Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем»

КвРКІ. 180155.20.02.24 ПЗ

Виконав: студент 2 курсу, група КІ2м-20-1 _____ Башук В.Ю.
Підпис Ініціали, прізвище

Керівник кандидат техн.наук, доцент _____ Гнатчук Є.Г.
Науковий ступінь, вчене звання Підпис Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Т.О. Говорущенко
11 05 2022 р.

Хмельницький, 2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма Освітньо-наукова програма «Комп'ютерна інженерія програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"01" 09 2021

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ)

Башуку Віталію Юрійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем

Керівник проекту (роботи) Гнатчук Є.Г., к.т.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 06.01.2022 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 03.05.2022 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз та характеристики спеціалізованої комп'ютерної системи голосового керування автомобілем

Засоби та методи забезпечення надійності голосового керування автомобілем

Алгоритми та технології забезпечення надійності від сучасних способів кібератак на систему голосового керування автомобіля

Додаткова біометрична система аутинтифікації користувача для забезпечення надійності від кібератак

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІС		

7. Дата видачі завдання « 06 » 09 2021р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики ДРМ з керівником	05.09.2021	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.10.2021	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	05.11.2021	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	05.12.2021	виконано
5	Робота над науковою статтею	05.01.2022	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2022	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	05.04.2022	виконано
8	Оформлення пояснювальної записки згідно вимог	15.04.2022	виконано
9	Попередній захист ДРМ	18.04.2022	виконано
10	Захист ДРМ на засіданні ЕК	До 10.05.2022	

Студент _____ В.Ю. Башук
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Є.Г. Гнатчук
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема дипломної роботи: Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем.

Автор роботи: Башук Віталій Юрійович.

Керівник роботи: Гнатчук Єлизавета Геннадіївна.

Пояснювальна записка: 117 с., 31 рис., 17 табл., 3 дод., 76 джерел.

СИСТЕМА, ГОЛОСОВЕ КЕРУВАННЯ, НАДІЙНІСТЬ, ЗАСОБИ, МЕТОД, СПЕЦІАЛІЗОВАНА КОМПЮТЕРНА СИСТЕМА.

Об'єктом дослідження є надійність спеціалізованої комп'ютерної системи голосового керування автомобілем

Предметом дослідження є спеціалізована комп'ютерна система голосового керування автомобілем

Метою дипломної роботи є дослідження та оцінка ефективності методів та засобів забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем

Для розв'язання поставлених задач використовувалися методи та засоби забезпечення надійності, моделі загроз, аналіз даних, дослідження, теорії голосового керування.

Наукова новизна отриманих результатів:

1. Розроблений метод підвищення безпеки системи голосового керування автомобілем, що дозволяє на підготовчому етапі проведення кібератаки попередити та унеможливити її виконання за рахунок блокування ультразвукових коливань пристрою, що проводить записування вхідного сигналу.

2. Запропоновано метод, що дозволяє вирішити задачу забезпечення надійності голосового керування автомобілем, використовуючи засоби додаткової біометричної аутентифікації користувача.

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення для системи додаткової біометричної аутентифікації користувача.

Практична цінність отриманих результатів. В результаті виконаного наукового дослідження запропоновано апаратні та програмні методи забезпечення надійності спеціалізованих комп'ютерних систем «Android Auto» та «Apple CarPlay» від кібератак на основі проведення ультразвуковими та світловими командами. Виконано комплексну оцінку ефективності використаних моделей та методів для вирішення поставленої задачі. Проведено експериментальне дослідження системи на різних користувачах, в результаті якого було встановлено, що система справно виконує всі задані функції. .

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ОС - операційна система

КС - комп’ютерна система

СКС - спеціалізована комп’ютерна система

ПЗ - програмне забезпечення

СРМ - система розпізнавання мовлення

СГК - система голосового керування

ПГК - передавач голосових команд

ФНЧ - фільтр низьких частот

ASIC - інтегральна схема спеціального призначення

ВСТУП

На сьогодні, інформаційні технології широко і прогресивно розвиваються з кожним днем у всіх напрямках, і це впливає на кожного з нас. Одним з важливих аспектів є можливість голосового керування. Системи з голосовим керуванням широко використовуються в різних галузях, в тому числі в автомобільному машинобудуванні.

Комп'ютерна система – це інформаційний комплекс, мета якого полягає в обробці, вводу-виводу інформації, збереження та іншого. Використовуючи комп'ютерну мережу за допомогою локальної системи передачі даних відбувається обмін інформацією та інше. В комп'ютерній системі використовують такі структури: програмні, організаційні, документальні та інші. Комп'ютерна система дозволяє інтегруватись з іншими інженерними технологіями, збільшувати можливості та створювати суцільне середовище для керування за допомогою різноманіття комп'ютерних технологій [1].

Спеціалізована комп'ютерна системи (СКС) належить до класу спеціально-орієнтованих систем, що вбудовані та розподілені в КС реального часу, та функціональних комп'ютерних систем відповідного спеціального призначення з відповідним апаратно-програмним забезпеченням.

Спеціалізована комп'ютерна система голосового керування автомобілем допомагає вам за допомогою голосових команд керувати функціями, наприклад прокладання маршруту в навігаторі, використання клімат-контролю і його функціоналу, керування мультимедійною системою, також в ній є можливість взаємодії з користувачем. За допомогою голосових помічників, система може відповідати на задані голосові команди та показувати різну інформацію, на екрані мультимедійного пристрою водія.

Актуальність роботи полягає в тому, що системи голосового керування стають дедалі популярнішими в різних сферах застосування, в тому числі і в галузях машинобудування. Ними все частіше користуються люди різного віку,

тому що вони є досить простими в експлуатації, а головне дієвими тому, що використовують різноманітні функції для вирішення різних типів задач.

По-друге голосові помічники систем голосового керування допомагають виконувати різноманітні типи задач для користувачів завдяки широкому функціоналу.

З одного боку, сучасні алгоритми розпізнавання голосових команд, є ще не зовсім досконалими, та не завжди чітко розуміють задану команду користувача і можуть піддаватися різним типам кібератак, але з іншого боку, завдяки розвитку технологій нейромереж і хмарних обчислень, та використання сучасних апаратних та програмних засобів або методів для забезпечення надійності, цю проблему можна звести до мінімуму.

Отже, дослідження та оцінка ефективності методів та засобів забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем є актуальною задачею.

Метою дипломної роботи є дослідження та оцінка ефективності методів та засобів забезпечення надійності спеціалізованої комп’ютерної системи голосового керування автомобілем.

Поставлена мета досягається розв’язанням таких основних задач:

– дослідити методи та засоби забезпечення надійності спеціалізованої комп’ютерної системи голосового керування автомобілем. Для вирішення цієї задачі необхідно розглянути основні концепції та оцінити ефективність використання зарубіжних спеціалізованих комп’ютерних системах таких як: «Android Auto» та «Apple CarPlay». Розробити моделі виявлення та методи підвищення надійності голосового керування. Також виявити існуючі небезпеки та недоліки в користуванні даними системами. Провести аналіз відомих характеристик методів та засобів для забезпечення надійності.;

– виконати моделювання процесу надійності та безпеки в спеціалізованих комп'ютерних системах голосового керування автомобілем;

– розглянути сучасні способи проведення кібератак на автомобільні системи;

– запропонувати апаратні та програмні методи підвищення надійності від сучасних кібератак.

Об’єктом дослідження є надійність спеціалізованої комп’ютерної системи голосового керування автомобілем.

Предметом дослідження є спеціалізована комп’ютерна система голосового керування автомобілем.

Наукова новизна отриманих результатів:

1. Розроблений метод підвищення безпеки системи голосового керування автомобілем, що дозволяє на підготовчому етапі проведення кібератаки попередити та унеможливити її виконання за рахунок блокування ультразвукових коливань пристрою, що проводить записування вхідного сигналу.

2. Запропоновано метод, що дозволяє вирішити задачу забезпечення надійності голосового керування, використовуючи засоби додаткової біометричної аутентифікації користувача.

Практична цінність отриманих результатів. В результаті виконаного наукового дослідження запропоновано апаратні та програмні методи забезпечення надійності спеціалізованих комп’ютерних систем «Android Auto» та «Apple CarPlay» від кібератак на основі проведення ультразвуковими та світловими командами. Виконано комплексну оцінку ефективності використаних моделей та методів для вирішення поставленої задачі. Проведено експериментальне дослідження системи на різних користувачах, в результаті якого було встановлено, що система справно виконує всі задані функції.

