центрального блоку про ступінь небезпеки впливу і його час. З огляду на ці дії можуть бути найрізноманітніші датчики, що повинні забезпечувати високу надійність і

достовірність контрольованих параметрів, залишаючи без уваги все те, що можна віднести до помилкових збурень: коливання і вібрації від вантажівки, що проїхала поруч великовантажного автомобіля, вплив кліматичних і атмосферних явищ, електромагнітні перешкоди [34].

Автомобільні сигналізації використовують різноманітні датчики, що працюють на основі різних принципів, і кожен з них захищає автомобіль від тієї чи іншої небезпеки. Від удару, від відкриття дверей, вікон, від дотику до автомобіля, від проникнення в салон. Кожен датчик повинен інформувати систему сигналізації про задуми протиправних дій по відношенню до автомобіля.

Одним з перших датчиків яким комплектувались автомобільні охоронні системи з моменту своєї появи були "датчики качка". Вони реагували на хитання кузова автомобіля, яке могло виникнути при знятті коліс або іншому схожому впливі. При розгойдуванні машини - сигналізація спрацьовувала. Однак, якщо зловмисник розбивав скло, то найчастіше сигналізація не спрацьовувала.

Поступово датчики качка витіснили датчики удару (шок-сенсори). Вони дещо гірше реагували на хитання автомобіля, але, зате, дуже чітко відслідковували удари по кузову. Перші датчики удару мали тільки один поріг чутливості. Такі датчики не дуже зручні. Тому при його налаштуванні використовувався дуже високий поріг спрацьовування щоб автомобільна сигналізація не спрацьовувала від випадкових ударів Двох порогові датчики удару налаштовувались на силу впливу при якій спрацює перший поріг і другий поріг. Якщо відбувається випадковий, несильний вплив на автомобіль, то система просто спрацює коротким звуком сирени. При сильному впливі система відпрацює програму відповідної підвищеної небезпеки. У дуже дорогих системах встановлюються датчики які окремо реєструють поздовжні і поперечні коливання кузова автомобіля. Такий принцип дії дозволяє практично виключити помилкові спрацьовування. Також застосовуються датчики у яких настройка сили удару першого і

другого порога відбувається з пульта сигналізації. Система вводиться в режим програмування, по кузову автомобіля наноситься удар певної сили. Датчик сам запам'ятовує його. Тепер це буде перший поріг. Точно так само відбувається настройка і другого порога. На рисунку 2.19 представлено двох-пороговий датчик удару KY-031. Модуль датчика найбільш чутливий до ударів спрямованих поперек площині плати. Вплив сприймає чутливий елемент, що представляє собою пружину, кінці якої оточені контактами. При ударі пружина згинається, кінець пружини дотикається контактів і кола датчика KY-031 замикається. Як зображено на схемі між входом живлення і виходом датчика знаходиться резистор 10 кОМ. При спрацьовуванні датчика замикається контакт, який може бути з'єднаний з входом самих різних приладів.

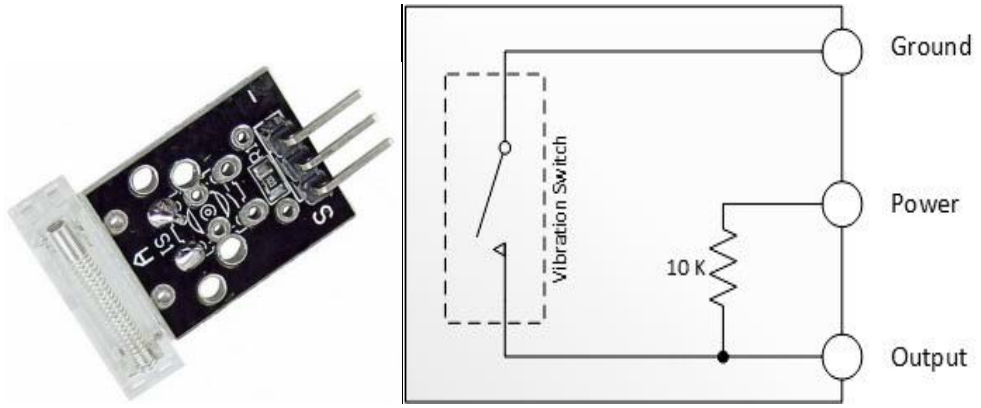


Рисунок 2.19- Датчик удару KY-031

Ультразвуковий датчик здійснює виявлення перебування сторонніх всередині салону автомобіля. Два виносних мікрофона постійно контролюють салон в режимі охорони. Цей високочутливий датчик складається з посилаючого сигналу випромінювачем ультразвукових хвиль і приймача, що приймає цей сигнал. На рисунку 2.20 представлено ультразвуковий датчик HC-S90. Принцип роботи пристрою дуже простий. Пристрій посилає 8 імпульсів звукових хвиль з частотою 40 кГц і приймає відбиту хвилю заданої довжини. Далі вимірюється тимчасова затримка між відправленим і прийнятим сигналом, і відбувається обчислення відстані за формулою D = TS / 2, де D - це відстань, T - тимчасова затримка і S -

швидкість звукового сигналу. На виході модуля HC-SR04 з'являється імпульс з шириною, пропорційною відстані. Якщо сигнал, що приймається переривається або спотворюється, то сигналізація спрацьовує.

Рисунок 2.20- Ультразвуковий датчик HC-S90

Будь-яке пересування об'єкта досить великого розміру в салоні, буде негайно виявлено і система сигналізації підніме тривогу. Однак, чутливість його така, що він здатний зафіксувати і рух повітря в салоні, викликані зміною температури при охолодженні автомобіля взимку і навіть акустичні шуми. Недолік цих датчиків - помилкові спрацьовування при різких коливаннях температури і сильних зовнішніх звукових коливань.

Всі недоліки ультрасоніків позбавлені у мікрохвильовому датчику [27]. Він був винайдений і застосовувався для охорони відкритих автомобілів - кабріолетів. Принцип дії наступний. Датчик накриває автомобіль двома полями. Перше поле може закінчуватися і за межами кузова автомобіля (на відстані 20 - 15 см). Це перший поріг. Друге поле бере під свій контроль салон автомобіля. Це другий поріг. Якщо людина підійшла надто близько до автомобіля і перетнула перше поле, то, як у випадку з датчиком удару, система сигналізації зробить звукове попередження. Якщо ж викрадач потрапив всередину автомобіля, він виявиться в зоні дії другого поля, і тоді система підніме тривогу. На рисунку 2.21 представлено мікрохвильовий датчик CID-41

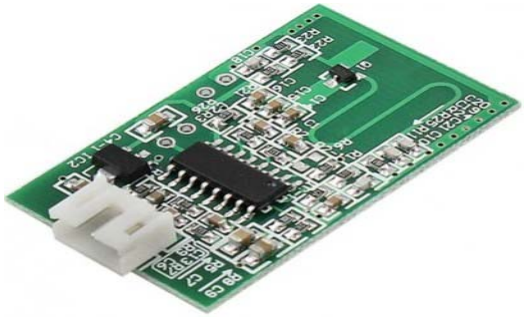


Рисунок 2.21- Мікрохвильовий датчик CID-41

Мікрохвильовий датчик має наступні характеристики:

- живлення: 3.3-20VDC;
- струм: 4MA;
- розмір: 23 * 33 мм;
-потужність передачі: 2 МВт;
-вихідний сигнал: TTL (3 В / 5 В), повторний запуск;
-чутлива відстань: 4-8 м;
- кут: 180 градусів;
-час затримки замовчуванням 20S/30S.

При роботі системи управління автосигналізацією використовуються сигнали, що надходять від датчиків закриття / відкриття дверей і капота. За допомогою інформації, що надходить від даних датчиків, контролером виробляється відповідний алгоритм подальшої роботи всієї системи. Функціональна схема датчика відкриття / закриття дверей і капота автомобіля представлена на рисунку 2.22.

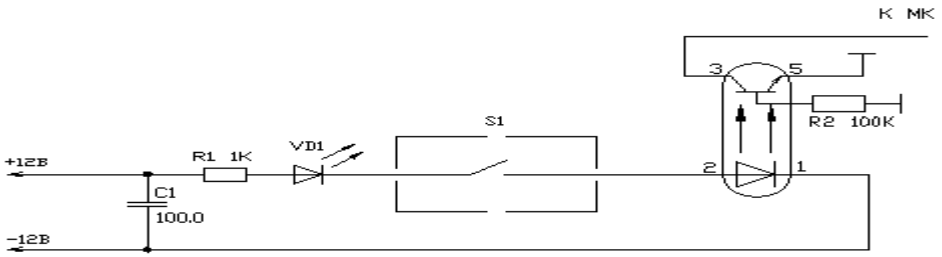


Рисунок 2.22- Функціональна схема роботи датчика відкриття закриття дверей

Датчик запалювання зібраний на операційному підсилювачі (ОП). Провідник, з'єднаний з входом ОП намотаний по спіралі (у вигляді обмотки

трансформатора) на силовий провід, що йде від котушки запалювання до розподільника запалювання (трамблера) (рисунок 2.23).

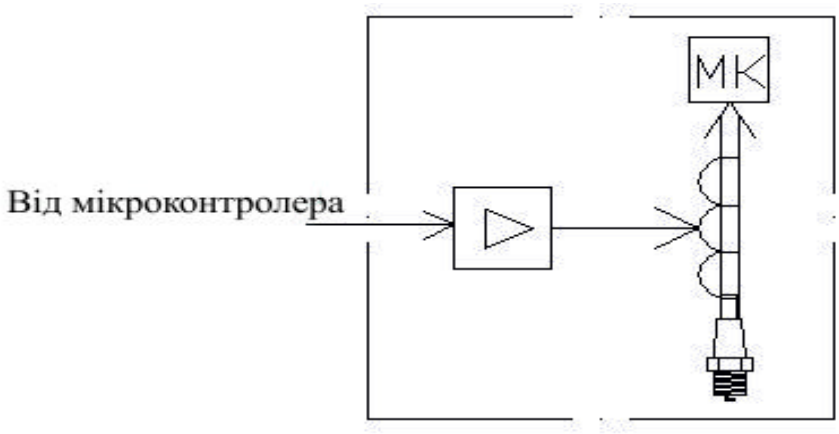


Рисунок 2.23-Структурна схема датчика запалювання

В результаті заведення автомобіля в силовому проводі виникає ЕРС, яка призводить до зміни різниці потенціалів в намотаному провіднику і виникнення напруги на вході в операційному підсилювачі. Мікроконтролер отримуючи сигнал від датчика сигналізує про включення запалювання. Якщо при цьому сигналізація не була відключена (тобто відбулася спроба викрадення автомобіля), то відбудеться спрацьовування сирени.

У багатьох автомобілів компонування агрегатів під капотом виконана таким чином, що можна просто перекусити дроти, що йдуть від акумулятора до розподільчого блоку авто сигналізації (рисунок 2.24).

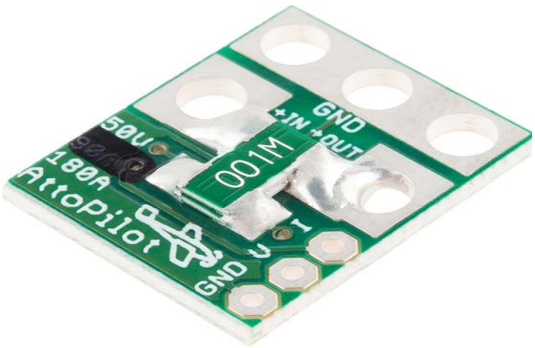


Рисунок 2.24- Датчик падіння напруги

Для того, щоб цей факт не залишився непоміченим і існують датчики падіння напруги [36]. Вони бувають двох основних типів. Датчик першого типу спрацьовує коли напруга падає нижче встановленого заздалегідь на заводі порогу (наприклад, 8 Вольт). Датчик другого типу спрацьовує коли

відбувається стрибок напруги вниз на задану величину (наприклад, 1 Вольт). Такий датчик зреагує навіть в разі якщо викрадач відкриває двері, запалюється лампочка салонного освітлення, відбувається невелике падіння напруги, яке тут же реєструється.

Потенціометр або змінний резистор використовується для управління зміною положення центрального блоку управління. Він має три контакти підключаються наступним чином: Два крайніх контакти (як правило) це живлення і земля, а середній - інформаційний. Детальна характеристика наведене в табл. 2.2.

Таблиця 2.2 – Харатеристика потенціометра

Потужність	0,25 Вт
Точність	± 20 %
Максимальна робоча напруга	250 В
Кут повороту движка	250 °
Характеристика змін опору	лінійна

Зображення потенціометру представлено на рисунку2.25.

Рисунок 2.25 – Вигляд потенціометра

Інфрачервоний давач руху дозволяє виявляти рух людини на відстані до 7 метрів (можна регулювати). Має два входи живлення (+ 5В і Земля) і один цифровий вихід, за яким можна знімати дані. Якщо перешкод немає, то на ньому буде високий рівень (3.3В), якщо є – низький (0В). Якщо перемичка встановлена в положення Н, то на виході буде високий рівень весь час, поки

давач буде вловлювати рух, якщо в стан L, то стан виходу буде переключатися з високого на низький і назад приблизно раз на секунду. Характеристика давача руху наведена в табиці 2.3.

Таблиця 2.3 – Характеристика давача руху

Діапазон спрацювання	110 °
Живлення	4,5 – 20 В
Вихідна напруга логічного рівня	0 – 3,3 В (регулюється)
Час затримки	0,3 – 18 с (регулюється)
Метод спрацювання	L – неповторюване, H – повторюване
Споживаний струм	0,05 мА
Робочі температури	– 20 °С – +50 °С
Розміри	32х24мм

Зображення давача руху зображено на рисунок 2.26.

Рисунок 2.26 – Давач руху

Інфрачервоний (ІЧ) спектр не видний людському оку, але відмінно сприймається цифровими камерами і ІЧ приймачами. Модуль ІЧ Приймача дозволить легко реалізувати дистанційне керування платою з пульта дистанційного керування від різної техніки. Для роботи з даним модулем "з коробки" необхідний пульт дистанційного керування з частотою 38 кГц. Плюсом даної плати є цанговий роз'єм, що дозволяє без застосування пайки замінити ІЧ приймач на інший, що працює на частоті необхідної для нашого проекту. Вигляд ІЧ приймача зображено на рисунку 2.27, де 1 – OUT (сигнал) до Pin 6 (контакт 6), 2 – В/с(+) до 5В, 3 – GND к GND.

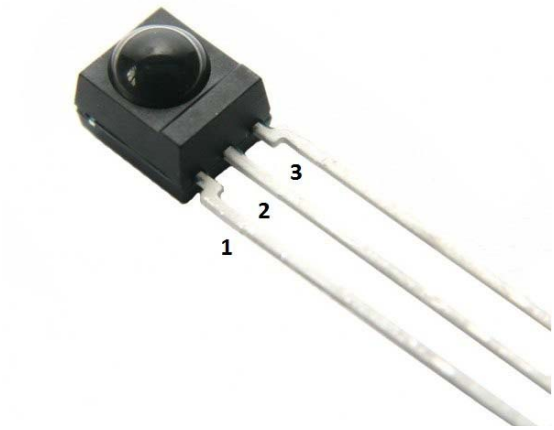


Рисунок 2.27 – ІЧ приймач

Детальніша характеристика ІЧ приймача наведена в таблиці 2.4.

Таблиця 2.4 – Характеристика ІЧ приймача

Напруга живлення	2,7 – 5,5 В
Частота модуляції	38 кГц
Діапазон температур	– 20 + 80 °С
Інтерфейс	Цифровий

Отже датчики є допоміжним обладнанням автосигналізацій, за допомогою яких центральний блок управління реагує та сигналізує про можливе вторгнення на периметр автомобіля.