За темою магістерської роботи подано статтю «RESEARCH OF METHODS AND MEANS OF ENSURING THE RELIABILITY OF A SPECIALIZED COMPUTER VOICE VEHICLE CONTROL SYSTEM» у фахове наукове видання Computer systems and information technologies (м.Хмельницький) [2].

1 АНАЛІЗ ТА ХАРАКТЕРИСТИКИ СПЕЦІАЛІЗОВАНОЇ КОМПЮТЕРНОЇ СИСТЕМИ ГОЛОСОВОГО КЕРУВАННЯ АВТОМОБІЛЕМ

1.1 Огляд характеристик та поняття голосового керування

Перші спеціалізовані комп’ютерні системи, які могли здійснювати голосове керування, були недосконалими та ненадійними. Різні види фонових шумів, неправильна інтонація, могли порушувати голос людини, це своєю чергою робило неможливим розпізнавання голосової команди для комп’ютера. Отже, необхідно досить уважно вивчити, якими саме функціями та компонентами автомобіля можливо керувати за допомогою голосових команд. У роботі [3] показано порівняння навичок та умінь людини та комп’ютера. Автор показує, що в несподіваних ситуаціях, комп’ютер зазвичай безпорадний. В питаннях розв’язання проблем, людина може розв’язувати невідомі проблеми, а ПК тільки відомі. Людина може адаптуватися за допомогою творчості, при цьому ПК працює лише через задані алгоритми дій. В складних підрахунках комп’ютер набагато швидший.

Водіння автомобіля, це складне завдання, яке містить невідомі та непередбачувані ситуації, тому потрібно зробити висновок, що система голосового керування повинна зосереджуватись лише на функціях, як не несуть небезпеку користувачеві. Тому водії залишаються технологічно обмеженими, лише тими можливостями які їм не загрожують. Представлена система [4] на цей час обмежена такими завданнями як керування мультимедією, регулюванням дзеркал, сидіння, замикання та відмикання дверей, голосова ідентифікація, додаткові функції відповідно до моделі автомобіля.

Однією з перших автомобільних систем голосового керування була СКС Linguatronic [5], введена в автомобіль Mercedes-Benz. Це було апаратне рішення в окремій коробці, що містить ASR на основі HMMenginе. Діалогові вікна мовлення охоплювали лише дуже прості завдання команди та керування для телефону та аудіо. Завдання телефону включали набір номера, шляхом вимовляння

послідовності цифр, для доступу до записів телефонної книги. Завдання аудіо включало вибір радіочастоти, вибір назви станції за голосовими позначками та вибір радіостанцій. Він також охоплює роботу пристрою зміни дисків, промовляючи номер компакт-диска та назву, або просто попросивши наступну назву.

Деякі функції головного пристрою, не мають можливості активації голосом, наприклад налаштування часу та дати. Інші функції головного блоку, наприклад, медіаплеєр, підтримуються лише елементарно. Все більше користувачів передають свою музику на свій розсуд і хочуть керувати цією функцією голосом. Нові медіа будуть все більше інтегруватися в головний блок або передаватися до нього пристроями. Користувачі хочуть вибрати артистів, альбоми та назви своєї музичної колекції на будь-якому підключеному пристрої за назвою. Автор у роботі [6], показують підхід до ефективного доступу до аудіо даних у великих базах за допомогою трьох різних стратегії пошуку на основі категорій, пошук без категорій і фізичного пошуку.

Окрім вже звичного перегортання музичних треків, радіостанцій та каналів, можна слухати читання текстових книг, що допоможе прикрасити проведення часу в пробках. Переміщенням за списками меню, керуванням кліматом та освітленням. Пошуку контактів телефону додалася можливість прослуховувати та створювати повідомлення електронної пошти та SMS. Для цього потрібно лише синхронізувати телефон з автомобілем за допомогою Bluetooth або кабелю USB, параметрами бортового комп'ютера.

Науковий прогрес також доторкнувся до СКС голосового керування автомобілем, сучасні системи значно розширили свій потенціал. Розробники прагнуть максимально наблизити формат взаємодії до природного діалогу. Розмовна мова, діалекти, сторонні шуми, швидкість вимови, особливості дикції людини та навіть нестандартні формулювання команд дедалі менше стають на заваді якісному функціонуванню.

Прагнення природності діалогового спілкування простежується кожному рівні. Крім того, це правильна інтерпретація. Система може розшифровувати

скорочення, «знає» багато абревіатур, форматів дати та чисел тощо природність відтворюваного мовлення керування кліматом (рисунок 1.1) та освітленням автомобіля.

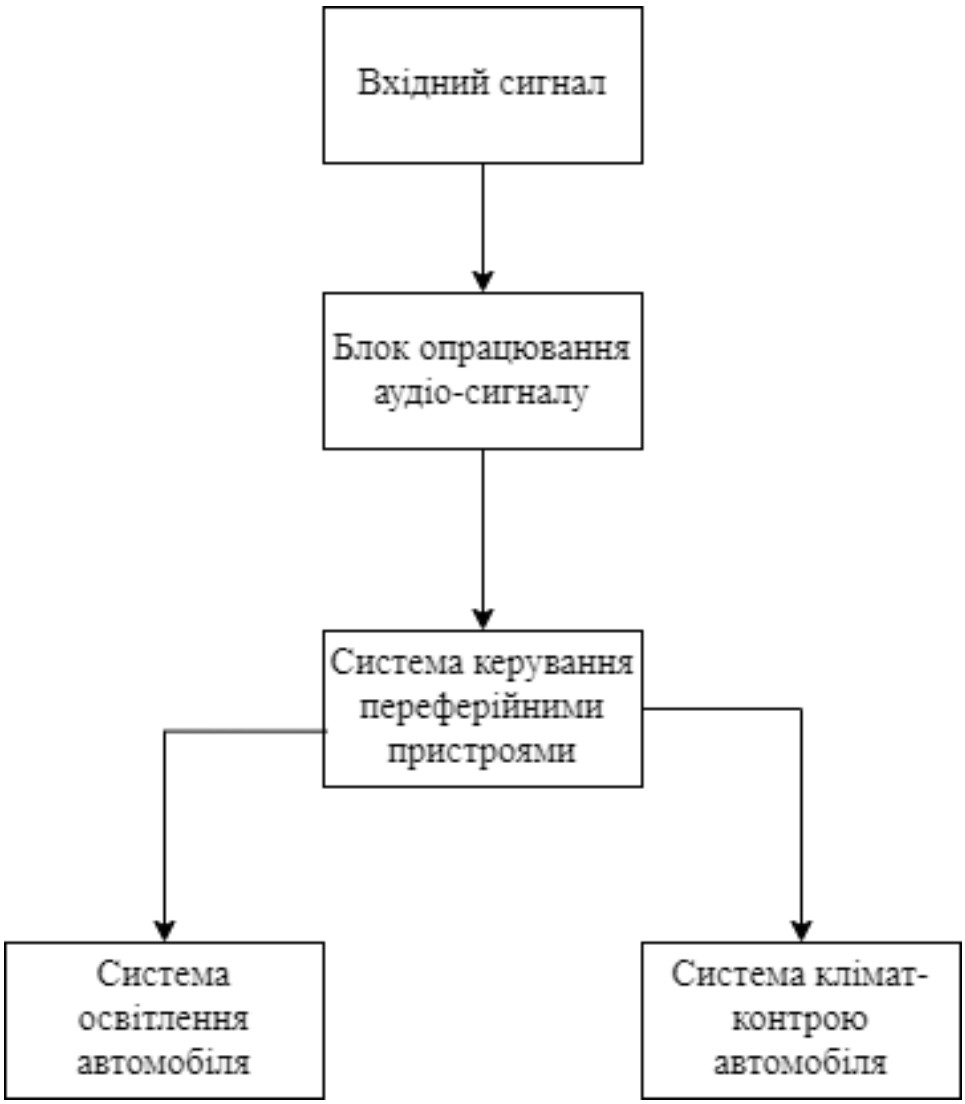


Рисунок 1.1 – Схема голосового керування кліматом та освітленням автомобіля

Після успішного розпізнавання команди подається відповідний сигнал, режим постійного відстеження команд. Зазвичай перед подачею команди потрібно натиснути на спеціальну кнопку, розташовану на кермі, але в деяких нових реалізаціях голосове керування має режим безперервного прослуховування і може виділяти команди без натискання на кнопку.

1.2 Принцип роботи та відомі методи підвищення надійності голосового керування автомобілем

Автономні автомобілі є темою широкого й актуального інтересу в автомобільній промисловості. Деякі форми автоматизованих транспортних технологій, такі як Advanced Driver Assistance Systems (ADAS), вже впроваджуються у виробничі транспортні засоби [7]. Виробники транспортних засобів оголошують про свої плани поступового впровадження можливостей автоматизації в свої транспортні засоби [8-9]. Інші, такі як Tesla, вже пропонують функції автопілоту у своїх серійних автомобілях за допомогою простого оновлення програмного забезпечення по повітрю [10].

Однак найбільш перспективні події відбудуться між 2025 і 2035 роками, коли очікується, що на дорогах з’являться повністю автономні автомобілі [11-12].

Сучасні автомобілі розвиваються з кожним роком, вдосконалюючись новими спеціалізованими комп’ютерними системами та рішеннями, для того, щоб зробити водіння максимально безпечним та комфортним.

Велика кількість кнопок і перемикачів для керування великою кількістю функцій і параметрів, робить місце водія схожим на пілотську кабіну. Система голосового керування, встановлена в автомобілі, дозволяє водієві не відвиртатися від ситуації на маніпуляції з кнопками для забезпечення максимальної сконцентрованості на дорозі.

У сучасних автомобілях голосове керування здійснюється шляхом вимови належних команд, які шляхом проходження певних перетворень перетворюються в сигнали керування для відповідних систем. На сьогодні за допомогою голосового керування можна керувати в автомобілі наступними системами зображеними в таблиці 1.1.

При створенні систем голосового керування повинні враховувати проблеми пов'язані з фоновими шумами, відмінності у вимові, акценти, розмір словника, початку і кінця промови. Проблеми пов'язані з шумами вирішуються за допомогою якісних мікрофонів і методів фільтрації [13].

Для розв’язання проблем пов'язаних з відмінності у вимові, акцентами, словниковим запасом застосовуються такі типи рішення:

– інтервал між окремими словами, якщо система розпізнає мову, користувач може вимовляти фрази в природному вигляді, не роблячи проміжків між словами;

– ступінь деталізації при застосуванні еталонів.

Таблиця 1.1 – Системи голосового керування та їхні функції

Тип системи	Виконання функції
Система клімат контролю	За допомогою системи клімат-контролю, користувач може змінювати температуру, вмикати підігрів сидінь, змінювати швидкість вентилятора та інше.
Мультимедійна система	Надає можливість отримувати, передавати, інформацію відео та аудіо-сигналів.
Система роботи з телефоном	Дозволяє здійснювати та приймати телефонні дзвінки.
Система параметрів бортового комп’ютера автомобіля	Визначає параметри керованого руху автомобіля.
Система керування навігацією	Дозволяє виконувати голосове керування для навігаційної системи.
Система санкціонованого доступу до автомобіля	Методом розпізнавання голосу користувача, визначає його біометрію.

При створенні систем голосового управління повинні враховувати проблеми пов'язані з фоновими шумами, відмінності у вимові, акценти, розмір початку і кінця промови. Проблеми пов'язані з шумами вирішуються за допомогою якісних мікрофонів і методів фільтрації.

Системи розпізнавання можуть використовувати як великі, так і маленькі словники. Системи, що працюють з маленькими словниками (близько 50 слів), дозволяють користувачеві давати прості команди комп'ютера. Розпізнавання мови містить в собі такі основні етапи як: синергетика, телематика дорожніх машин и систем у навчальному процесі попередню обробку сигналу та його класифікацію [13].

На попередній обробці вихідний сигнал перетворюється в вектор ознаки, на основі якої проводитися його класифікація. Він дає змогу включати в себе наступні кроки, наприклад, перетворення сигналу з аналогової форми в цифрову, застосування фільтрів для придушення шумів, виділення границь мовлення, ознаки виділення сигналів.

Для вирішення завдання класифікації використовуються різні математичні методи побудовані в основному на основі порівняння з еталоном [13-14]:

– динамічного програмування;

– залежної класифікації;

– тимчасових динамічних алгоритмів (Dynamic Time Warping) [15];

– аналізу заснованому на Баєсовій дискримінації (Basyesian discrimination) [16];

– прихованих Марківських моделей (Hidden Markov Model)[17];

– нейронних мережах.

Для практичної реалізації голосового управління сьогодні випущені різні бібліотеки серед яких можна виділити наступні [18-19]:

– Pocketsphinx - бібліотека розпізнавання з відкритим вихідним кодом під Android;

– Accord.NET. - бібліотека реалізує алгоритми машинного навчання. Має функції для роботи з голосом;

– System.Speech - бібліотека для розпізнавання і синтезу мови.

Головний модуль голосового управління розпізнає мовні команди, перетворює їх у відповідні сигнали, що передаються системам автомобіля, що

виконує необхідну дію. Як правило, мікрофон може бути вбудований у салонне дзеркало заднього виду, але також можливий варіант з кріпленням у руль (рисунок 1.2) [20].

Але конкретна реалізація залежить від установки: це штатна система або поповнена, адже голосове керування зустрічається в багатьох опціонах. Яскравим прикладом тут є охоронна система Pandora DXL5000 [21]. Її функції з охорони доповнені взаємодією водія та автомобіля на будь-якій відстані за допомогою мобільного телефону. На згадку зберігаються зразки всіх мовних команд. При надходженні усного повідомлення (дзвінок з телефону) шукається збіг. Якщо його не знайдено, спрацьовує охоронне блокування.

Рисунок 1.2 – Вбудований мікрофон з кріпленням у руль [20]

Також можна придбати модуль голосового керування, що не передбачений виробником вашого автомобіля. У цьому випадку перелік пристроїв невеликий, як правило, це стіклопідіймач, двірники, салонне освітлення та зовнішня оптика, люк, центральний замок тощо. Підключення таких систем не завжди вимагає в

автомобілі наявності спеціальної шини, приєднуючись до керованого механізму безпосередньо.

В системі голосового керування, однією з основних функцій є розпізнавання голосу, яка дає змогу, керувати мобільним телефоном, підключеним до неї, користуватися різними можливостями мультимедійної системи, використовувати радіо, навігаційну систему та багато іншого.

Введення голосових команд, набагато скорочують ваш час та керування, це своєю чергою допомагає зосередитися на дорозі та керуванням автомобілем. Також є можливість використовувати голосові команди для взаємодії з навігаційними системами, тобто прокладення або зміни маршруту тощо. Системи голосового керування підтримують різні мови, в тому числі і несильно популярні.

1.3 Дослідження засобів забезпечення надійності голосового керування автомобіля

Технологія розпізнавання голосу дозволяє керувати системою за допомогою голосових команд для забезпечення безпечної роботи з мультимедійною системою чи іншого (за наявності) функціоналу автомобіля під час руху. Але, через технічні обмеження системою голосового керування визначаються не кожні голосові команди. Для того, щоб зменшити ці обмеження, система може зображати лише ті команди, які можуть використовуватися.

При розмові один з одним люди припускаються помилок. Так само і система голосового керування інколи може неправильно зрозуміти задану голосову команду користувачем. Якщо це трапилося, тоді потрібно перевірити екран на наявність доступних варіантів і повторити її, або ввести її вручну на вашому мультимедійному пристрої [22].

Підтримка системи голосового керування залежить від вибраної системної мови. Перед процедурою розпізнавання голосу слід перевірте мову вашого пристрою.

Якщо випадково змінити мову системи голосового керування на ту яка не підтримується виробником вашого автомобіля, вона працювати не буде. Необхідно змінити її власноруч. Команди навігації, виключають в себе: "Пошук за адресою/Пошук точок інтересу/Пошук <Категорія>", та підтримують такі мови: португальську, польську, шведську, турецьку, чеську, данську та норвезьку мови [22]. Переваги та недоліки системи голосового керування автомобілем зображені у таблиці 1.2.

Таблиця 1.2 – Переваги та недоліки системи голосового керування

Переваги	Недоліки
Зручність користування системою та її компонентами.	Не кожна система голосового керування може розпізнати голос користувача.
Не потрібно запам’ятовувати різні комбінації кнопок автомобіля та їхнє розташування керування функціями.	При пошкодженні мікрофона або іншого компонента системи голосового керування, користувач шукатиме відповідну кнопку керування, що приведе до відволікання від дороги.
Можливість виконувати телефонні дзвінки, а також відправляти та прослуховувати голосові повідомлення.	Недосконаліть системи аутентифікації користувача, що приводить до отримання несанкціонованого доступу злочинцями.
Наявність голосових помічників «Siri» та «Google Assistant» у системі голосового керування. За допомогою яких можна прокласти вибраний маршрут, чи знайти заправку, яка знаходиться поблизу.	Наявність шумів, що погіршують розпізнавання системою голосових команд сказаних користувачем.