3. РЕАЛІЗАЦІЯ АЛГОРИТМУ ТА РОЗРАХУНОК СИСТЕМИ УПРАВЛІННЯ АВТОМОБІЛЬНОЮ СИГНАЛІЗАЦІЄЮ

3.1. Програмно-апаратна реалізація принципів формування криптографічного біт-орієнтованого коду Галуа для авто сигналізації

Код Галуа є псевдовипадковою послідовністю з періодом ($2^{64} - 1$) біт. Для ідентифікації передавача використовують блоки довжиною 32 біта. Унікальний для кожного передавача 64-битовый ключ – це початкове положення регістру, що зміщує в генераторі псевдовипадкових послідовностей.

Послідовності зсувних регістрів, й генерують псевдовипадковий сигнал, що давно використовують у криптографії, у дослідженнях динаміки систем автоматики. Їх математична теорія добре розроблена, вона легко реалізується, й застосовувалася в криптографії ще до появи електроніки.

Період такого генератора не більший, ніж *m-1*. Якщо *a*, *b* і *m* обрані правильно, то генератор буде генератором з максимальним періодом (генератор *M*-послідовності), і його період буде дорівнювати m. Детальний опис вибору констант для отримання максимального періоду описано у роботах [37].

Найпростішим видом генератора кодових послідовностей є лінійний регістр зі зворотним зв’язком (рисунок 3.1). Зворотний зв’язок являє собою логічний елемент XOR для деяких бітів регістра, перелік цих бітів називається відвідною послідовністю (tap sequence).

Коли потрібно витягти біт, всі біти регістру зсуваються вправо на 1 позицію. Новий крайній лівий біт є функцією всіх інших бітів регістра. На виході зсувного регістру виявляється один, зазвичай молодший значущий, біт. Періодом зсувного регістру є довжина одержуваної послідовності до початку її повторення.

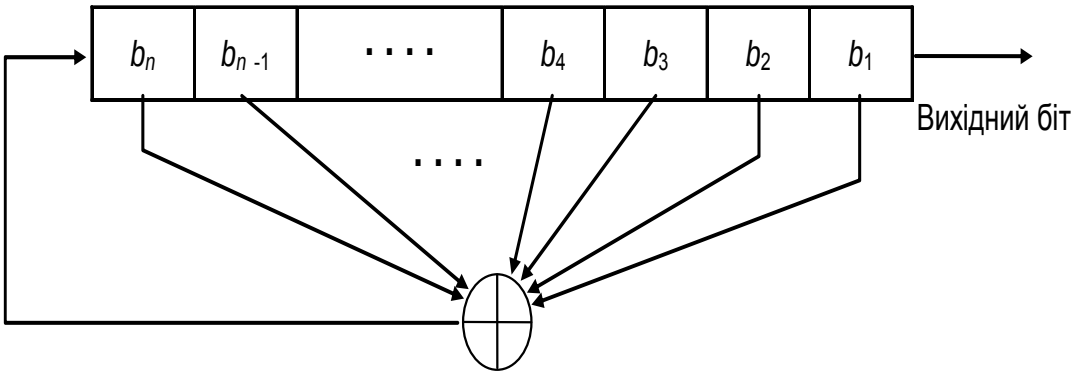


Рисунок 3.1-Регістр зсуву з лінійно-зворотнім зв'язком

Регістр зсуву, представлений на рисунок 2.19 знаходитися в одному з 2^n-1 внутрішніх станів. Даний регістр може генерувати псевдовипадкову послідовність з періодом *2n-1* бітів. Для того, щоб регістр зсуву мав максимальний період, многочлен, утворений з відвідної послідовності і константи 1, повинен бути примітивним за модулем 2. Ступінь многочлена є довжиною зсувного регістру. Примітивний багаточлен ступеня n – це незвідний многочлен, який є дільником $x^{2^{n-1}}+1$ [37].

У загальному випадку не існує простого способу генерувати примітивні многочлени даних за модулем 2. Найпростіше вибирати багаточлен випадковим чином і перевіряти, чи є він примітивним, що виконується перевіркою, чи є простим випадково вибране число, метод перевірки наведено у [38]. Незвідні примітивні поліноми різних ступенів за модулем 2 [39]. Одним з таких поліномів є запис (32, 7, 5, 3, 2, 1, 0) означає, що наступний многочлен примітивний за модулем 2:

$$G=x^{32}+X^7+X^5+x^3+x^2+X+1, \qquad (3.1)$$

останнє число завжди дорівнює 0, і його можна опустити. Всі числа, за винятком 0, задають відвідну послідовність, відраховану від лівого краю зсувного регістру. Тобто, члени многочлена з меншим ступенем відповідають позиціям, ближче до правого краю регістра. Продовжуючи приклад, запис (32, 7, 5, 3, 2, 1, 0) означає, що для взятого 32-бітового зсувного регістру новий біт генерується за допомогою XOR 32-го, сьомого, п'ятого, третього, другого і першого бітів, згідно рисунок3.2.

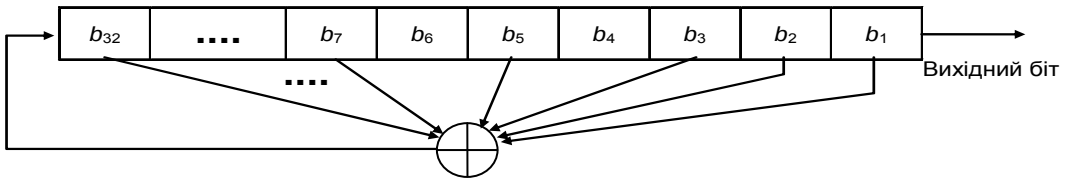


Рисунок 3.2- 32-бітовий регістр із зворотнім зв’язком

Схему зворотного зв’язку у регістрі можна модифікувати. Модифікований генератор (рисунок3.3) буде володіти максимальним періодом і набуває простої програмної реалізації [38]. Використання для генерації нового крайнього лівого біта відвідної послідовності виконується логічним XOR для кожного біта. З виходу генератора при заміні його значення операцією XOR, формується новий крайній лівий біт.

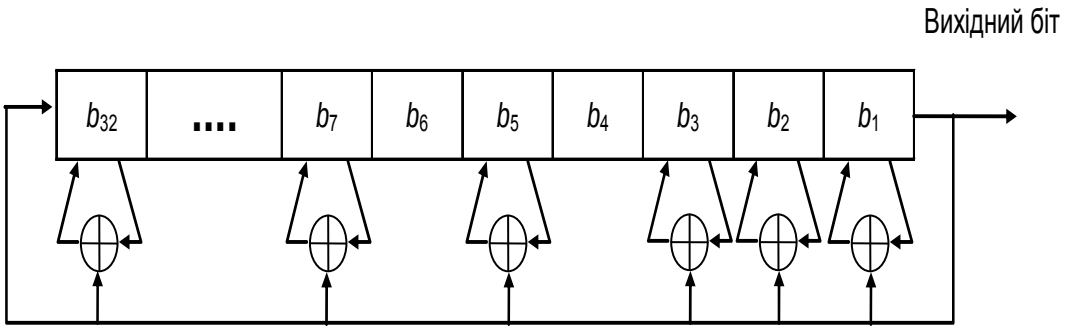


Рисунок 3.3-Модифікований регістр зі зворотнім зв’язком

Виграш полягає в тому, що всі XOR можна зробити за одну операцію. Така конфігурація Галуа дає виграш при апаратній реалізації, особливо у вигляді великих інтегральних схем.

Основний підхід при проектуванні генераторів потоку кодових послідовностей на базі регістра зі зворотнім зв’язком наступний:

- використовується один або декілька регістрів зі зворотніми зв’язками з різними довжинами і різними многочленами. Якщо довжини взаємно прості, а всі многочлени зворотного зв’язку примітивні, то у утвореного генератора буде максимальна довжина;
- незвідний поліном є початковим станом регістрів. Коли необхідно згенерувати новий біт, значення регістра посувається на одну позицію і відбувається тактування регістрів;

- біт виходу являє собою нелінійну функцію деяких бітів регістрів зсуву.

Для ускладнення у генераторах кодових послідовностей Галуа для різних регістрів зсуву використовується різна тактова частота, іноді частота одного генератора залежить від виходу іншого. Управління тактовою частотою може бути з прямим зв'язком, коли вихід одного регістра зсуву управляє тактовою частотою іншого регістра, або зі зворотним зв'язком, коли вихід одного регістра управляється власною тактовою частотою [38].

Розглянемо декілька модифікацій генераторів псевдовипадкових послідовностей Галуа з багатьма зворотними регістрами зсуву (ЗРЗ).

У генераторі Геффена [38] використовується три ЗРЗ, об'єднані нелінійним чином (рисунок3.4). Два ЗРЗ є входами мультиплексора, а третій ЗРЗ управляє виходом мультиплексора. Якщо a_1, a_2 і a_3 – виходи трьох ЗРЗ, вихід генератора Геффена можна описати як:

$$b = (a_1 \wedge a_2) \oplus (\overline{a_1}) \wedge a_3), \tag{3.2}$$

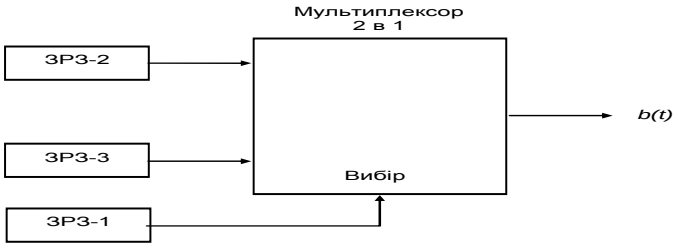


Рисунок 3.4-Генератор Геффена

Якщо довжини ЗРЗ дорівнюють n_1, n_2 і n_3, відповідно, то лінійна складність генератора дорівнює:

$$T=(n_1+1)n_2+n_1n_3 \tag{3.3}$$

Період генератора дорівнює найменшому спільному дільнику періодів трьох ЗРЗ. За умови, що модулі трьох примітивних многочленів зворотного зв'язку взаємно прості, період цього генератора буде дорівнювати добутку періодів трьох ЗРЗ.

У схемі генератора Дженнінгса [38] мультиплексор використовується для об'єднання двох ЗРЗ.

Мультиплексор керований ЗРЗ-l вибирає один біт ЗРЗ-2 в якості чергового вихідного біта, крім того використовується функція, яка відображає вихід ЗРЗ-2 на вхід мультиплексора (рисунок 3.5). Ключем є початковий стан двох ЗРЗ і функції відображення.

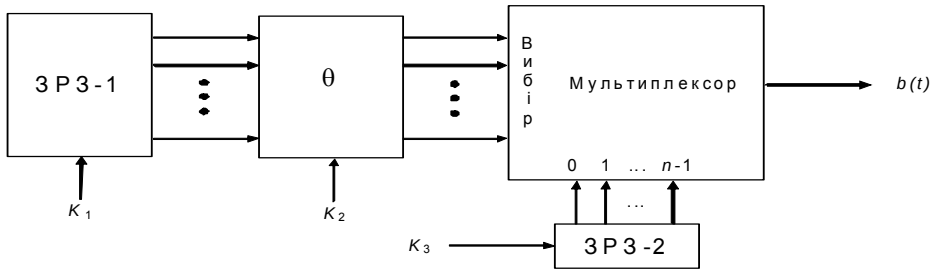


Рисунок 3.5-Генератор Дженнінгса

Генератор «стоп пішов», представлений на рисунок3.6 використовує вихід одного ЗРЗ для управління тактовою частотою іншого ЗРЗ [38]. Тактовий вхід ЗРЗ-2 управляється виходом ЗРЗ-l, тоді ЗРЗ-2 може змінювати свій стан у момент часу t тільки, якщо вихід ЗРЗ-l в момент часу t дорвінює 1.

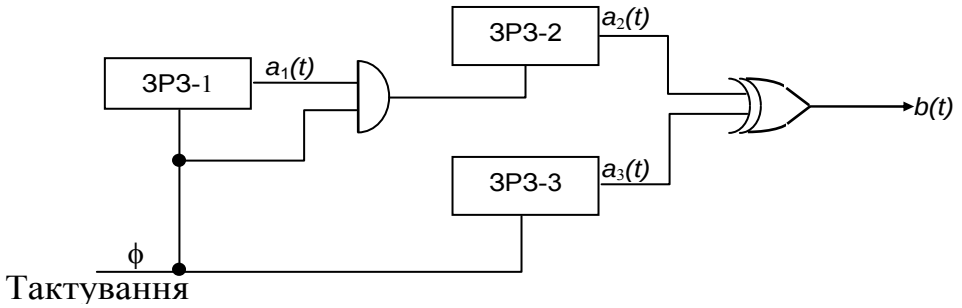


Рисунок 3.6- Генератор «стоп пішов»

У пороговому генераторі (рисунок3.7). для формування кодових послідовностей використовується *n* кількість ЗРЗ [38]. Якщо більше половини вихідних бітів ЗРЗ рівні 1, то виходом генератора є 1. Якщо більше половини вихідних бітів ЗРЗ рівна 0, то виходом генератора є 0

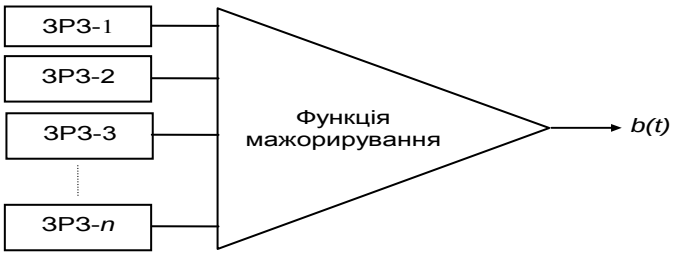


Рисунок 3.7-Пороговий генератор

Для трьох ЗРЗ вихід генератора можна представити як:

$$b = (a_1 \wedge a_2) \oplus (a_1 \wedge a_3) \oplus (a_2 \wedge a_3) \quad (3.4)$$

Пороговий генератор володіє лінійної складністю:

$$T=n_1n_2 + n_1n_3 + n_2n_3 \quad (1.5)$$

де n_1, n_2 і n_3 – довжини першого, другого і третього ЗРЗ.

Каскад Голлманна (рисунок3.8), описаний в [38], являє собою посилену версію генератора «стоп-пішов». Він складається з послідовності ЗРЗ, тактування кожного з яких управляється попереднім ЗРЗ. Якщо виходом ЗРЗ-l в момент часу t є 1, то тактується ЗРЗ-2. Якщо виходом ЗРЗ-2 в момент часу t є 1, то тактується ЗРЗ-3 і так далі. Вихід останнього ЗРЗ і є виходом генератора. Якщо довжина всіх ЗРЗ однакова і дорівнює n, лінійна складність системи з *k ЗРЗ* дорівнює $n(2^n - 1)^{k-1}$.

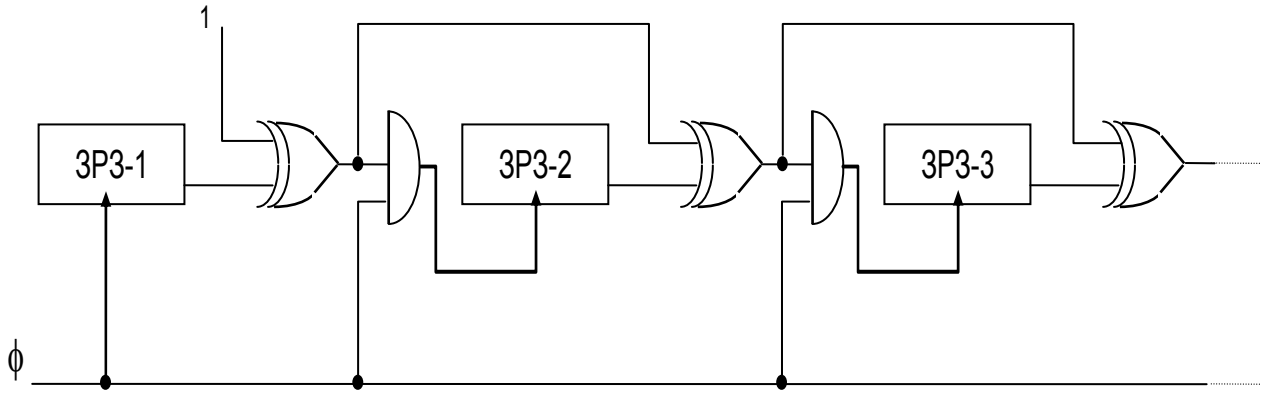


Рисунок-3.8-Каскад Голлманна

Концептуально каскад Голлманна може бути використаний для генерації послідовностей з величезними періодами, динамічними та статистичними властивостями.

Досліджені генератори кодових послідовностей Галуа використовуються у задачах опрацювання інформаційних потоків різної довжини та складності.

У алгоритмі передаються не 64-разрядні слова стану регістру, а 32-розрядні блоки, цілісна вихідна послідовність завдовжки більше 2*n* біт тут недоступна.

Шифратори HCS200, HCS201 і дешифратори HCS515 Microchip є типовими спеціалізованими мікросхемами у системах дистанційного управління, зокрема у автомобільних системах проти викрадення.

Шифратори (наприклад, HCS201) дуже компактні і щоб виготовити на їх базі брелоки потрібні мікросхема передавача і мінімум зовнішніх компонентів.

В процесі натискання будь-якої з кнопок передається динамічний код і статус натиснутої кнопки, приймач виконує команду відповідну цій кнопці. За умови одночасного натискання всіх кнопок передається замість динамічного коду 32-розрядне слово (seed) для генерації в приймачі секретного ключа. Це один з варіантів реалізації процедури реєстрації брелока в приймачі.

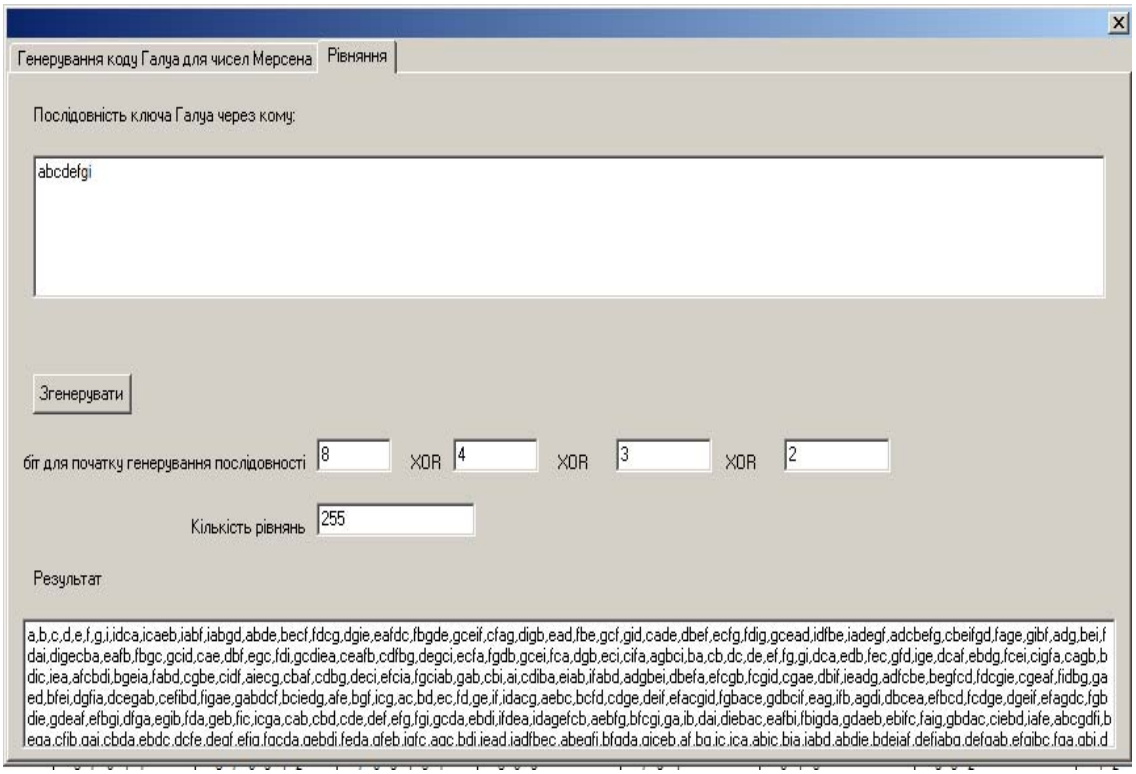


Рисунок 3.9- Програмна реалізації генератора крипто захищених повідомлень для авто сигналізації

На основі досліджених генераторів криптографічних кодових послідовностей для автосигналізації була розроблена програма, що генерує багато розрядні значення. Для автомобільних сигналізації необхідна довжина кодової послідовності складає 128 біт. Пристрій передачі коду працює у

робочому діапазоні від 400МГц до 950МГц. Високий рівень інтеграції і гнучкість конфігурація забезпечує можливість застосування генератора у різних засобах передавання захищених повідомлень на основі незвідних поліномів. Двосторонній обмін дозволяє використовувати прилад для захищеної передачі інформації з перевіркою і підтвердженням її правильності.

3.2. Розрахунок параметрів датчиків автоматизованої автомобільної сигналізації

Датчик тиску реалізований на основі ємнісного датчика (конденсатор), одна обкладка (пластина) якого нерухома, а інший переміщається під вплив зовнішньої сили.

Для дослідження параметрів датчика тиску необхідно здійснити наступні

розрахунки:

- розрахувати граничні значення ємності датчика тиску і побудувати графік залежності ємності від відстані між обкладинками (пластини) (вважати, що ε = 100);

- побудувати графік залежності опору датчика тиску від частоти електричного сигналу для середньої місткості;

- вибрати оптимальну робочу частоту ($f_{опт}$) датчика;

- розрахувати і побудувати графік падіння напруги на датчику, який включений в електричному вимірювальному ланцюзі у всьому діапазоні зміни ємності датчика. Вимірювальний ланцюг живиться від генератора синусоїдального сигналу.

Вихідні дані:

– площа обкладок пластин, $S = 31 \cdot 10^{6}$ м^2;

– відстані між обкладками конденсатора, $d_{\min} = 1{,}06 \cdot 10^{-3}$ м, $d_{\max} = 5 \cdot 10^{-3}$ м;

− напруга, $U_{\max} = 22$ В;

− характеристика середовища, $\xi = 100$;

− діалектрична константа, $\xi_0 = 8{,}85 \cdot 10^{-12}$;

Граничні значення ємність визначає за формулами 1 і 2.

$$C_{\min} = \frac{\xi \cdot \xi_0 \cdot S}{d_{\max}}, \tag{3.1}$$

$$C_{\max} = \frac{\xi \cdot \xi_0 \cdot S}{d_{\min}}; \tag{3.2}$$

$$\tilde{N}_{\min} = \frac{100 \cdot 8{,}85 \cdot 10^{12} \cdot 31 \cdot 10^{6}}{5 \cdot 10^{3}} = 5{,}49 \cdot 10^{-12} \text{ Ф},$$

$$\tilde{N}_{\max} = \frac{100 \cdot 8{,}85 \cdot 10^{-12} \cdot 31 \cdot 10^{-6}}{1{,}06 \cdot 10^{-3}} = 2{,}59 \cdot 10^{-11} \text{ Ф}.$$

На рисунок3.10 представлений графік залежності ємності від відстані між обкладинками конденсатора $C(d) = \frac{\xi \cdot \xi_0 \cdot S}{d}$.

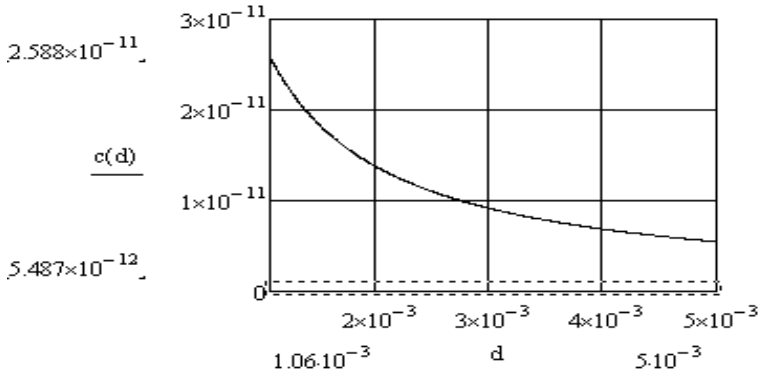


Рисунок 3.10- Графік залежності ємності від відстані між обкладинками конденсатора

Середня відстань між обкладинками конденсатора визначаємо по формулі (3.3):

$$d_{\text{ср.}} = \frac{d_{\max} - d_{\min}}{2}, \tag{3.3}$$

$$d_{ср.} = \frac{5 \cdot 10^{-3} - 1{,}06 \cdot 10^{-3}}{2} = 1{,}97 \cdot 10^{-3}\, m.$$

Середня ємність визначається по формулі (3.4):

$$C_{ср.} = \frac{\xi \cdot \xi_0 \cdot S}{d_{ср.}} \tag{3.4}$$

$$C_{ср.} = \frac{100 \cdot 8{,}85 \cdot 10^{-12} \cdot 31 \cdot 10^{-6}}{1{,}97 \cdot 10^{-3}} = 1{,}393 \cdot 10^{-5}\,Ф.$$

Опір конденсатора розраховується з формули (3.5):

$$r_C = \frac{1}{2 \cdot \pi \cdot f \cdot C}. \tag{3.5}$$

де f – частота електричного сигнала, Гц.

На рисунку 3.11 представлений графік залежності опору конденсатора від частоти електричного сигналу:

$$r_C(f) = \frac{1}{2 \cdot \pi \cdot f \cdot C_{ср.}}.$$

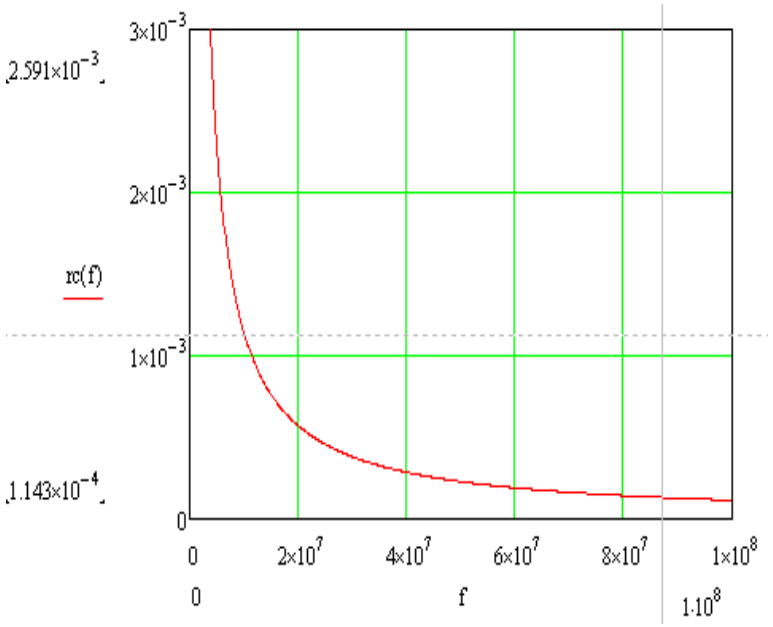


Рисунок 3.11 - Графік залежності опору конденсатора від частоти електричного сигналу

Вибір оптимальної частоти $f_{опт}$ зводиться до знаходження дотичної до графіка, представленого на рисунок 3.11, яка має нахил 45 °.Звідси згідно графіка $f_{îò} = 2{,}2 \cdot 10^7$ Гц при $r_C = 5 \cdot 10^{-4}$ Ом.

Схема включення в ланцюг датчика тиску представлена на рисуноку 3.12.

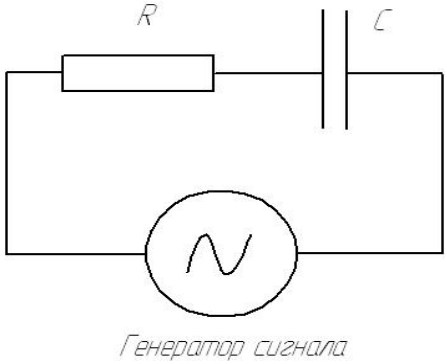


Рисунок 3.12- Схема включення в ланцюг датчика тиску

Генератор сигналів працює на оптимальній частоті. Сигнал від нього має форму. $U(t) = U_{\max} \sin(2\pi f_{опт} t)$ Опір R вибирається з умови $R = Rc$, де Rc розраховується для $d_{сра}$ на $f_{опт}$. Чинне значення напруги для синусоїдального сигналу не залежить від частоти і розраховується по формулі (3.6):

$$U_d = \frac{U_{max}}{\sqrt{2}}, \tag{3.6}$$

$U_d = \frac{22}{\sqrt{2}} = 15{,}556 B$.

Напруга у датчику визначається по формулі (3.7):

$$U_{Cd} = \frac{U_d \cdot r_c}{(R + r_c)} \tag{3.7}$$

Залежно від відстані між обкладинками конденсатора формула (3.7) набуде вигляду (3.8):

$$U_{Cd}(d) = \frac{U_d \cdot r_c(d)}{(R + r_c(d))} \tag{3.8}$$

де

$$r_c(d) = \left| \frac{1}{2 \cdot \pi \cdot f_{опт.} \cdot c(d)} \right|.$$

Графік падіння напруги на датчику в межах д [$d_{мін}$; $d_{макс}$] представлені на рисунку 3.13.

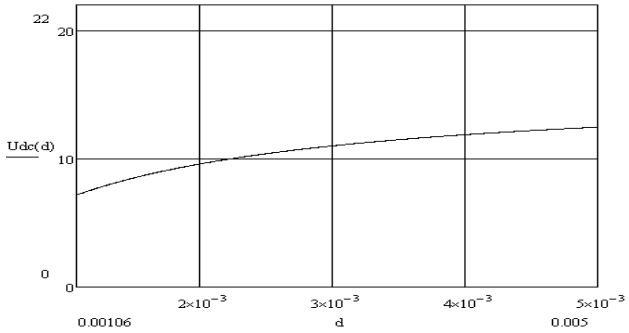


Рисунок 3.13- Графік падіння напруги на датчику

Отже, розрахунок параметрів датчиків дозволить покращити технічні характеристики для взаємодії центральним блоком управління автомобільної сигналізації та зможе покращити її параметри та властивості.

3.3Розробка структури системи управління автосигналізацією та розрахунок її параметрів

Розробка структури системи автомобільної сигналізації полягає у виборі серед типових алгоритмів управління такий, що забезпечить потрібну якість процесу регулювання відносно обраного критерію управління.

В якості закону регулювання використаємо ПІ – закон. В ідеальному випадку даний закон забезпечує достатню якість і час регулювання та відсутність статичної похибки, але в реальних системах в яких присутня зона нечутливості, присутня також і статична похибка. Допустимі межі цієї похибки становлять ±0,5 від діапазону вимірювання параметра.