Керування багатьма функціями можна здійснювати голосом. Для досягнення найкращих результатів у розпізнаванні мови використовувати такі засоби та методи [22]:

– закрийте всі вікна та люк у даху. Якість розпізнавання мови може бути покращена, якщо в автомобілі тихо;

– натисніть кнопку розпізнавання мови та промовте необхідну голосову команду після звукового сигналу;

– мікрофон зазвичай розташований над водієм, тому голосові команди слід вимовляти у звичайному положенні;

– промовляти голосові команди природним чином та чітко, як під час звичайної розмови;

– номери будинків або цифри з телефонної книги слід вимовляти окремо. Наприклад: "Схід два, чотири» і так далі;

– система не враховує спеціальних символів при розпізнаванні контактних імен з телефонної книги, тому їх називати не потрібно;

Залежно від технічних характеристик деякі команди можуть не підтримуватися.

Однак, всі ці недоліки не дуже суттєві й притаманні, як правило, лише неякісним системам голосового управління. Таких проблем легко уникнути, якщо не заощаджувати та придбати якісне обладнання або новий автомобіль з відмінними характеристиками. Голосове керування має дуже великі перспективи на автомобільному ринку, однак ні вітчизняні, ні зарубіжні автомобілі не можуть відчути ”силу слова” [23].

У зв'язку з цим розроблена комп'ютерна система голосового керування і контролю за бортовими функціями автомобіля. Дана система зможе бути інтегрована у звичайний автомобіль і при цьому забезпечувати як і зручність у час поїздки, так і безпека роботи автомобіля.

Сьогодні існують два основних види технологій розпізнавання голосу. Перший це розпізнавання мови, залежне від диктора, коли користувач повинен спочатку навчити систему розпізнати його голос, і тільки після цього система

може функціонувати. Другий – це розпізнавання мови, не залежне від диктора, тобто система здібна розпізнати будь-яку мову, незалежно від того, хто говорить.

Системи розпізнавання мовлення, що залежать від диктора призначені для одного користувача. Інші способи розпізнавання, системи розробляються для будь-якого користувача конкретного типу (наприклад, американський англійський). Це самі складні в розробці і самі дорогі системи, а точність розпізнавання у них нижче. Але ці системи є більш гнучкими [24].

Адаптивні системи адаптуються до характеристик нового диктора. Їхній рівень лежить десь посередині між незалежними та залежними голосовими системами.

Системи розпізнавання ізольованих слів працюють дискретними словами – в даному випадку потрібна пауза між словами. Це сама проста форма розпізнавання, так як досить легко знаходиться кінець сигналу, а слова які виникли не використовують інші слова. Оскільки в цих системах кількість слів постійно, то їх легко проектувати.

Неперервну мову обробляти набагато складніше по різним причинам, по–перше, важко визначити початок і кінець слова. Друга проблема – артикуляція. На звучання кожної фонеми впливає звучання сусідніх фонем, а на початок та кінець слів вливають попередні та наступні слова. Розпізнавання неперервної мови залежить також від швидкості з якою мові працювати складніше [24-25].

Розмір словника системи голосового керування впливає на ступінь складності, вимоги процедурам обробки і точності системи.

Однією системою для роботи необхідно всього кілька слів (наприклад, тільки число), а інші працюють з дуже великими словниками (наприклад, диктофонні машини).

Є ще дві проблеми, об’ємом словників. Перша з них стосується розробки та забезпечення доступу до спеціальних баз даних (словникам): необхідно забезпечити ведення такої бази та можливість оновлення даних для спеціальних груп користувачів різних професій, наприклад в медичній або правовій сфері.

Другою проблемою, є перевірка граматики. Чітких градацій об’єму словника немає, класифікація словників зображена в таблиці 1.3.

Таблиця 1.3 – Класифікація словника системи голосового керування

Види словників	Кількість слів
Словники малого розміру.	Близько десяти слів.
Словники середнього розміру.	Понад сотні слів.
Великі словник.	Більше тисячі слів.
Дуже великі словник.	Десятки тисяч слів.

Головні програми розробляються не тільки для запису продиктованих слів, але і включають функції перевірки та справності структура пропозицій. З вищесказаного системи розпізнавання голосу вимагають величезних ресурсів, включаючи потужність, пам'ять і мережеві можливості

Розпізнавання голосу використовує дві технології:

– цифрової обробки сигналу;

– розпізнавання користувацьких образів.

За допомогою методів цифрової обробки сигналу виконується перетворення, калібрування, очищення та трансформатування акустичного сигналу в цифровий формат даних та інші, що можуть безпосередньо оброблятися за допомоги системи розпізнавання голосу користувача [25].

Це своєю чергою, виконує завдання, що включає фільтрацію шумів сигналу, які примішуються до звуку, коли відбувається передача акустичних сигналів від мікрофону, що приймає або по мережею, чи іншого пристрою користувача..

Методи розпізнавання користувацьких образів використовуються для виділення та розпізнавання по одиничних слів, або пропозицій речення та в деяких (окремих) випадках потрібні для аутентифікації мовлення користувача.

Крім цього, необхідна лінгвістична теорія в основу якої закладено найголовніші концепції та норми виявлення та розпізнавання голосових команд користувача для взаєморозуміння мови системою. Процес розпізнавання голосу системою (рисунок 1.3) проходить в декілька етапів.

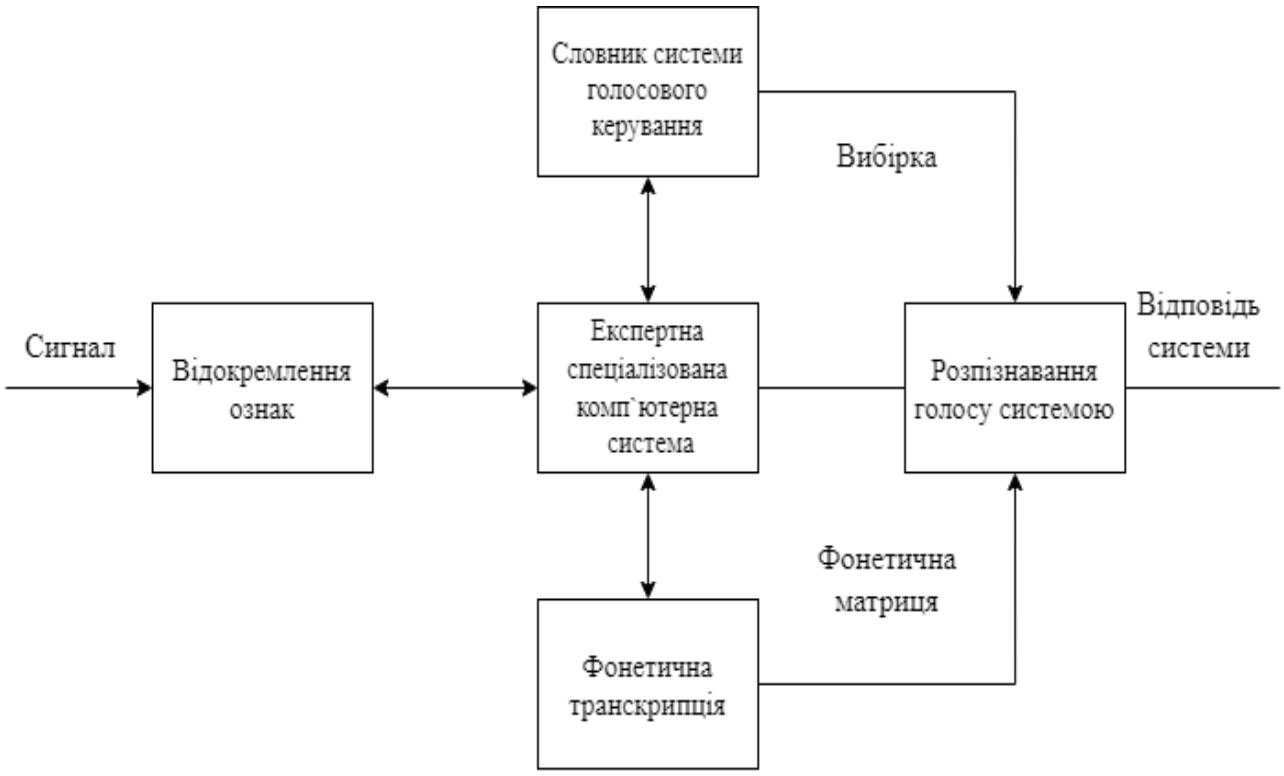


Рисунок 1.3 – Процес розпізнавання голосу

На кожному з етапів для обробки голосового сигналу використовується цілий ряд різних методів. Процес розпізнавання голосу можна розбити на три етапи технології:

– отримання голосового сигналу від користувача та обробка команд;
– розпізнавання фонем та слів;
– розуміння голосової команди.

Розуміння голосової команди саме важке. На цьому етапі послідовності слів (пропозицій) повинні бути перетворені в представлення про те, що хотів би сказати говорючий користувач. Добре відомо, що розуміння голосової команди опирається на величезний обсяг лінгвістичних і культурних знань. Велика частина

системи розпізнавання голосу враховує при цьому знання про природну мову та окремі обставини. Задача, пов'язана з розпізнаванням голосу користувача. Процес автоматичного визначення, «хто говорить» на основі вхідної в голосовому сигналі індивідуальної інформації [25].

У технологічно розвиненому сучасному світі перевага віддається транспортним засобам, для виконання небезпечної та важкої роботи. Хоча раніше транспортними засобами керували лише вручну, сьогодні ними можна керувати голосом і жестами, що є досить популярною практикою. Крім цього, додатково додано датчик виявлення перешкод, щоб зупинити транспортний засіб, коли він зіткнеться з перешкодою. Під час керування транспортним засобом голосові та жестові команди людини вводяться як вхідні дані транспортного засобу [26].

Популярними автомобільними системами, що підтримують голосове керування є «Android Auto» [27] та «Apple CarPlay» [28].

«Android Auto» - це спеціалізована комп’ютерна система, створена компанією «Google» для автомобіля з можливістю голосового керування. Система, дозволяє забезпечувати зв'язок з додатками вашого смартфону та автомобілем, використовуючи голосові команди за допомогою помічника «Google Assistant». При підключенні вашого смартфону, до панелі керування автомобіля, можна побачити обрізану версію свого смартфону з різними додатками які були встановлені [27].

Це допомагає спрости та зробити смартфон безпечним його використання під час керування автомобілем, також це дозволить забезпечити вам використання різного функціоналу голосового керування, наприклад: виконувати телефонні дзвінки та відправляти СМС, користуватися музикою та навігацією.

На сьогодні «Android Auto» доступно не для кожного автомобіля, але має можливість, як і ПЗ в смартфонах на ОС Android, часто оновлюватись. Можна сказати, що часті оновлення, є однією з переваг ПЗ «Android Auto».

На початку 2014 року провідна компанія «Apple» випустила інноваційну систему «CarPlay», яка надає можливість користуватися iPhone підєднавши його до вашого автомобіля та використовувати голосове керування для різних задач.

Раніше система «Apple CarPlay» від «Apple» була доступна лише шанувальникам «Apple», з новими автомобілями, але на сьогоднішній час цілком можливо, налаштувати «Apple CarPlay» у своєму автомобілі. Існує багато додатків, які можна використовувати для отримання функціональності системи «Apple CarPlay» для вашого авто [28].

Система «Apple CarPlay» розміщує голосовий помічник «Siri» на вашому кермі для здійснення голосового керування. Панель керування, досить проста в користування і схожа на операційну систему IOS, вона дозволяє вам взаємодіяти з «iPhone» під час керування автомобілем та виконувати різноманітні функції, включаючи голосове керування.

Проаналізувавши популярність мобільних телефонів, багато виробників автомобілів зараз підтримують «Apple CarPlay» [28] і «Android Auto» [29]. Ці дві системи, дуже схожі, за способом використання. Аудиторія користувачів смартфонів з операційною системою андроїд, сягає майже п’яти мільярдів, саме це робить «Android Auto» одним з найпопулярніших СКС автомобіля для інформаційно-розважальної системи.

1.4 Висновки

У першому розділі було здійснено огляд системи голосового керування автомобілем. Розглянуто концепції та поняття спеціалізованих комп’ютерних систем автомобіля. Проведено аналіз засобів для забезпечення надійності, в результаті якого були сформульовані методи підвищення надійності голосового керування автомобілем. Узагальнено принцип роботи автомобільних систем «Android Auto» та «Apple CarPlay».

1.5 Постановка задачі

Метою кваліфікаційної роботи є визначення методів та засобів забезпечення надійності спеціалізованої комп’ютерної системи голосового керування

автомобілем. Для вирішення цієї задачі необхідно оцінити ефективність використання даних методів в спеціалізованих комп’ютерних системах таких як Android Auto, Apple CarPlay,. Також виявити існуючі небезпеки в користуванні даними СКС голосового керування автомобілем. Провести аналіз відомих характеристик методів та засобів для забезпечення надійності. Виконати моделювання процесу надійності та безпеки в СКС голосового керування автомобілем, провести пошук відомих небезпек та загроз.

2 МОДЕЛЬ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ГОЛОСОВОГО КЕРУВАННЯ АВТОМОБІЛЕМ

2.1 Концепція систем голосового керування автомобілем «Android Auto» та «Apple CarPlay»

«Android Auto» [27] може об’єднати в собі стильний і сучасний інтерфейс (рисунок 2.1). Компанія «Google» спеціальні додатки та програми зі спеціальними заходами безпеки для водія. Система може взаємодіяти з декількома пристроями, які підключені до автомобіля, ця можливість ставить автомобіль в вразливе становище для злодіїв, тому що, забезпечує багато підходів для кібератаки, в тому числі для системи голосового керування.

Рисунок 2.1 – Головне меню інформаційної системи «Android Auto» [27]

«Android Auto» насамперед був призначений для систем, які вже були розроблені виробниками автомобілів, але на сьогодні, встановлення мультимедійної системи з «Android Auto» можливе навіть тоді, коли інформація про нього в офіційному списку підтримки виробника відсутня. Підключення телефону до Android Auto має схожий процес підключення через «Bluetooth» до будь-якого іншого Вам відомого пристрою.

Спочатку, необхідно мати в телефоні доступ до Інтернету. Далі потрібно завантажити програму «Android Auto» на свій телефон з «Google Play», потім запустивши програму, потрібно приєднати телефон через USB та перейти до дисплея системи «Android Auto» вашого автомобіля (рисунок 2.2). Це дає можливість увімкнути новий пристрій і після вибору свого смартфону, необхідно схвалити створення пари в програмі Android Auto на екрані вашого пристрою. Дана процедура підключення виконується один раз, потім з'єднання будуть відбуватися автоматично.

Рисунок 2.2 – Дисплей з підключеним смартфоном до «Android Auto» [27]

В науковій статті [30] були представлені результати взаємодії користувачів зі спеціалізованої комп'ютерною системою «Android Auto». Дослідження перевіряло взаємодію водії з виконанням функцій системи голосового керування

та безпечності їхнього керування на дорозі. Результат дослідження показав, що користування системою «Android Auto» цілком безпечне.

Додаткові програми які доступні для завантаження, в магазині «Google Play», були перевірені. Результати перевірки показують, що майже вісімдесят відсотків додатків потенційно вразливі та можуть бути використанні для заподіювання шкоди, з них двадцять п’ять відсотків створюють загроз безпеки, пов'язані з виконанням «JavaScrip» [31].

Компанія «McAfee» у разом з своїми партнерами опублікували дослідження під назвою «Обережно злочинне програмне забезпечення» [32], в якому вони проаналізували нові загрози та ризики в автомобільній спеціалізованій комп’ютерній системі які є присутні в сучасних автомобілях. В роботах [33-34] надається комплексний підхід для того, щоб показати, що сучасних автомобілях безпека може бути під загрозою через перешкоджання та втручання проходження сигналів Bluetooth та Wi-Fi. В деяких статтях, наприклад [35], проблеми з безпекою та конфіденційністю в системах голосового керування автомобілем вирішуються за допомогою різних криптографічних методів, або використовують різне безпечне середовище розробки [36]. Провівши аналіз цих робіт, можна зробити висновок, що більша частина лише показує проблему, а не вирішує її.

Для розв’язання проблеми безпеки та конфіденційності в спеціалізованій комп’ютерній системі «Android Auto» можна використовувати метод статичного аналізу на основі абстрактної інтерпретації [37], за допомогою цього методу можна виявити загрози програмного забезпечення в спеціалізованій комп’ютерній системі «Android Auto».

На сьогодні існує багато статичних аналізаторів, які можуть аналізувати вихідний код, але більшість із них синтаксичному аналізі і досконало не можуть виявляти вразливості ПЗ. Найбільш досконалим статичним аналізатором є Julia [38], за його допомогою можна виконувати семантичний звуковий аналіз.

Цей аналізатор створений на базі Android API 25 і може працювати в розібраному байт-коді. Коли він знаходить недолік чи вразливість, видається його попередження з деталями.