Для вимірювання температури використаємо датчик, аналогом якого є аперіодична ланка першого порядку з Т = 100 с і К=1. Всі пристрої для вимірювання та регулювання мають поріг нечутливості, який становить не більше 0,1 діапазонна вимірювання, тому необхідно ввести в модель зону нечутливості регулятора (тобто ланку нечутливості) з параметрами ± 0,1. Оскільки в реальних системах є обмеження на управляючу дію, то вводимо також ланку насичення, параметри якої розраховуємо із співвідношення:

Для витрати гріючої пари у 1-у зону:

0,136 – 60% 0,136 – 60%

х – 100%, звідси х=0,23 кг/с у – 5%, звідси у=0,0113 кг/с

отже параметри будуть: 0,23–0,136=+0,094 та 0,011–0,136=-0,1247

Аналогічно розраховуємо параметри для витрати датчика спрацювання у другу зону:

0,091 – 60% 0,091 – 60%

х – 100%, х=0,15 кг/с у – 5%, у=0,0076 кг/с

0,15–0,091=+0,059 та 0,0076–0,091=-0,0834

Для розрахунку оптимальних настройок регулятора використаємо метод Циглера-Нікольса. Цей метод полягає у відключенні І – складової та виведення системи на межу стійкості (поступовим збільшенням kp до моменту появи в системі явно виражених незатухаючих коливань). Далі фіксуємо значення коефіцієнта передачі $\mathrm{kp}_{\mathrm{кр}}$, при якому виникли незатухаючі коливання, та період цих коливань $\mathrm{T}_{\mathrm{кр}}$, далі оптимальні настройки регулятора визначаються за формулами (3.9) та (3.10).

$$kp_{опт} = 0{,}45 kp_{кр} \tag{3.9}$$

$$Ti_{опт} = 1{,}25 T_{кр} \tag{3.10}$$

Для першого контуру регулювання $\Delta \mathrm{t}_1$:

$\mathrm{kp1}_{\mathrm{кр}} = 2 \ \frac{\text{кг/с}}{{}^0\mathrm{C}}$; $\mathrm{T1}_{\mathrm{кр}} = 230$ с.

$kp1_{опт} = 0{,}45 \cdot 2 = 0{,}9 \ \frac{\text{кг/с}}{{}^0\mathrm{C}}$

$Ti1_{опт} = 1{,}25 \cdot 230 = 287{,}5$ с

Для другого контуру регулювання Δt2:

$\mathrm{kp2}_{\mathrm{кр}} = 2{,}8 \ \frac{\text{кг/с}}{{}^0\mathrm{C}}$; $\mathrm{T2}_{\mathrm{кр}} = 150$ с

$kp2_{опт} = 0{,}45 \cdot 2{,}8 = 1{,}3 \ \frac{\text{кг/с}}{{}^0\mathrm{C}}$

$Ti2_{опт} = 1{,}25 \cdot 150 = 187{,}5$ с

Перехідні процеси з оптимальними настройками регуляторів та ±20% від оптимальних настройок зображенні на рисунках 3.14-3.19.

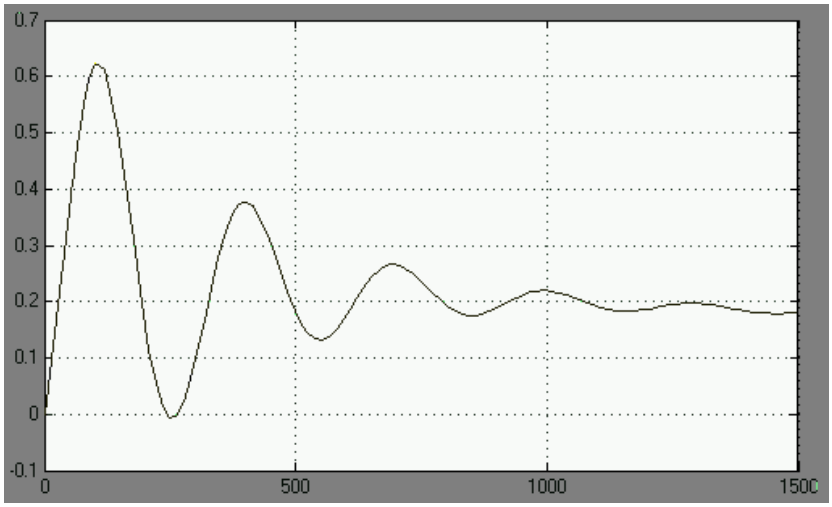


Рисунок 3.14 - Перехідний процес в одноконтурній САР з ПІ-регулятором по каналу Δt_1

Оптимальні налаштування регулятора $kp1_{опт} = 0.9 \ \frac{кг/с}{^0C}$, $Ti1_{опт} = 287{,}5 \ с$, $I1=77{,}32 \ ^0C^2 \cdot с$

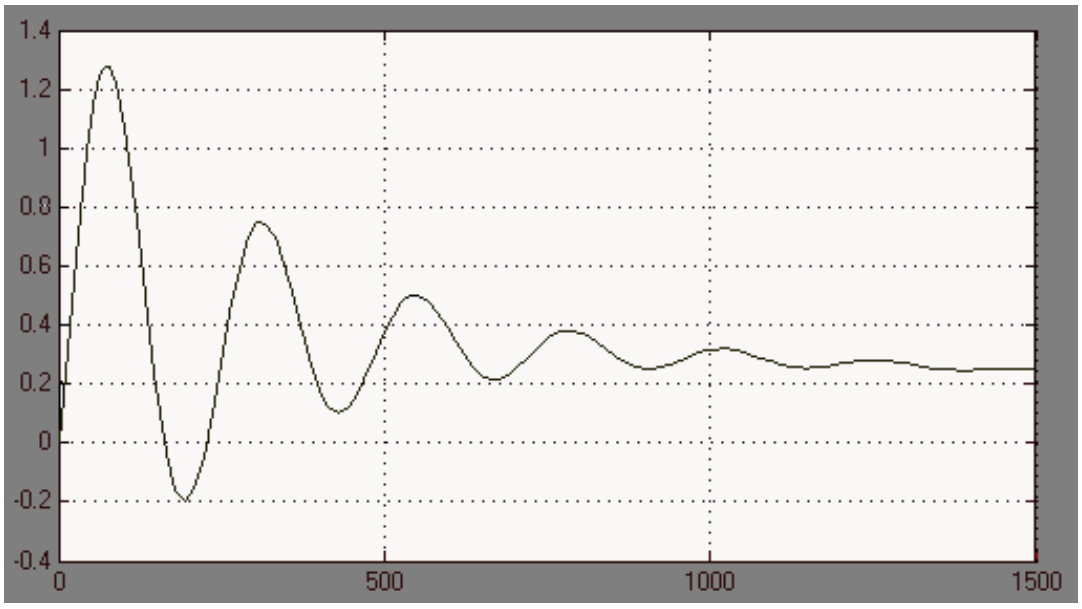


Рисунок 3.15 - Перехідний процес в одноконтурній САР з ПІ-регулятором по каналу Δt_2

Оптимальні налаштування регулятора $kp2_{опт} = 1{,}3 \ \frac{кг/с}{^0C}$, $Ti2_{опт} = 187{,}5 \ с$, $I2=231 \ ^0C^2 \cdot с$

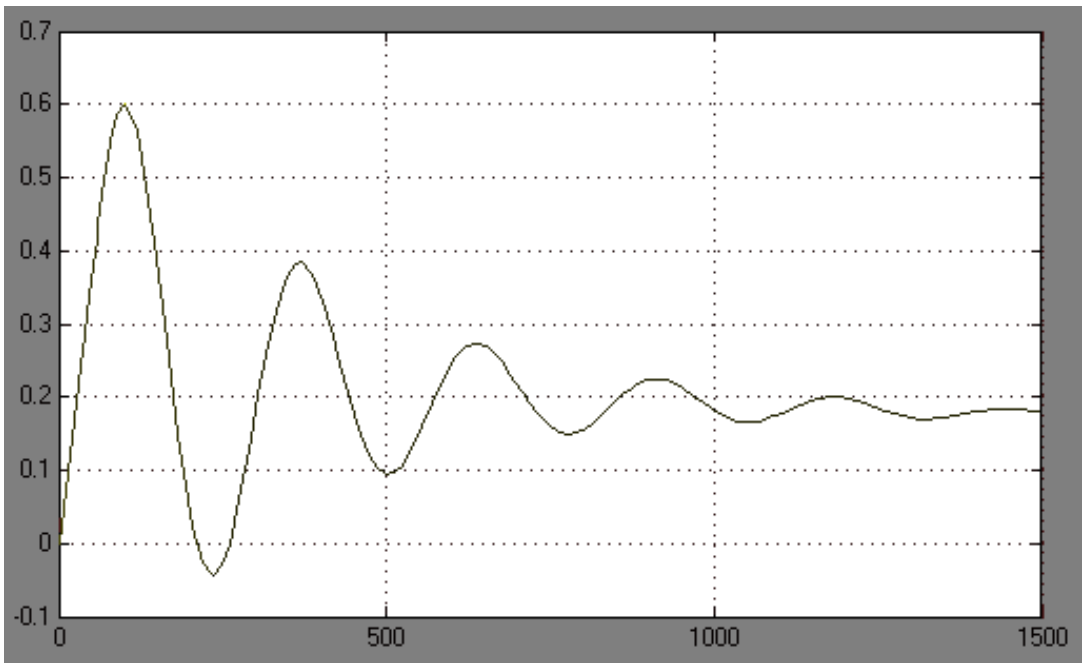


Рисунок 3.16 - Перехідний процес в одноконтурній САР з ПІ-регулятором по каналу Δt_1

Налаштування регулятора +20% $kp1 = 1{,}08 \ \frac{кг/с}{^0C}$, $Ti1 = 345\,с$, $I1=85{,}19\,^0C^2 \cdot с$

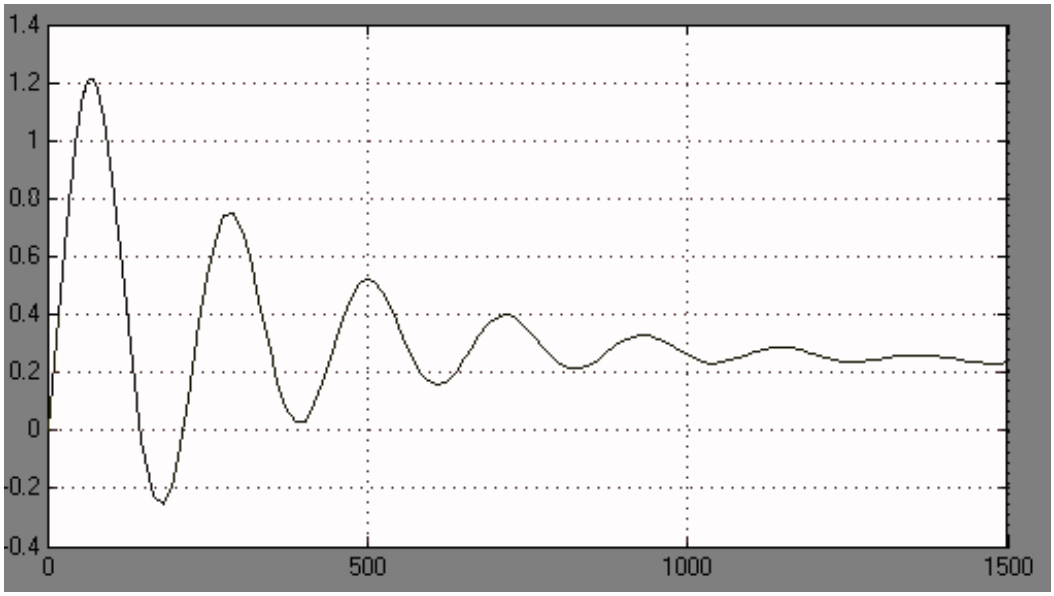


Рисунок 3.17 - Перехідний процес в одноконтурній САР з ПІ-регулятором по каналу Δt_2

Налаштування регулятора +20% $kp2 = 1{,}56 \ \frac{кг/с}{^0C}$, $Ti2 = 225\,с$, $I2=233{,}8\,^0C^2 \cdot с$

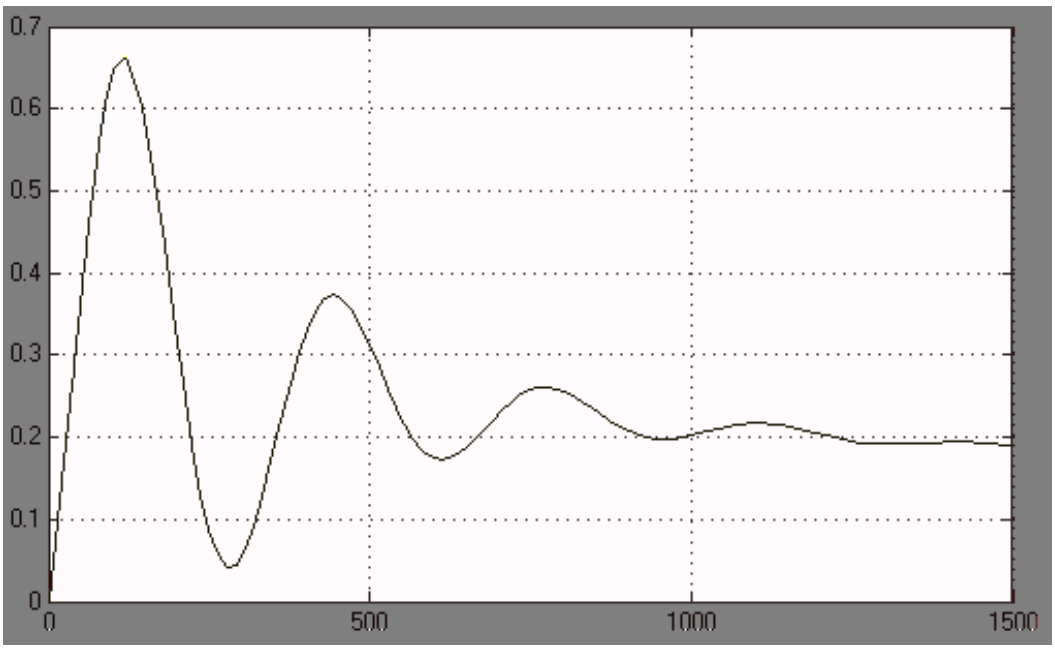


Рисунок 3.18 - Перехідний процес в одноконтурній САР з ПІ-регулятором по каналу Δt_1

Налаштування регулятора -20% $kp1 = 0{,}72 \ \frac{кг/с}{^0C}$, $Ti1 = 230\,с$, I1=$112\,^0C^2 \cdot с$

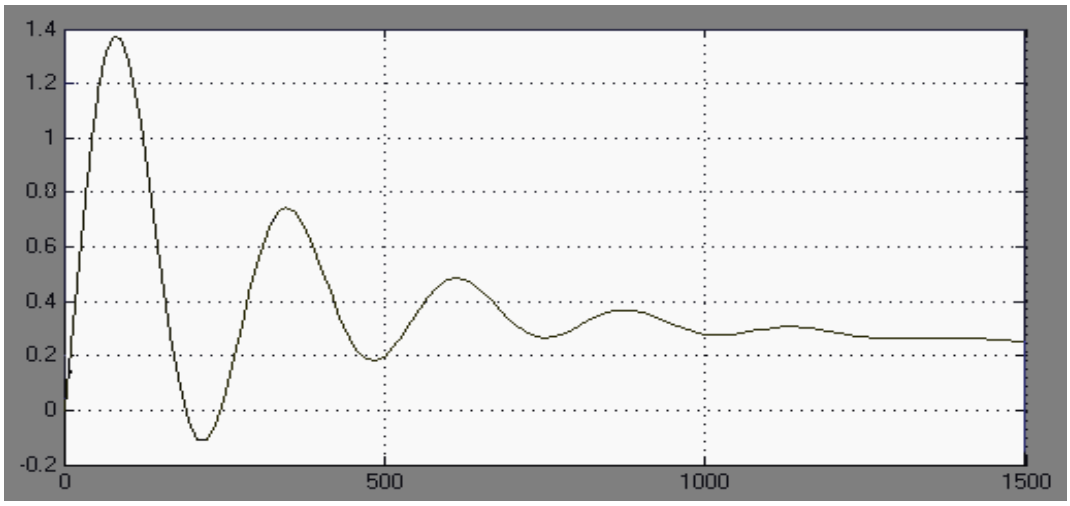


Рисунок 3.19 - Перехідний процес в одноконтурній САР з ПІ-регулятором по каналу Δt_2

Налаштування регулятора -20% $kp2 = 1{,}04 \ \frac{кг/с}{^0C}$, $Ti2 = 150\,с$, I2=$319{,}5\,^0C^2 \cdot с$

Наступним етапом розробки структури системи є перехід до моделювання багатоконтурної АСР, це робиться для зменшення динамічної та статичної похибок.

Оскільки автомобільна сигналізація є багатовимірним об’єктом (має кілька регульованих змінних та перехресні зв’язки), то об’єкт можна вважати багатозв’язаним. Для регулювання таких об’єктів використовують зв’язане регулювання із застосуванням автономних багатоконтурних систем. Такі системи дають можливість проводити незалежне регулювання взаємозалежних змінних. Вони мають у своєму складі додаткові динамічні компенсатори. Основою побудови цих систем є принцип автономності. На рисунку 3.20 зображена структурна схема системи автономного регулювання.

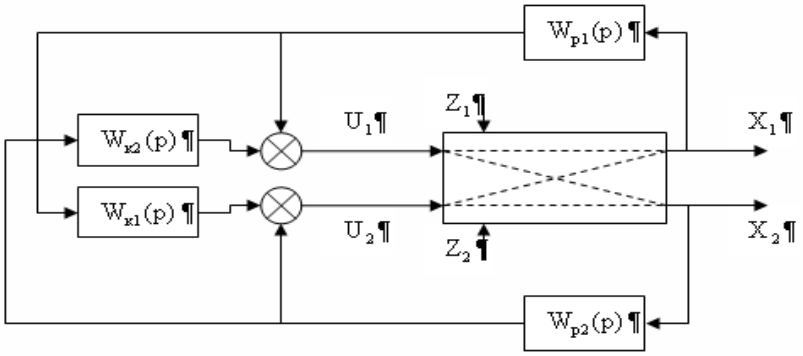


Рисунок 3.20 - Структурна схема автономної АСР

Передаточні функції зовнішніх динамічних компенсаторів визначаються через передаточні функції об’єкта:

$$W_{к1}(p)=\frac{W_{12}(p)}{W_{22}(p)};\qquad W_{к2}(p)=\frac{W_{21}(p)}{W_{11}(p)} \tag{3.7}$$

Тобто відношення передаточних функцій по перехресному та прямому каналах.

Розраховуємо передаточні функції об’єкта за прямими та перехресними каналами:

$$W_{11}(p)=\frac{271{,}32}{7{,}68p+1}\cdot\frac{0{,}32}{1670{,}4p+1}=\frac{86{,}82}{(7{,}68p+1)(1670{,}4p+1)}$$

$$W_{12}(p)=\frac{86{,}82}{(7{,}68p+1)(1670{,}4p+1)}\cdot\frac{0{,}431}{1670{,}4p+1}=\frac{37{,}42}{(7{,}68p+1)(1670{,}4p+1)^2}$$

$$W_{22}(p)=\frac{291{,}51}{4{,}23p+1}\cdot\frac{0{,}32}{1670{,}4p+1}=\frac{93{,}28}{(4{,}23p+1)(1670{,}4p+1)}$$

$$W_{21}(p)=\frac{93,28}{(4,23p+1)(1670,4p+1)}\cdot\frac{0,541}{1670,4p+1}=\frac{50,46}{(4,23p+1)(1670,4p+1)^2}$$

За формулами (3.7) знаходимо передаточні функції компенсаторів.

$$W_{к1}(p)=\frac{\frac{37,42}{(7,68p+1)(1670,4p+1)^2}}{\frac{93,28}{(4,23p+1)(1670,4p+1)}}=\frac{0,4(4,23p+1)}{(7,68p+1)(1670,4p+1)},$$

Даний компенсатор реалізується за допомогою послідовно з'єднаних аперіодичної ланки першого порядку та інтегрально-диференціювальної ланки.

$$W_{к2}(p)=\frac{\frac{50,46}{(4,23p+1)(1670,4p+1)^2}}{\frac{86,82}{(7,68p+1)(1670,4p+1)}}=\frac{0,58(7,68p+1)}{(4,23p+1)(1670,4p+1)},$$

Другий компенсатор фізично реалізується аналогічно першому – послідовним з'єднанням інтегрально-диференціювальної та аперіодичної ланок. Алгоритм роботи модельованоъ системи автоматизованого управлыння на основі автомобыльноі сигналізації розроблено у додатку А.

Перехідні процеси замкненої системи з компенсатором збражені на рисунках 3.21, 3.22.

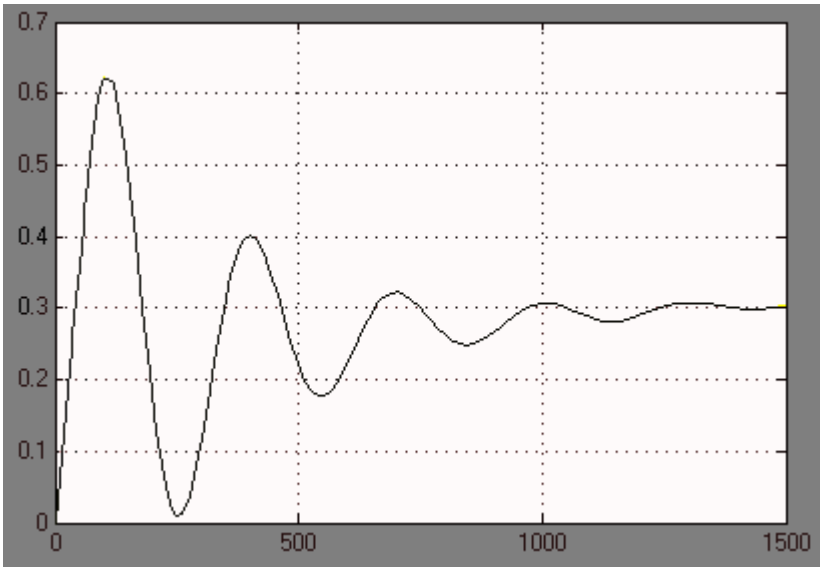


Рисунок 3.21 - Перехідний процес замкненої системи з компенсатором по каналу Δt_1, I1=140,1 $^0C^2\cdot c$

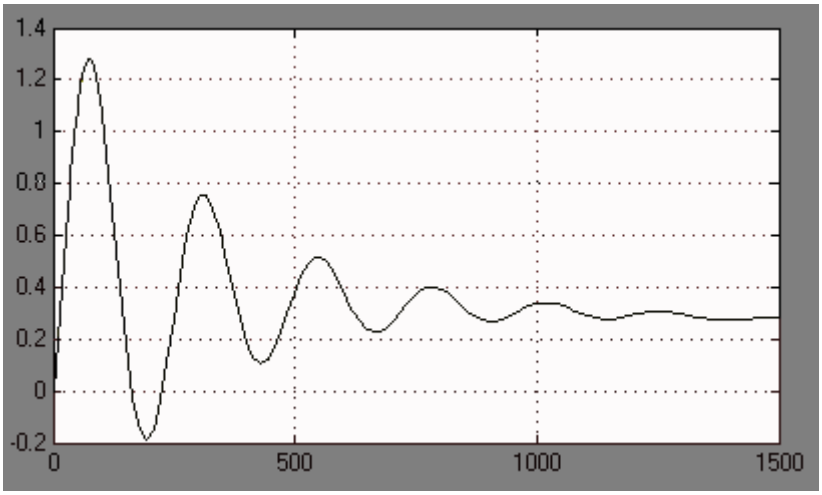


Рисунок 3.22 - Перехідний процес замкненої системи з компенсатором по каналу Δt_2, I2=281,4 $^0C^2 \cdot c$

Отже розроблена система автоматичного регулювання для автомобільної сигналізації дозволить краще освоїти взаємодію між компонентами та дослідити перехідні процеси, що відбуваються та критерії спрацьовування датчиків на основі ПІ-регулятора.

4. РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ ДЛЯ КОНТРОЛЮ ТЕХНОЛОГІЧНИХ ПАРАМЕТРІВ АВТОМОБІЛЬНОЇ GSM СИГНАЛІЗАЦІЇ

4.1 Математичні основи криптографічного захисту системи автосигналізації на основі кодів поля Галуа

Система захисту автомобіля від несанкціонованого доступу у переважній більшості базується на на динамічному чи стрибкоподібному коді (hopping code) система KeeLoq [27]. Ця система використовується в багатьох галузях та є однією з найпоширеніших апаратних рішень, що ґрунтується на регістрі зсуву з нелінійною функцією. Згадана функція є стандартною складовою, яка використовується в радіозв'язку та картах доступу як найменш уразлива для криптоаналітичних атак у порівнянні зі стандартною лінійною функцією в поєднанні з регістром зсуву. Інші системи, в яких застосовуються нелінійні функції, це – Achterbahn, Grain, Trivium, VEST.

Односторонні системи захисту автомобіля мають два істотні недоліки: код, який передається передавачем, загалом відомий і кількість комбінацій є відносно низькою. З цієї причини ці пристрої можуть бути уразливі щодо несанкціонованого доступу [27]. Тому надійною буде система, в якій вищезгадані недоліки усунуті. До такого рішення належить змінно-кодова система KeeLoq, в якій передбачена велика кількість можливих комбінацій коду [3, 4]. З метою безпеки також повинна виконуватися друга умова – система не може вдруге реагувати на цей самий трансльований код [21].

Односторонній зв'язок у рамках технології KeeLoq запропонував доктор наук Ф. Брувер з компанії Nanoteq Ltd., а систему шифрування розробив професором Ґ. Кун. У подальшому її реалізував у мікросхемі доктор наук В. Сміт з компанії Nanoteq Ltd. У середині 80-х років система KeeLoq набула стрімкого розвитку після купівлі ліцензії на нього компанії Microchip Technology Inc. Відтоді ця система набула великої популярності

завдяки своїй надійності, а також низькій вартості таких мікросхем, як NTQ105/106/115/125D/129D та HCS101/2XX/3XX/4XX/5XX. Їх застосовують у більшості безпровідних систем контролю доступу фірми Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, VW, Clifford, Shurlok, Jaguar.

Система моделювання безпечної комунікації у авто сигналізації на основі KeeLoq грунтується на двох пристроях – шифраторі HCS410 та дешифраторі HCS500 [6]. На рисунку 4.1 представлена плата, побудована на базі 16-бітного мікроконтролера PIC24FJ128 [7]. До інтерфейсів під'єднані схеми шифратора і дешифратора KeeLoq. Зазначений мікроконтролер моніторує їх через розміщену в своїй пам'яті програму.

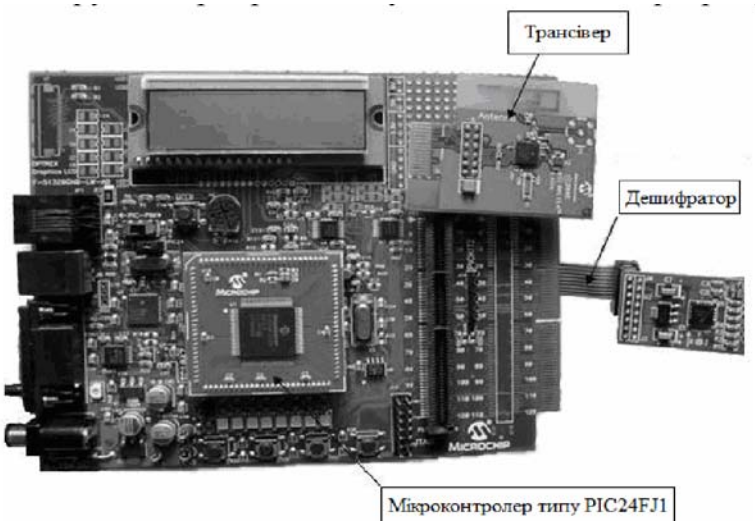


Рисунок 4.1 Система KeeLoq з дешифратором HCS500 на платі PIC24FJ128

Проте використання двійкового коду у системі KeeLoq має деякі функціональні обмеження накладенні його складною двійковою структурою формування. У порівнянні з двійковим кодуванням, застосування кодових систем Галуа забезпечує можливість вибору одного з безлічі кодових упорядкувань, згідно обраного вектора зворотних зв'язків та порядку векторного набору, що дозволяє обмежити несанкціонований доступ до повідомлень на рівні формування інформаційних потоків, а також зменшити інтенсивність інформаційного обміну в мережі внаслідок зменшення кількості необхідних бітів для кодування повідомлень у порівнянні з

відомими методами кодування [39]. Кодові системи Галуа дозволяють ефективно кодувати інформацію, вирішуючи ряд проблем, які виникають в типових системах [39-40], що визначило актуальність досліджень в напрямку використання рекурсивних методів кодування. Клас надлишкових завадодозахисних кодів (Галуа, деревовидних та арифметичних) породжується похідними вибірковими комбінованими базисами функцій і сьогодні набув широкого застосування при завадодозахищеному інформаційному обміні. Внаслідок того, що кодові системи Галуа в загальній класифікації володіють широким спектром математичних властивостей, це дозволило класифікувати їх, в одному з випадків, до блокових систематичних поліноміальних циклічних кодів, а в іншому – до безперервних кодів у залежності від специфіки розв'язуваної задачі, обраної кодової системи і планованих властивостей кодів, на використанні яких досягається перевага в порівнянні з іншими методами кодування [40]. Основною характеристикою кодових систем Галуа є рекурсивна упаковка кодових елементів і повна кореляційна залежність елементів послідовності [41], що дозволяє перейти від паралельного формату представлення розрядів чисел, як у традиційних системах числення (паралельна інфотехнологія), до вертикального з послідовним рекурсивним біт-орієнтованим формуванням кожного з повідомлень (вертикальна інфотехнологія) за умови накопичення n попередніх кодових елементів, де n = *logpN*, *N* – модуль перерахунку системи. У результаті рекурсивної залежності кодових елементів, системи кодування Галуа володіють унікальною властивістю – на періоді $N = pn$, або $N = pn - 1$ всі елементи розташовуються таким чином, що довільний *n*-розрядний фрагмент (кодон) з рекурсивно породженої послідовності Галуа не повторюється на інтервалі періоду [38]. Таким чином, рекурсивні кодові послідовності Галуа представляються, як рекурсивно вкладені *n*-розрядні *p*-ічні коди (кодони) на періоді $N = pn$. При кодуванні Галуа повідомлення ототожнюються з поліномами, а сама процедура кодування полягає у множенні вектора повідомлення на фіксований поліном.

З метою оцінки ефективності кодування даних на основі різних ТЧБ доцільно провести аналіз кодових матриць, які породжують різні системи числення.

При цьому важливою характеристикою кожного базису є об'єм його кодової матриці M_j та число активних елементів m_j, що визначає характеристики надлишковості представлення інформації на основі аналітичної оцінки [73]:

$$V = n \cdot N \,, \tag{4.1}$$

де n – розрядність числа;

N - число незалежних кодових значень.

Швидкість передавання кодової матриці визначається за формулою:

$$C = \frac{1}{T \cdot n}, \tag{4.2}$$

де Т- час передавання одного біту.