В роботі [36] представлена концепція платформи автономного автомобіля на «Android Auto», яка надає платформу розробки стороннім користувачам. Для розв’язання проблеми з питання безпеки запропонована розширена схема дизайну автономного транспортного засобу на додатках під назвою «АВАНГАРД». Це своєю чергою зосередить увагу на пом’якшенні загроз при використанні не довіреного коду, методом використання та аналізом програм.

Провівши аналіз, в таблиці 2.1 зображено основні недоліки використання спеціалізованої комп’ютерної системи автомобіля «Android Auto», далі будуть використані засоби та рішення для забезпечення надійності користування цією системою.

Таблиця 2.1 – Недоліки автомобільної системи «Android Auto»

Обмеженість користування.	Компанія обмежує користувачам (водіям), кількість додатків зі смартфона на екрані автомобіля.
Недосконалість голосового керування.	Не чітка вимова заданої команди, може привести до того, що система її просто не зрозуміє і команда не виконається.
Сумісність з телефоном	Система інколи не може підключитися до вашого смартфону через те, що на ньому застаріле ПЗ.
Підключення через USB- кабель	Деякі USB кабелі можуть не підключатися через не якість до “Android Auto”. Також необхідно щоб довжина кабелю була не більше одного метру.

Для розв’язання проблеми з недосконалістю голосового керування потрібно, наскільки це можливо чіткіше вимовляти голосову команду, також необхідно для правильного розуміння її системою, використовувати команди які є

запрограмовані системою, тобто можуть бути підтримані і зрозумілі системі. Для пошуку таких команд необхідно звернутися до технічної підтримки вашої системи. Наприклад система голосового керування не зрозуміє таку команду як: «Потрібно на вулицю Перемоги», для виконання цієї команди потрібно чітко промовити: «Ok, Google/ Прокласти маршрут/ вулиця Перемоги/ будинок 7». Також необхідно зменшити рівень шуму та різних завад які не дозволяють чітко вимовляти голосову команду.

У системі «Apple CarPlay» (рисунок 2.3) є надання кнопки «Siri» на кермі якості голосового помічника. За допомогою «Siri» надається також можливість керування і використання екраном «CarPlay» вашого автомобіля. Також є можливість керувати своїм «IPhone» за допомогою голосового керування «Siri». Голосовий помічник надає можливість використовувати її практично для всього. Наприклад від зображення та прослуховування різноманітних вказівок до записування та надсилання відповідей на повідомлення.

Рисунок 2.3 – Автомобільна система «Apple CarPlay [39]»

Існує можливість використання кнопки «Siri», за допомогою кнопок «Mobile Home» виготовленого компанією «Banco Tech». Цей пристрій можна легко приєднати до свого «IPhone» через канал зв'язку «Bluetooth», а після цього з легкістю користуватися голосовим помічником. На сьогодні цей пристрій доступний лише у США, але компанія виробник може доставити його у будь-яку країну, за певну суму яка може коливатися від 80 до 100 американських доларів.

Наявність підключеного смартфона в автомобілі може принести багато різноманітних переваг наприклад, відтворення музики, використання кількох навігаційних програм. Також важливо не забувати про небезпеки на дорозі і користуватися обережно, тому що використання телефону під час водіння може відволікти.

У роботі [40] сказано, що при взаємодії автомобіля і смартфона, вони обмінюються сервісами та інтерфейсом. Графічний інтерфейс динамічно створюється методом обміну описами інтерфейсу користувача. Послуги в свою чергу підключаються завдяки обміну описами інтерфейсів для кожної (за доступністю) послугою.

На мою думку, система «Apple CarPlay» є одним з найбезпечніших способів використання свого смартфону в автомобілі, що своєю чергою дозволяє зосередитися на дорозі

Далі показано, як саме працює ця система та як її слід використовувати, для того, щоб найкраще відчути функціонал на повну

Система «CarPlay» насамперед дозволяє підключати свій смартфон до автомобіля та показувати спрощений інтерфейс, на дисплеї вашого автомобіля. Це дозволяє отримати доступ до певних програм для використання в автомобілі. «Apple CarPlay» надає можливість ефективно використовувати «Siri», дозволяючи віддавати голосові команди не відволікаючись від дороги.

На сьогоднішній час у багатьох сучасних автомобілів вже розумний інтерфейс йде вбудованим, досить часто він поганий та недосконалий. А саме погана і недосконала технологія голосового помічника для керування, заважає на максимум використовувати його потенціал для голосового керування.

В роботі автор [41] вводить концепцію «Terminal Mode» для інтеграції інтерфейсу смарфону в інтерфейс автомобіля за допомогою протоколу VNC [42]. Це розширення включає також в себе авторизацію додатків, що показуються на смарфонах у віддаленому інтерфейсі користувача.

«Apple CarPlay» сумісний із будь-яким автомобілем, який його підтримує, надаючи інтерфейс, знайомий користувачам смартфонів. Система не замінює оригінальну систему виробника автомобіля. Для повернення до системи замовчування досить натиснути звичайну кнопку. Але порівнюючи з «Android Auto», «Apple CarPlay» не надає можливості користування на екрані смартфону для забезпечення безпеки за кермом, для того, щоб водій зосередився на дорозі.

Наступним кроком показано як саме працює дана система. З системою «CarPlay» можна отримати доступ до основних функцій підтримуваних програм на вашого смартфону. Існують і різні варіанти голосового відтворення музики, прослуховування повідомлень, прокладення маршруту тощо але, вони мають деякі недоліки. Перегляд повідомлення з усіх ваших програм можуть відволікати вас у дорозі. Крім того, маленькі елементи екрана більшості програм не підходять для швидкої взаємодії під час водіння. Система «Apple CarPlay» дозволяє легко керуючи автомобілем відповідати на повідомлення, слухати музику та отримувати інформацію за допомогою голосового помічника «Siri».

Це стало можливим завдяки великим значкам та голосовим командам. Це своєю чергою дозволяє зосередитись на дорозі. Коли смартфон підключений до CarPlay, можна отримувати покрокові інструкції, здійснювати дзвінки, надсилати та отримувати повідомлення, слухати музику та багато іншого.

Для використання «Apple CarPlay» необхідна спеціальна програма. При наявності пристрою, ця функція вже вбудована у ваш смартфон. Можна використовувати його, просто увімкнувши свій смартфон до сумісного автомобіля або стереосистеми.

Після підключення логотип «CarPlay» з'явиться на вашому екрані автомобіля. Потім потрібно натиснути на нього, щоб вийти з інтерфейсу віртуальної машини та запустити «CarPlay».

Далі не потрібно спеціально встановлювати програми «CarPlay». Натомість під час використання цієї функції на вашому iPhone з'являються програми, сумісні з CarPlay.

Система «Apple CarPlay» працює з багатьма програмами, вбудованими в iOS, включаючи телефон, повідомлення, навігацію. Система також може працювати з багатьма сторонніми програмами, такими як «WhatsApp», «Spotify», «iHeart Radio».

Для оптимальної роботи з «Apple CarPlay» потрібен «iPhone 5» або новіший пристрій з операційною системою IOS 7.1 і більше. Також слід переконатися, що в регіоні, що підтримується, для «CarPlay». Для роботи з «Apple CarPlay» потрібно увімкнути «Sir», щоб забезпечити можливість голосового керування автомобілем. Для цього необхідно перейти до меню налаштування, знайти там пункт меню відповідальний за «Siri» і переконатись, що функція включена, і працює. Для безпосереднього доступу до «CarPlay», необхідно завести автомобіль та приєднати смартфон до порту USB за допомогою кабелю Lightning.

Зазвичай порт знаходиться під або панеллю керування. Якщо його не можливо знайти необхідно звернутися до посібника з експлуатації вашого автомобіля.

Якщо «Apple CarPlay» не відкривається після підключення, натисніть на ярлик в системи «CarPlay», що на екрані інформаційної панелі (напряму залежить від виробника). Після першого підключення на екрані розміститься повідомлення про те, що вам потрібно розблокувати свій iPhone. Слід погодитися на вашому телефоні та можна приступати до користування [43].

У iOS 13 і пізніших версіях спочатку показується новий екран панелі задач, на якому поточна карта, голосове керування та різні пропозиції «Siri». Для більш старих версіях набір піктограм програми, аналогічний iOS.

Щоб перейти від панелі керування до програм «CarPlay» необхідно провести пальцем ліворуч. На кожній сторінці показано вісім програм, якщо встановлено більше програм необхідно повернутися. На лівій бічній панелі

системи «Apple CarPlay» показуватися поточний бездротовий сигнал і час, а також швидкі посилання на використані користувачем нещодавні програми.