Оцінка ефективності кодових базисів проводиться за виразом:

$$\mathrm{K}_{\text{ефект}} = \frac{\mathrm{N}}{\mathrm{V}}, \tag{4.3}$$

де $\mathrm{K}_{\text{ефект}}$ – коефіцієнт ефективності кодових базисів;

N – кількість кодових комбінацій, V – об'єм кодової матриці.

Результат порівняння кодових базисів представлено графіком (рисунок 4.2).

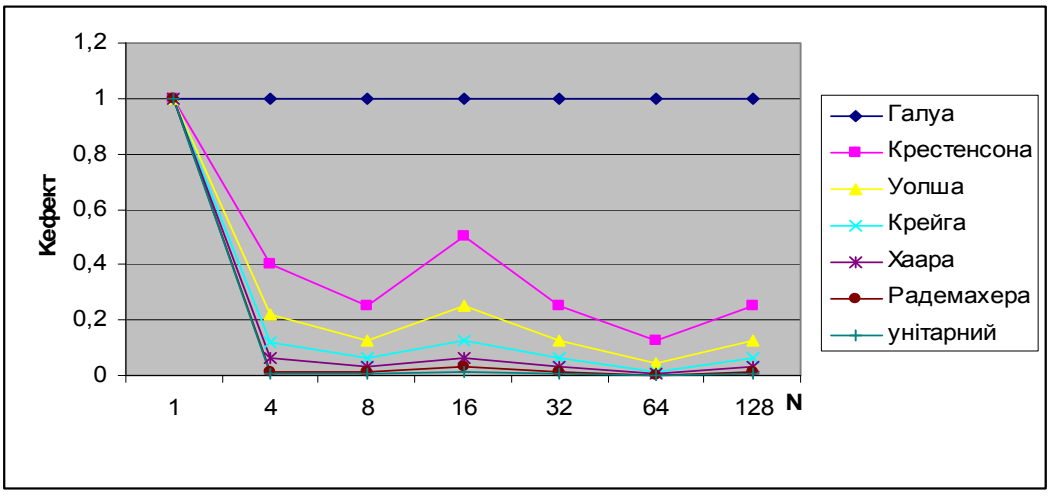


Рисунок 4.2- Коефіцієнт ефективності дискретних кодових базисів

Аналіз графіків, наведених на рисунку 4.3, показує, що найбільш компактним і ефективним для кодування і представлення даних є теоретико-числовий базис Галуа, оскільки він має коефіцієнт ефективності $К_{ефект}$=1.

Головною особливістю представлення даних в базисі Галуа є рекурентність [42, 70, 74,]. Суть рекурентності полягає в максимальній упаковці біт- орієнтованої послідовності кодового ключа

$$X_{i+1} = \sum_{i=1}^{n} (X_i \oplus X_{i-j}), \tag{4.4}$$

де $\oplus$ - символ додавання по mod2;

n – число пар елементів кодового ключа.

Коди поля Галуа [2] за загальною класифікацією відносяться до підкласу циклічних блокових кодів, які володіють всіма основними властивостями завадозахищених кодів. В блокових кодах послідовність елементарних повідомлень розбивається на блоки символів (B1, B2, B3, …, Bn) фіксованої довжини К, кожному з яких ставиться у відповідності певна комбінація символів кодового слова (b1, b2, b3, …, bn). Циклічні коди Галуа відносяться до класу систематичних кодів. Для останніх можна записати відповідний їм аналітичний вираз у вигляді логічного співвідношення, яке визначається правилами створення цих кодів. Найбільш зручною формою представлення циклічних кодів є використання алгебраїчного виразу [42]

$$G(x) = a_{n-1} \times x^{n-1} + a_{n-2} \times x^{n-2} + \ldots + a_1 \times x + a_0,$$

де a_0 – a_{n-1} – числа, що дорівнюють «0» чи «1», які визначають відповідні значення розрядів кодових комбінацій.

Таким чином, дія над циклічними кодами зводиться до дії над відповідними математичними виразами. Коефіцієнти однакових степенів додаються за модулем 2.

Повна система залишків по модулю простого числа p утворює кінцеве поле порядку p, яке позначається через $GF(p)$ і називається простим полем

Галуа [42]. Кінцеві поля $GF(p^r)$ порядку $\binom{r}{p}$ утворюються з допомогою незвідних поліномів [19], представлених у табл. 4.1. При використанні незвідних поліномів $\pi(x)$ просте поле $GF(p)$ можна розширити до поля $GF(p^r)$ за рахунок приєднання кореня a поліному $\pi(x)$, тобто з допомогою порівняння по двох модулях p і $\pi(x)$. У табл. 4.1 представлені примітивні незвідні поліноми $\pi(x)$ характеристики, з коефіцієнтами із простого поля $GF(2)$, а також поліноми характеристик 3, 5, 7 малих степенів з мінімальним числом ненульових коефіцієнтів. З математичної точки зору, вибір полінома несуттєвий, так як всі кінцеві поля одного і того ж порядку ізоморфні, але вибір поліному суттєвий з точки зору апаратної реалізації.

Якщо елемент $\alpha \in GF(2^r)$ представляє собою корінь незвідного двійкового тричлена степеня r, то перші r степенів елемента α представляють собою ефективний базис для запису поля $GF(2^r)$, так як множення на α може бути виконано з допомогою r – розрядного регістра, в зворотній зв'язок якого входить один суматор з двома входами.

Таблиця 4.1. – Незвідні поліноми $\pi(x) = x^r + f(x)$

p	r	$\pi(x)\,;\ \left[x^r = f(x)\right]$	p	r	$\pi(x)\,;\ \left[x^r = f(x)\right]$
	2	$x^2 + x + 1$		17	$x^{17} + x^3 + 1$
	3	$x^3 + x + 1\,; x^3 + x^2 + 1$		18	$x^{18} + x^7 + 1$
	4	$x^4 + x + 1$		19	$x^{19} + x^5 + x^2 + x + 1$
	5	$x^5 + x^2 + 1$	2	20	$x^{20} + x^3 + 1$
	6	$x^6 + x + 1$		21	$x^{21} + x^2 + 1$
	7	$x^7 + x + 1\,; x^7 + x^3 + 1$		22	$x^{22} + x + 1$

Продовження таблиці 4.1

	8	$x^8+x^4+x^3+x^2+1$		23	$x^{23}+x^5+1$
	9	x^9+x^4+1		24	$x^{24}+x^7+x^2+x+1$
	10	$x^{10}+x^3+1$		25	$x^{25}+x^3+1$
	11	$x^{11}+x^2+1$		26	$x^{26}+x^6+x^2+x+1$
	12	$x^{12}+x^6+x^4+x+1$	3	2	$x^2+x+2;\ \left[x^2=2\cdot x+1\right]$
	13	$x^{13}+x^4+x^3+x+1$		3	$x^3+2\cdot x+1;\ \left[x^3=x+2\right]$
	14	$x^{14}+x^{10}+x^6+x+1$		4	$x^4+x+2;\ \left[x^4=2\cdot x+1\right]$
	15	$x^{15}+x+1$	5	2	$x^2+x+3;\ \left[x^2=4\cdot x+2\right]$
	16	$x^{16}+x^{12}+x^3+x+1$	7	2	$x^2+x+3;\ \left[x^2=6\cdot x+4\right]$

Складність виконання обчислень в полі $GF(p^r)$, а, відповідно, конструкція і вартість обладнання, які здійснюють ці обчислення, суттєво залежать від вибору представлення поля[41].

Наприклад, у полі Галуа $GF\begin{pmatrix}5\\2\end{pmatrix}$ з ключем 10010 на основі незвідного полінома x^5+x^2+1 взятого з табл.2.1 послідовність елементів a_0, a_1, a_2,…, a_{31}, де а31 це - Ø останній многочлен, визначається на основі рекурентного рівняння

$$G_{i+1}=G_i \overline{\oplus} G_{i-n};\ \text{n=5}, \tag{4.5}$$

та має вигляд послідовності елементів:

11111001101001000001010111011000,

які кодують числа у діапазоні 0, 1, 2, …, 31:

$b_5,b_4,b_3,b_2,b_1,\ b_2\oplus b_5,b_1\oplus b_4,b_2\oplus b_3\oplus b_5,b_1\oplus b_2\oplus b_4,\ b_1\oplus b_2\oplus b_3\oplus b_5,b_1\oplus b_4\oplus b_5,$
$b_2\oplus b_3\oplus b_4\oplus b_5,b_1\oplus b_2\oplus b_3\oplus b_4,b_1\oplus b_3\oplus b_5,b_4\oplus b_5,b_3\oplus b_4,b_2\oplus b_3,b_1\oplus b_2,\text{Ø},\ b_1\oplus b_2\oplus b_5,$
$b_1\oplus b_2\oplus b_4\oplus b_5,b_1\oplus b_2\oplus b_3\oplus b_4\oplus b_5,b_1\oplus b_3\oplus b_4\oplus b_5,b_3\oplus b_4\oplus b_5,b_2\oplus b_3\oplus b_4,b_1\oplus b_2\oplus b_3,$
$b_1\oplus b_5,b_2\oplus b_4\oplus b_5,b_1\oplus b_3\oplus b_4,b_3\oplus b_5,b_2\oplus b_4,b_1\oplus b_3.$

b_{31} = Ø, де Ø – пуста множина.

На основі даного співвідношення на рисунку. 4.3 показаний принцип формування 5- розрядного коду Галуа [42].

Рисунок 4.3-Формування коду Галуа при n=5

Відповідно за даним принципом на основі незвідних поліномів (табл.4.2) формуються n-розрядні двійкові коди Галуа.

Векторне представлення елементів поля $GF\begin{pmatrix}5\\2\end{pmatrix}$ можна отримати послідовно за допомогою схеми (рисунок 4.4), використовуючи примітивний незвідний поліном x^5+x^2+1. Клас залишків $\{x\}=\alpha$, де α – корінь многочлена x^5+x^2+1, є примітивним елементом поля $GF\begin{pmatrix}5\\2\end{pmatrix}$.

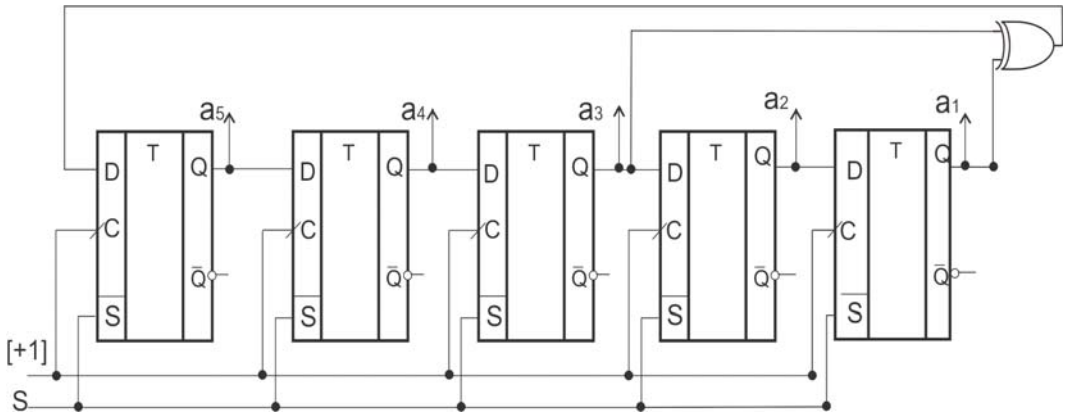


Рисунок 4.4 -Формувач елементів поля Галуа $GF\begin{pmatrix}5\\2\end{pmatrix}$

Якщо в тригер молодшого розряду занести одиницю, а в інші тригери-нулі, то одержимо представлення послідовних степенів елемента α.Від векторного представлення (двійкових комбінацій) елементів поля можна перейти до їх представлення з допомогою поліномів, якщо співставити двійкові розряди із степенями змінної x, які збільшуються справа наліво від 0 до $r-1$ Так для $r=4$:

$$
\begin{array}{cccc}
x^3 & x^2 & x^1 & x^0 \\
1 & 1 & 1 & 1 \quad \leftrightarrow x^3 + x^2 + x + 1 \\
1 & 0 & 1 & 1 \quad \leftrightarrow x^3 + x + 1
\end{array}
$$

Для кодування значень технологічних параметрів на основі вертикальної інформаційної технології використовують поліноми порядку 2^r, де $r > 20$. Щоб закодувати десяткові цифри від 0 до 1048575 кодом поля Галуа, необхідно вибрати незвідний примітивний поліном $h(x) = x^{20} + x^3 + 12$. Звідси використання кодових послідовностей Галуа для криптографічного захисту систем авто сигналізації є перспективним науково-технічним рішенням.

4.2 Принцип захисту автомобільної сигналізації на основі кодових послідовностей Галуа з перериваннями

Формування кодів поля Галуа з перериваннями успішно застосовується у системах передавання інформації з підвищеною завадозахищеністю від помилок на основі подання інформаційних бітів кодовими послідовностями Баркера та послідовностями максимальної довжини (М- сигналами). Суть даного способу полягає у тому, що на границі зміни ознаки маніпуляції інформаційного біта «0» та «1» виконується переривання генерованого КПГ іншим ключем незвідного полінома або його інверсія. Тому використання кодів поля Галуа з перериваннями дозволиться покращити характеристики безпеки GSM систем сигналізацій та унеможливити її взлом за допогою різноманітних кодграберів, оскільки будуть використовуватись різні поліноми задання модульованої послідовності, що небудуть повторятись.

На рисунку 4.5 показаний приклад реалізації такого способу формування кодів поля Галуа з перериваннями для найбільш поширених способів маніпуляції сигналів, які використовуються у сучасних

комп'ютерних мережах та телекомунікаційних системах згідно манчестерського коду та інших кодів [121].

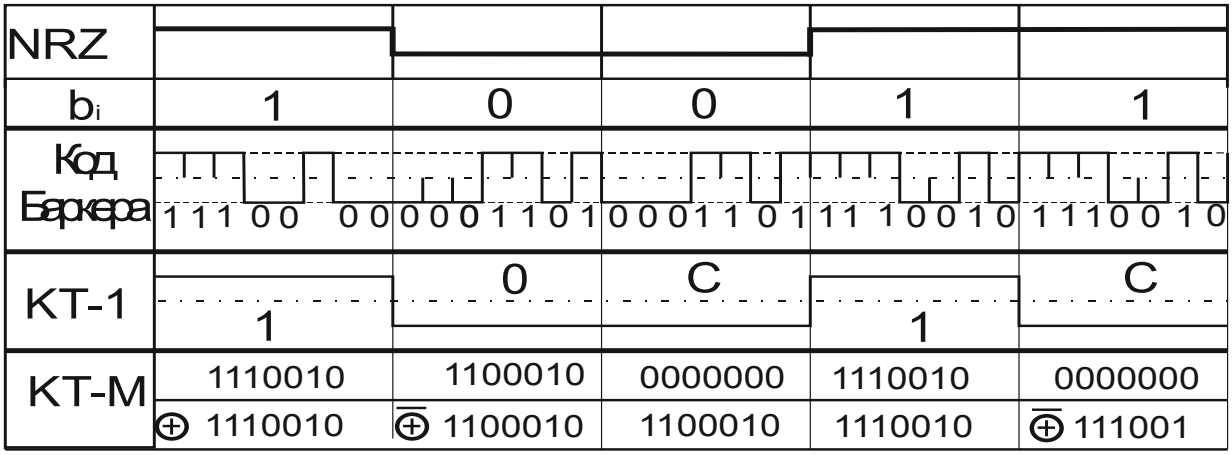


Рисунок 4.5-Формування коду поля Галуа з перериваннями для різних способів маніпуляції сигналів

Інший спосіб формування кодів поля Галуа з перериваннями базується на використанні базисних функцій КПГ нульового та першого порядку [44].