2.2 Засоби та методи забезпечення надійності автомобільних систем «Android Auto» та «Apple CarPlay»

У роботі [44] сказано, що більша частина систем голосового розпізнавання використовує в собі модульну архітектуру, тобто вона використовує детектор голосу, блок для очищення від шумів і головного модуля який включає алгоритм для розпізнавання голосової команди. Тобто цифровий сигнал спочатку надходить на блок очищення від шуму, де підвищується якість голосової команди завдяки видаленню непотрібних шумів, далі детектор голосу виділяє ділянки, які містять мову, вони своєю чергою перетворюються на набори коефіцієнтів і надходять в голосовий модуль де відбувається розпізнавання голосової моделі.

Провівши аналіз роботи автомобільної системи «Android Auto» [26], можна зробити висновок, що однією з проблем є системи голосового керування - це голосова аутентифікації. Завдяки цій проблемі, злочинці можуть виконувати кібератаки, так звані нечутні ультразвукові команди (DolphinAttak), на системи голосового керування.

Для забезпечення надійності цієї системи можна використовувати метод «Прихованої Марківської моделі» [45]. Існує два способи подання голосового сигналу на пристрій. Вони використовують фонетичний і підхід цілого слова. Метод полягає в ідентифікації динаміка та авторизації його поруч із базою даних голосів. Спочатку система навчається за допомогою певних голосів, далі тестується з невідомим голосом і тоді система розпізнає користувача кому належить невідомий голос. Система розпізнавання ділиться на дві підсистеми, такі як залежні від тексту і незалежні від тексту.

Далі розглянуто проблеми та недоліки які трапляються в системі, та створена модель засобів для забезпечення надійності голосового керування при підключеному смартфоні до автомобіля.

Отже, для використання голосового керування в «Android Auto», потрібно сказати «OK, Google», перед цим звичайно натиснувши кнопку або символ мікрофона на кермі чи на панелі керування автомобіля. Але інколи трапляється, що голосове керування не відповідає, для виправлення і коректної роботи, нижче описана модель процесу використання засобів для підвищення надійності. Отже, необхідно використовувати такі засоби та дії:

– необхідно перевірити чи включені можливості керування, або ж їх взагалі немає. Для цього необхідно перейти у меню смартфона, потім в ньому в налаштуваннях знайти та перейти у розділ «Мова та введення», далі необхідно перейти в під категорію «Голосового вводу Google» і натиснути на «Розпізнавання голосу» і перемістити повзунок в праву сторону. Після виконання даних дій голосове керування в «Android Auto» має запрацювати;

– натиснувши кнопку голосового керування, її потрібно протримати до появи відповідного звукового сигналу. Якщо ж відпустити клавішу раніше, то це значить, що скоріше всього голосове керування в «Android Auto» відключилося і для відновлення роботи, необхідно перезапустити програмне забезпечення;

– також можна провести звукову команду, наявність такого сигналу свідчить про те, що голосове керування автомобілем повністю працює і готове виконувати команди;

– однією з причин несправності голосового керування є також програмний збій. В такому випадку необхідно спробувати просто перезапусти смартфон, чи магнітолу в «Android Auto»;

– зменшити рівень шуму перед подачею голосової команди користувачем;

– переконатись в справності функціонування мікрофону в автомобілі, при необхідності звернутися до майстра для визначення проблеми.

Також автомобільна система «Android Auto» з голосовим керуванням вразливі до інших видів кібератак, наприклад до атаки світловими командами яка виконується шляхом, подання світлової команди на мікрофон системи голосового керування спеціальним пристроєм, для захисту від таких кібератак

використовують апаратні та програмні засоби забезпечення надійності, наприклад тонування вікон автомобіля та інше

Проаналізувавши роботу автомобільної системи «Apple CarPlay» [46], можна зробити висновок, що проблемою голосового помічника часто стає хмарна обробка даних і залежність від якості Інтернет підключення. Отже, для того, щоб забезпечити надійність своєї системи голосового керування потрібне якісне і швидке Інтернет з’єднання. Для цього можна придбати 3G/4G WI-FI розтер (рисунок 2.6) в автомобіль, який забезпечить швидкодію вашої системи з хмарною обробкою даних. Роутер можна підключити в прикурювач автомобіля, до USB порту вашого автомобіля в залежності від вашого вибору та характеристик автомобіля. Але також не слід забувати, що досить часто підключати та налаштовувати пристрої інших виробників неможливо, або вони будуть працювати з обмеженим функціоналом [47].

Рисунок 2.4 – Автомобільний WI-FI розтер з антеною[48]

Якісний та стабільний зв'язок Інтернету також допоможе вирішити, ще один недолік використання голосового керування, а саме неправильне функціонування, різноманітні збої в системі, зв’язані з несвоєчасним обновленням програмного забезпечення. Для розв’язання цієї проблеми необхідно обновляти ваш пристрій до останньої доступної версії ПЗ.

Ще одна досить серйозна проблема яка часто зустрічається з голосовим помічником в системі «Apple CarPlay», полягає в тому, що він може зчитувати голосові команди які йому не призначались, тобто на такі команди які користувач безпосередньо не використовував, або реагувати на різні види шумів, також завдяки шуму система голосового керування може неправильно зрозуміти та виконати сказану вами голосову команду.

Для розв’язання даної проблеми можна скористатися розробкою системи від компанії Bose [49]. Компанія розробила систему «QuietComfort Road Noise Control» яку можна встановити у вашому автомобілі, для зменшення рівня шуму, що забезпечить надійність голосового керування. Система складається з мікрофонів та певної кількості наборів акселераторів, використовуючи акустику, встановлену безпосередньо в самому автомобілі, проводячи фільтрування фонових шумів, система підвищує чіпкість голосових команд та розширяє можливості голосового керування.

Також можна використати метод запропонований у роботі [50] даний метод покращення мовлення інтегрує зображень характеристики, часової області в уніфіковану структуру з використанням мережі GAN, він обробляє хвилі голосової команди та роз’єднує сигнали мови та шуму, що надходять у два одновимірні шари згортки перетворення Фур’є, які зображають форми сигналу у спектрограми мовлення і шуму, які в своєю чергою використовуються для обчислення витрат.

Цей метод перевершує методи для покращення голосових команд, на основі нейронної мережі DNN.

2.3 Процес виявлення та забезпечення надійності голосових помічників Siri та Google Assistant

Безпека за кермом автомобіля повинна бути одним з найважливіших факторів, тому що водій сівши за кермо несе відповідальність не тільки за себе, а насамперед за оточення.

Відволікання уваги водія є основною причиною дорожньо-транспортних пригод і головним винуватцем небезпечних ситуацій є використання смартфону. Фактори, що відвертають увагу можна поділити на різні категорії, але основними є візуальні та слухові.

Для їхнього усунення на сьогодні існує багато різноманітних технологічних рішень. Прикладом є голосовий помічник «Siri» який використовується в спеціалізованій комп'ютерній системі «Apple CarPlay» [46], яку було описано раніше. Цей голосовий помічник потенційно зменшує різні візуальні фактори, що відвертають увагу водія.

На наступній блок - схемі (рисунок 2.5) показано процес використання голосового помічника «Siri» під час керування автомобілем.

На схемі показано, що після взаємодії бортового комп'ютера і людини відбувається метод проектування, потім йде тестування і тестування взаємодії з інтерфейсом, взаємодія з інтерфейсом може відбуватися різними мовами. В свою чергу інформаційна система виконує пошук інформації, виконує оцінювання і показує результат пошуку.

Далі будуть розглянуті методи та засоби для забезпечення надійності в користуванні голосовим помічником «Siri», та різні причини її неполадок.

Інколи система «CarPlay» некоректно зв'язується і з'являється помилка синхронізації. Це своєю чергою обмежує функціональність яка є в ОС і також в самому автомобілі. Помилка синхронізації найчастіше з'являється якщо використовувати одну і ту саму функцію кожний день. Ця проблема напряму зв'язана з голосовим помічником «Siri», для розв'язання цієї проблеми потрібно виконати наступні дії, а саме зайти в налаштування пристрою, далі перейти в

розділ «Siri і пошук», потім необхідно переконатися, що опція зв'язана з «Привіт, Siri», активована. Якщо все правильно система працювати коректно.

Рисунок 2.5 – Блок - схема використання голосового помічника «Siri» під час керування автомобілем

Система «CarPlay», з голосовим керуванням автомобіля за допомоги голосового помічника «Siri», може працювати не належним чином, для того, щоб це виправити потрібно, використати наступні удосконалені засоби, які наведені у таблиці 2.2.