Суть однозначного кодування інформаційних потоків з ефектом стиснення даних представлені стартовими позиціями базисних функцій *p* інтервалом поширення у часі коду базисної функції КПГ, який повинен бути не менше довжини ключа *k* у полі $GF\left(\begin{matrix}k\\2\end{matrix}\right)$.

На рисунку 4.6 приведений приклад формування базисних функцій КПГ нульового порядку на основі різних стартових позицій в одному ключі.

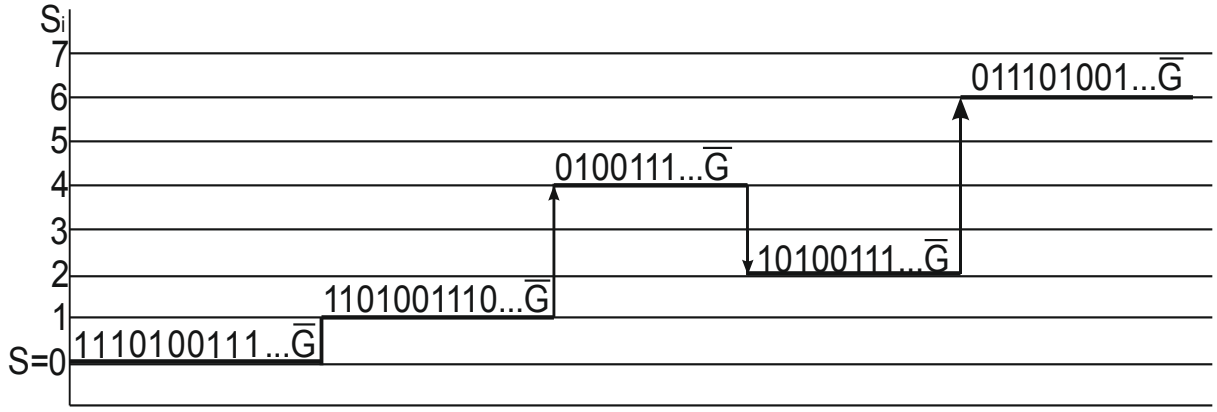


Рисунок 4.6- Формування біт-орієнтованих КПГ із перериваннями на основі стартових позицій переривання базисних функцій

Формалізація даного способу формування КПГ з перериванням відповідає функціоналу $\{S_j\} = G_{i+1+j} = G_{i+1+j} \oplus G_{i-n+j}$.

На рисунку 4.7 представлено принцип реалізації способу формування КПГ з перериваннями на основі використання базисних функцій Галуа нульового порядку та різних ключів у полі $GF\binom{k}{2}$, *k*- розрядність незвідного полінома.

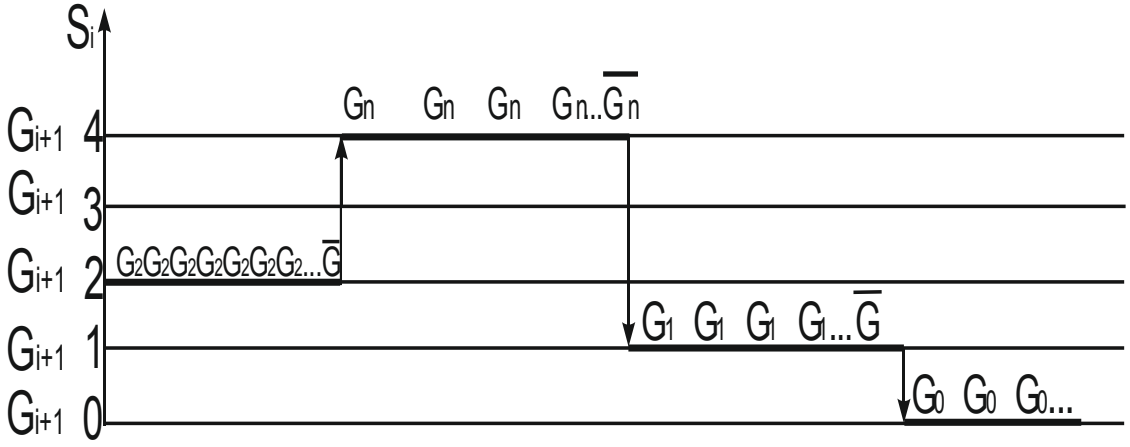


Рисунок 4.7-Формування КПГ з перериваннями на основі базисних функцій нульового порядку та різних ключів згідно незвідних поліномів

Базисні функції Галуа першого порядку також можуть бути застосовані для формування КПГ з перериваннями. При цьому, в якості їх кодової різниці від функції нульового порядку можуть вибиратись інші стартові позиції, що представляють функції нульового порядку.

Наприклад, у полі Галуа $GF\binom{8}{2}$ існує вісім стартових позицій, які можуть бути розділені певним чином у залежності від потреби і мети, наприклад, 4 і 4 – відповідних базисних функцій Галуа нульового та першого порядку, або 6 і 2 кожної з них.

На рисунку 4.8 показаний приклад формування КПГ з перериваннями на основі базисних функцій нульового та першого порядку із різними стартовими позиціями і двома різними ключами та перериваннями на основі інвертування двох бітів Галуа при переході з базисної функції нульового

порядку до наростаючої функції першого порядку та трьох інвертуючих бітів Галуа при старті функції першого порядку.

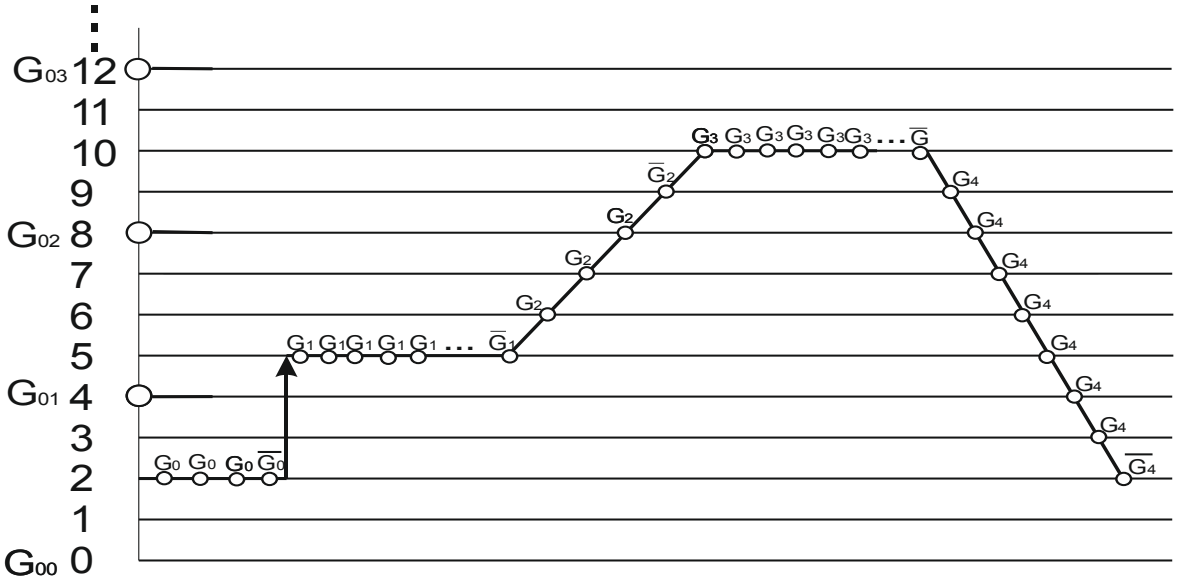


Рисунок 4.8-Формування кодів поля Галуа з перериваннями на основі базисних функцій нульового та першого порядку

Формування КПГ з перериваннями також застосовується у теорії логіко-статистичних інформаційних моделей (ЛСІМ) [42]. Суть способу полягає у тому, що ЛСІМ, які контролюють відхилення станів об'єктів управління від норми по амплітуді, динаміці, фазі, та спектру, (ЛСІМ 1-4) кодуються шляхом переривання інвертованим бітом $\overline{G}$ унітарної послідовності реального часу, що дозволяє ідентифікувати не тільки факт зареєстрованого ЛСІМ відхилення від амплітуди, але і сам код моменту часу.

На рисунках .4.9 та 4.10 приведений приклад такого способу формування КПГ з перериваннями.

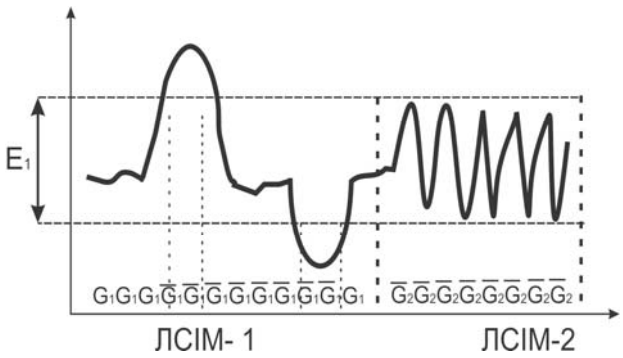


Рисунок 4.9-Логіко-статистичні інформаційні моделі 1-2.

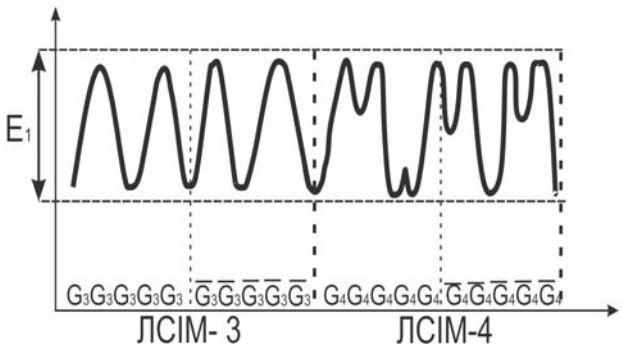


Рисунок 4.10-Логіко-статистичні інформаційні моделі 3-4.

Таким чином систематизовані та формалізовані способи формування КПГ із ознаками перериваннями, які показують широкі та ефективні можливості застосування у системах захисту автомобіля.

4.3 Моніторинг стану об'єкту захисту автоматизованої систем управління автосигналізацією

При зростанні складності технології виробництва автомобільних GSM сигналізацій, що керуються мікропроцесорними засобами, відповідно зростають об'єми, структурна складність моніторингу інформаційних потоків від датчиків системи у разі викрадення, або нанесення фізичної шкоди транспорту. Відповідно при спрацюванні датчиків автомобіля поступає сигнал через GSM модуль до власника автомобіля для забезпечення швидкої суб'єктивної реакції на відхилення ОУ від норми та швидкого прийняття правильних адекватних рішень. На рисунку 4.11 наведена структура моніторингу та ідентифікації станів ОУ

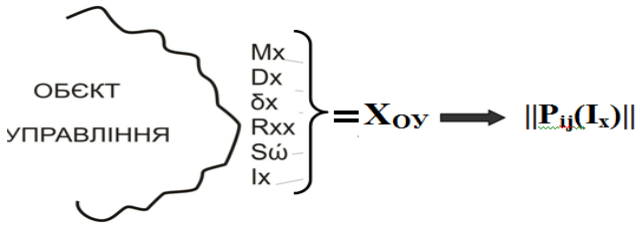


Рисунок 4.11 - Ідентифікація станів ОУ

Згідно структури (рисунок 4.1), параметри ОУ описуються M_x, D_x, δ_x, R_{xx},S_w, I_x – атрибутами фрейму оператора $X_{OУ}$ [45].

Згідно визначення параметрів ОУ, контроль параметрів технологічного процесу з можливістю передбачення розвитку екстренних станів технологічного процесу, здійснюється згідно наступної послідовності операцій:

$$X_{\hat{I}\acute{O}} = F(\{x_i\},\{x_j\},S_{\hat{i}\acute{o}},M_x,M_j,M_v,D_x,\delta_x,R_{xx},R_{xy},S_w,L_i,\rho_{ij},S_{ij},P_{ij},I_x), \quad (4.1)$$

де: $\{x_i\},\{y_i\}$ - масиви оцифрованих моніторингових даних параметрів ОУ;

$S_{iю}$ - відповідно семантичний, інформаційний та технологічний стани ОУ;

M_x, M_j, M_v - відповідно вибіркове, ковзне та вагове математичні сподівання;

D_x, δ_x - відповідно дисперсія та середньоквадратичне відхилення;

R_{xx} - автокореляційна функція;

S_w - спектри параметрів ОУ у різних теоретико-числових базисах;

L_i – логіко-статистичні інформаційні моделі (ЛСІМ), $i \in \overline{1,5}$;

ρ_{ij} - матриця коефіцієнтів взаємокореляції;

I_x - кореляційна міра ентропії стану ОУ.

Реалізацію способу контролю параметрів для різних станів технологічного процесу у порівнянні з еталонним, показано в таблиці 4.2.

Таблиця 4.2 - Стани технологічного процессу

Стан технологічного процесу	Параметри технологічного процесу									
	$\{x_i\}$	$\{y_i\}$	S	M_j	M_{xj}	M_{yj}	σ_x	σ_y	$C_{xx}(j)$	$R_{xy}(0)$
Еталон	•	•	•	•	•	•	•	•	•	•
Норма	+	+	+	+	+	+	+	+	+	+
Прогноз взлому	+	+	+	+	-	-	+	+	+	+
Взлом	+	+	+	-	-	-	+	-	-	-

Стан технологічного процесу	Параметри технологічного процесу										
	ρ_{xy}	L_1	L_2	L_3	M_x	M_y	M_{vx}	M_{vy}	L_4	P_{ij}	I_x
Еталон	•	•	•	•	•	•	•	•	•	•	•
Норма	+	+	+	+	+	+	+	+	+	+	+
Прогноз взлому	+	-	-	-	+	+	+	+	+	+	+
Взлом	-	-	-	-	-	-	-	-	-	-	-

Запропонований спосіб передбачає наступні види контролю, виконувані в приведеному нижче порядку:

- контроль перебування отриманого значення ковзного математичного сподівання M_j контрольованих параметрів в області можливих значень норми L_1;

- контроль середньостатистичної динаміки $C_{xx}(j)$ станів технологічного процесу по кожному параметру в області можливих значень норми L_2;

- контроль нормованих коефіцієнтів взаємокореляції між кожною парою параметрів ρ_{xy} в області можливих значень норми L_3;

- додатковий контроль вибіркових математичних сподівань M_x, M_y;

- додатковий контроль зважених математичних сподівань M_{vx}, M_{vy};

- додатковий контроль відхилень параметрів технологічного процесу по спектру L_4 в області можливих значень норми;

- додатковий контроль кластерної моделі матриці ймовірностей переходу технологічного процесу з одного стану в інший (P_{ij});

- додатковий контроль відхилень параметрів технологічного процесу згідно кореляційної міри ентропії I_x.

Відображення динаміки зміни структуризованого зображення образно-кластерної моделі на екрані монітора оператора відбувається згідно відповідного програмного забезпечення шляхом порівняння виміряних, спостережуваних та розрахованих параметрів технологічного процесу з еталонними.

На рисунку 4.12 представлена система контролю, параметрів роботи автомобільної GSM сигналізації на основі динамічного коду Галуа з перериваннями, що базується на змішаному використанні незвідним поліномів у одному кодовому наборі. Система працює наступним чином центральний блок контролює роботу периферійних пристроїв. На нього

постійно надходить інформація про стан датчиків відкривання дверей, датчика ударів, датчика проникнення. Режим роботи центрального блоку можна задавати пультом управління, що знаходяться в салоні автомобіля або дистанційно, прийняттям радіосигналів з підсистеми користувача з використанням GSM пристрою. У разі проникнення або спрацювання контрольних датчиків центральний блок влючає сирену, блокує систему запалювання, а так само керує виведенням інформації через радіоканал за допомогою передавача. Живлення підсистеми автомобіля проводиться від бортової мережі автомобіля. Подача сигналів тривоги здійснюється за допомогою сирени, миготінням габаритних вогнів і через GSM пристрій. Радіоприймальні і радіопередаючий пристрій працюють на одну антену.

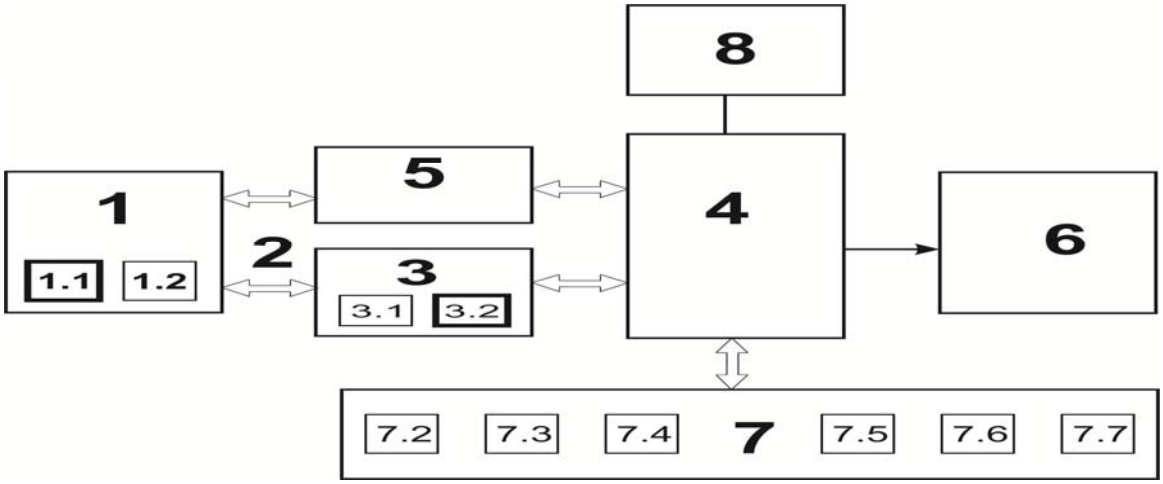


Рисунок 4.12 - Система контролю параметрів технологічного процессу

Система контролю параметрів технологічного процессу включає

1 – пульт управління автомобільною сигналізацією,

1.1- кодовий шифратор Галуа,

1.2- передавач кодового сигналу,

2- кодовий сигнал Галуа,

3- приймач сигналу,

3.1- пристрій ідентифікації відправника,

3.2- дешифратор коду Галуа,

4- центральний блок управління,

5- GSM модуль

6- пристрій блокування двигуна,

7- Блок збору інформації з датчиків,

7.2-7-7 - датчики вимірів параметрів (датчики відкривання дверей, 7.3-ультразвуковий датчик руху,7.4-датчик удару, 7.5- датчик сирени, 7.6-датчик включення фар, 7.7- датчик тиску)

8- модуль енергозабезпечення сигналізації.

Блок збору інформації з датчиків 7 призначений для ідентифікації стану об'єкта контролю у разі спрацювання якогось датчика блок збору інформації передає сигнал на центральний блок 4, де за допомогою GSM модуля передаються коди виміряних значень, що супроводжуються кодом стану об'єкта, які передаються до пульта.

Центральний блок управління -4 являє собою програмний контролер, що реалізує паралельне опитування датчиків і перетворення кодів вихідних величин датчиків, отриманих від блока збору інформації -2 у значення відповідних параметрів. На виході центрального блоку за допомогою шини в пристрій підготовки інформації надходить набір кодів ансамблю параметрів, які визначаються кодом стану керування, що надходять до пульта оператора -1. Необхідність паралельного формування кодів параметрів об'єкта, які надходять у центральний блок 4, що обумовлено необхідністю виключення ефектів старіння інформації, які можуть виникати при організації циклічного опитування датчиків і негативно впливають на розрахунок структурної кореляційної функції та коефіцієнтів нормованої взаємокореляції.

Процес виміру та ідентифікації стану об'єкту контролю включає наступні етапи:

- з пульта оператора 1 відбувається подача зашифрованого шифратором Галуа -1.2 кодового сигналу Галуа-2 на приймач сигналу 3, де відбувається ідентифікація пристрою відправника -3.1 та дешифрування сигналу 3.2.

- прийом і розшифровку сигналу виклику ансамблів n з m параметрів приймача 3 та видачу ідентифікованого правильного коду та відправника у центральний блок управління 4. Де визначаються наступні дії

- перетворення і запам’ятовування отриманих значень кодів параметрів;

- визначення стану датчиків автомобіля;

- додаткове формування еталонного зображення образно-кластерної моделі стану технологічного процесу "норма";

- додаткове порівняння параметрів еталонного стану з виміряними, спостережуваними та розрахованими параметрами технологічного процесу;

- розблокування датчика відкриття дверей .

Результатом запропонованого способу контролю параметрів технологічного процесу є розширення функціональних можливостей та підвищення інформативності інтегрованого представлення станів об’єкта управління, що дозволяє збільшити швидкодію реакції оператора на виникнення нештатних ситуацій та покращення можливостей попередження виникнення взлому автомобіля.

ВИСНОВКИ

Розроблений варіант системи автоматизації направлений на вдосконалення системи автоматизації автомобільної охоронної сигналізації з GSM модулем. У роботі були розглянуті існуючі способи побудови автомобільних сигналізацій, проведена їх класифікація. Було прийнято, що найбільший комерційний успіх матиме автомобільна сигналізація, що має модульну структуру та моє можливість оповіщення власника про своє місцезнаходження засобами GSM та GPS, яка дозволить їй охоплювати всі класи сигналізацій.

Синтезована АСУ володіє такими характеристиками як дискретне регулювання показників датчиків та можливість віддаленого запуску двигуна за допомогою датчика запалювання. Відповідно до заданих параметрів ОУ шляхом моделювання були обраховані параметри налаштування ПІ-регулятора, що забезпечує необхідну точність під час регулювання.

Був проведений аналіз необхідних пристроїв, визначені їх основні технічні характеристики і можливості, відповідно до яких було обрано пристрої, що мають найкращі можливості до автоматизації.

Вдосконалений варіант системи авто сигналізації на основі кодових систем Галуа з перериванями дозволитьть покращити захист такої системи, що відповідає більш сучасним вимогам, які ставляться до систем, має більшу швидкодію і функціональні можливості, дає можливість розширенню об’єму функцій, які виконуються для поспішного переходу на різні режими роботи.

При розробці даного дипломного проекту були розроблене логіко статистичні інформаційні моделі на основі кодів Галуа, що дозволили покращити функціональні властивості таких систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Говорущенко Н. Я. Экономическая кибернетика транспорта /Н.Я. Говорущенко, В.Н. Варфоломеев. – Харьков : РИО ХГАДТУ, 2000. – 218 с. – ISBN 966-7428-21-8.
2. Говорущенко Н. Я. Техническая кибернетика транспорта /Н. Я. Говорущенко, В. Н. Варфоломеев. – Харьков : РИО ХГАДТУ, 2001. –271 с. – ISBN 966-7839-23-0.
3. Говорущенко Н. Я. Системотехника транспорта /Н.Я. Говорущенко, А.Н.Туренко. – Харьков : РИО ХГАДТУ, 1999. –468 с. – ISBN 966-7427-218.
4. Туренко А. Н. История инженерной деятельности. Развитиеавтомобилестроения: уч. пособ. / А. Н. Туренко, В. А. Богомолов, В. И. Клименко. – Харьков : ХГАДТУ, 1999. – 252с.
5. Автомобильный справочник BOSCH. Перевод с англ. – Москва :За рулем, 2004. – 992 с. – ISBN 5-85907-327-5.
6. Данов Б. А. Электронные системы управления иностранныхавтомобилей / Б. А. Данов. – М. : Горячая линия – Телеком, 2002. – 224 с. –ISBN 5-93517-085-X.
7. Сосин Д. А. Новейшие автомобильные электронные системы /Д. А. Сосин, В. Ф. Яковлєв – Москва : Солон-Пресс, 2005. – 240 с. –ISBN 5-98003-201-0.
8. Сига Х. Введение в автомобильную электронику / Х. Сига,С. Мидзутани. – Москва: Мир, 1989. – 232 с. – ISBN 5-03-000367-3.
9. Федосов В. П. Автомобильная электроника : уч. пособ. /В. П. Федосов, В. Д. Сытенький. – Таганрог : ТРТУ, 1998. – 73 с.
10. Петров В. М. Электрооборудование, электронные системы ибортовая диагностика автомобилей : уч. пособ. / В. М. Петров,И. Ф. Дьяков. – Ульяновск: УлГТУ, 2005. – 115 с.
11. Технические системы обеспечения безопасности дорожногодвижения / [Комаров В. М. и др.]. – Москва : Транспорт, 1990. – 351 с.

12. Поляк Д. Г. Электроника автомобильных систем управления /Д. Г. Поляк, Ю. К. Есеновский–Лашков. – Москва : Машиностроение,1987. – 199 с.
13. Кучер В. П. Диагностика японских автомобилей / В. П. Кучер. –Москва : Легион–Автодата, 2002. – 176 с. – ISBN 5-88850-146-8.
14. Твег Р. Диагностика электронной системы управления двигателяавтомобиля: руководство по техническому обслуживанию и ремонту / РоссТвег. – Москва : Астрель, 2003. – 144 с. – ISBN 5-271-05883-2.
15. Афонин С. В. Устройство и диагностика автоматических коробокпередач легковых автомобилей. Переднеприводные, заднеприводные, полноприводные : практ. руководство / С. В. Афонин – Ростов-на-Дону :ПОНЧиК, 2000. – 136 с. – ISBN 5-8069-0011-8.
16. Андрианов В. И. Автомобильные охранные системы : справ.пособ. / В. И. Андрианов, А. В. Соколов – Санкт-Петербург : Арлит, 2000.– 272 с. – ISBN 5-8206-0121-1.
17. Воловник А. А. Знакомтесь, информационные технологии /А. А. Воловник. – Санкт-Петербург : БХВ-Петербург, 2002. – 352 с. –ISBN 5-94157-182-8.
18. Литвиненко В. В. Автомобильные датчики, реле и
переключатели. Краткий справочник / В. В. Литвиненко, А. П. Майструк. – Москва : За рулем, 2004. – 176 с. – ISBN 5-85907-353-4.
19. Заде Л. Понятие лингвистической переменной и его применение кпринятию приближенных решений / Лотфі Заде. - М. : Мир, 1976. 165 с.
20. Борисов А.Н. Принятие решений на основе нечетких моделей.Примеры использования / А. Н. Борисов, О. А. Крумберг, И. П. Федоров.-Рига : Зинатне, 1990. – 184с.
21. Ротштейн А. П. Интеллектуальные технологии идентификации:нечеткие множества, генетические алгоритмы, нейронные сети /А. П. Ротштейн. – Винница : УНІВЕРСУМ-Вінниця, 1999. – 230с. –ISBN 966-7199-49-5.

22. Intel, “Fuzzy Anti-Lock Braking System, ”developer. intel. Com /design/ MCS96 /DESIGNEX/ 2351.htm, 1996.
23. N. Matsumoto et al., “Expert antiskid system,” IEEE IECON’87, 810–816, 1987.
24. H. Kawai et al., “Engine control system,” Proc. of the Int’l Conf. onFuzzy Logic and Neural Networks, Iizuka, Japan, 929–937, 1990.
25. “Benchmark Suites for Fuzzy Logic”http://www. fuzzytech.com/e_dwnld.htm, 1997.
26. H. Takahashi, K. Ikeura, and T. Yamamori, “5-speed automatictransmission installed fuzzy reason-ing,” IFES’91–Fuzzy Engineering towardHuman Friendly Systems, 1136–1137, 1991.
27. P. Sakaguchi et al., “Application of fuzzy logic to shift schedulingmethod for automatic transmis-sion,” 2nd IEEE Int’l. Conf. on Fuzzy Systems,52–58, 1993.
28. C. von Altrock, B. Krause, and H.-J. Zimmermann, “Advanced fuzzylogic control of a model car in extreme situations,” Fuzzy Sets and Systems,48:1, 41–52, 1992.
29. L. I. Davis et al., “Fuzzy Logic for Vehicle Climate Control,” 3rdIEEE Int’l. Conf. on Fuzzy Sys-tems, 530–534, 1994.
30. J.-P. Aurrand-Lions, M. des Saint Blancard, and P. Jarri,“Autonomous Intelligent Cruise Control with Fuzzy Logic,” EUFIT’93–1st Eur.Congress on Fuzzy and Intelligent Technologies, Aachen, 1–7, 1993.
31. Харисова В. Н. Глобальная спутниковая радионавигационная система ГЛОНАСС/ [под ред. В. Н. Харисова, А. И. Перова, В. А. Болдина]. – М. : ИПРЖР,1998. – 400 с. – ISBN 5-88070-004-6.
32. Каган Б.М. Основы проектирования микропроцессорных устройств автоматики./ Б.М. Каган, В.В. Сташин // М.: Энергоатомиздат, 1987.
33. Игнатущеико Организация структур управляющих микропроцессорных вычислительных систем / В.В. Игнатущеико// М.: Энергоатомиздат, 1984.

34. Алекеенко А.Г., Галицин А.А., Иванннков А.Д. Проектирование радиоэлектронной аппаратуры на микропроцессорах. М.: Радио и связь, 1984.
35. Алекеенко А.Г., Шагурин И.И. Микросхемотехника: Учебное пособие / Под ред. И.П. Степаненко. М.: Радио и связь, 1982.
36. Видениекс П.О., Ветиньш Я.Я., Кравченков А.А. Проблемно-ориентированные микропроцессорные системы в производстве РЭА. М.: Радио и связь, 1987.
37. Яценков В.С. Микроконтроллеры MicroCip. Практическое руководство. М., 2002 г.
38. Николайчук Я.М. Теорія джерел інформації / Я.М. Николайчук / Тернопіль: ТНЕУ, 2008.-536с.
39. Николайчук Я.М. Проектування спеціалізованих комп'ютерних систем / Я.М. Николайчук, Н.Я. Возна, І.Р. Пітух / Навчальний посібник / – Тернопіль: ТзОВ «Терно-граф», 2010.–392 с.
40. Николайчук Я.М. Коди поля Галуа / Я.М. Николайчук // ТзОВ «Терногpаф», – Тернопіль, –2012. –576 с.
41. Патент на корисну модель. №70744 Україна, МПК H038M. Аналого-цифровий перетворювач /Я.М. Николайчук, П.В. Гуменний. – опуб. 25.06.2012, бюл. №12.
42. Гуменний П.В. Метод побудови паралельного аналого-цифрового перетворювача у теоретико-числовому базисі Галуа з найменшим числом імпульсних компараторів /П.В. Гуменний// Вісник Хмельницького національного технічного університету. – 2013. – №4. – С.152-157.
43. Гуменний П.В. Функціональна структура спецпроцесора вертикально-інформаційної технології та його компоненти. /П.В. Гуменний, Я.М. Николайчук// Вісник національного університету "Львівська політехніка", "Комп'ютерні системи та мережі". –2012. –№745. –С.69-74.
44. Гуменний П.В. Автоматизована система керування на основі вертикально-інформаційної технології у кодовому базисі Галуа / П.В. Гуменний,

Б.Ю.Гуменюк , В.Р.Расевич , І.М .Хомишин//Збірник матеріалів проблемно-наукової міжгалузевої конференції “Юриспруденція та проблеми інформаційного суспільства (ЮПІС-2018)” – Тернопіль – 2018 – с.79-84.

ДОДАТОК А

Алгоритм автоматизованого управління автомобильною сигналізацією.