Таблиця 2.2 – Неполадки системи «Apple CarPlay» та засоби вирішення

Несправність системи «Apple CarPlay»	Засоби забезпечення надійності
Недоступність в певній країні чи регіоні.	Необхідно переконатися, що в тій країні чи регіоні, де функція системи «CarPlay» доступна для використання і підтримується, для цього потрібно найти інформацію на сайті підтримки компанії «Apple».
Несумісність з вашим автомобілем.	Ця проблема є досить поширеною, тому що, не всі автомобілі навіть недавніх років випуску можуть підтримувати систему, тому для вирішення потрібно звернутись до компанії виробника.
Функція системи автоматичного запуску «Apple CarPlay» не активується.	Перевірити наявність логотипу системи на дисплеї вашого автомобіля, якщо він відсутній, спробувати перезавантажити смартфон та автомобільну систему.
Відсутність підключення до стерео системи « Apple CarPlay».	При наявності підключення через провід, необхідно спробувати пере підключитися ще раз, але замінивши провід підключення і використати другий роз’їм USB на панелі керування. Якщо використовується безпровідне підключення, слід переконатись, що WI-Fi та Bluetooth включені та працюють.

Кінець таблиці 2.2 – Неполадки системи «Apple CarPlay» та засоби вирішення

Несправність голосового керування систем чи голосового помічника «Siri»	Перевірити автомобіль на підтримку голосового керування, натиснувши кнопку голосових команд на кермі і утримувати її коли промовляєте запит. Більш детально метод описувався у тексті раніше.
Смартфон не визначається системою «Apple CarPlay"	Інколи смартфон не визначається функцією системи «CarPlay», можливо на ньому встановлено обмеження. Для вирішення проблеми необхідно перейти до меню «Налаштування», далі вибрати пункт «Екранний час» та спробувати знайти пункт «Обмеження контенту та конфіденційності» та переконатися, що у підпункті «Дозволені програми» увімкнено функцію «CarPlay».
Застаріла версія ПЗ системи.	Переконатися, що в системі працює з останньою версією ПЗ. При наявності новішої версії ПЗ, виконати оновлення системи.

Одним з недоліків в автомобільній системі «Apple CarPlay» з голосовим помічником «Siri» є механізм голосової аутентифікації, наприклад злочинець може обійти функцію безпеки голосового помічника видавши себе за власника за допомогою атаки світловими командами, цим самим отримати несанкціонований доступ до транспортного засобу. В дослідженні наочно продемонстровано [51], як

можна потайки і віддалено вводити голосові команди зі власноруч створеним голосом, різними способами навіть не привертаючи увагу користувачів.

Для забезпечення надійності можна використати метод динамічного транс форматування часової шкали (DTW) [52]. Даний метод дозволяє знаходити близькість, для двох послідовностей вимірювання, в певний проміжок часу. Його можна використовувати для розпізнавання голосової команди, якщо два мовленнєвих сигнали представляють однакову вихідну голосову команду, навіть з різною швидкістю і довжиною. Однією з переваг даного методу є простота в реалізації.

Також для розв'язання цієї проблеми у роботі [53] запропонована система «VAuth», яка може забезпечувати захист від різних типів кібератак на голосовий помічник, наприклад атаки з повтореннями, імітацією голосу іншого користувача. Система забезпечує безперервну аутентифікацію для голосових помічників, в тому числі системи «Apple CarPlay» з голосовим помічником «Siri», система збирає вібрації користувача та порівнює їх з голосовою командою отриманою з мікрофона голосового помічника, далі їх аналізує і виконує команду лише яка збігається з голосом власника пристрою.

Система «Apple CarPlay» як і «Android Auto», також вразлива до кібератак, таких як атака світловими командами. Далі на прикладі моделі загрози показано як сама відбувається така атака.

Мета злодія полягає в тому щоб, дистанційно ввести команди які несуть певну загрозу, для пристрою користувача, використовуючи спеціальний пристрій (лазер). Наприклад злочинець не має фізичного доступу до пристрою користувача, отже він не може змінювати недоступні голосом налаштування, але він може отримати за допомогою введення світлових команд віддалений доступ цільового пристрою та його мікрофону. Також слід звернути увагу на те, що віддалений доступ до цільового пристрою, надає можливість слідкувати за світлодіодними індикаторами пристрою, це в своєю чергою показує йому як вони реагують (загоряються) після розпізнання голосової команди та дозволяє

дистанційно використовувати як зворотний зв'язок, для визначення успішності спроби атаки.

Для підвищення надійності пристрою голосового керування в автомобілі як захист можна використовувати як апаратні, так і програмні засоби захисту.

Виходячи з пункту про «Android Auto» [27], можна зробити висновок та аналіз, що система використовує голосовий помічник «Google Assistant» в спеціальному режимі «На автомобілі», це надає можливості використовувати різні функції та дії, в тому числі з голосовим керуванням за кермом автомобіля. Цей режим дозволяє, телефонувати, надсилати СМС повідомлення, керувати відтворенням мультимедії за допомогою голосових команд не відволікаючись від дороги.

Даний режим дозволить налаштувати, автоматичний запуск навігації в «Google Maps», його можна увімкнути на будь-якому пристрої, але не слід забувати, що пристрій має підтримуватись. Щоб режим «На автомобілі» працював коректно та мати можливість отримувати різноманітні сповіщення, коли телефон приєднано через Bluetooth, необхідно слідкувати за оновленнями. Для того, щоб прокласти маршрут (рисунок 2.6) за допомогою голосового керування, необхідно промовити “ОК, Google прокласти маршрут до (необхідно назвати пункт призначення куди прямувати)” [54].

Рисунок 2.6 – Прокладання маршруту за допомогою «Google Assistant» [55]

Окрім прокладання маршруту в «Google Assistant» у режимі «На автомобілі» також можна виконувати різні команди за допомогою голосового керування, показані в таблиці 2.3, для їхнього використання необхідно сказати «Ok, Google» або натисніть на мікрофон, що знаходиться зазвичай на кермі, перед тим, як почати говорити.

Таблиця 2.3 – Реалізація функції та можливостей голосового помічника «Google Assistant»

Функції голосового помічника:	Голосова команда яку потрібно промовити користувачу:
Здійснення дзвінка:	«ОК, Google набери номер» або «подзвони (ім'я контакту)»;
Відповідь на дзвінок:	Голосовий помічник «Google Assistant» попередить Вас, промовивши: «Вам телефонують (ім'я контакту), бажаєте відповісти?" Необхідно відповісти: «Так» або «Прийняти виклик»;
Надіслати (СМС) повідомлення:	«ОК, Google, надіслати повідомлення (ім'я контакту)» або «Надіслати SMS»;
Прочитати отримане повідомлення:	Потрібно промовити:«ОК, Google, прочитай повідомлення»;
Включати музику в автомобілі:	«ОК, Google увімкни музику (ім'я виконавця або назва пісні)» чи «ОК, Google увімкни (жанр)».

2.4 Модель загрози та основи методу виявлення та захисту системи голосової аутентифікації від сучасних способів кібератак

На сьогодні голосові помічники «Siri» від компанії «Apple», чи «Google Assistant» компанії «Google», які використовуються для голосового керування в системах «Apple CarPlay» [27] і «Android Auto»[28] відповідно, стають популярним методом взаємодії людини з автомобілем за допомогою голосового керування. З появою даних систем також з’явилася необхідність забезпечення захисту для них. Як було описано раніше ці системи мають спільну вразливість для системи голосової аутентифікації.

Далі розібрано один з найпопулярніших методів кібератаки на систему голосової аутентифікації на прикладі кібератаки «DolphinAttack» для СКС голосового керування для пошуку методів та засобів забезпечення їхньої надійності

Отже, кібератака «DolphinAttack» - це термін, який був наданий методом доступу для смартфону чи іншого пристрою без згоди користувача шляхом виконання ультразвукових команд [56]. «DolphinAttack» може модулювати голосові команди на ультразвуку який людина відчути не зможе, їх діапазон складає менше 20 кГц, використовуючи ці модульовані низькочастотні аудіо команди можна виконувати різні дії, а найважливіше їх можна інтерпретувати за допомогою голосового розпізнавання системи.

Наступний крок, це проведення аналізу, як саме працює кібератака на системах голосового керування «Google Assistant» та «Siri» методом введення ультразвукових команд, для перевірки можливостей корегування навігаційних систем автомобіля, здійснення викликів, посилання повідомлень та іншого.

На цей час новітні технології голосового керування стрімко розвиваються. На рисунку 2.7 видно як працює СГК і надає можливість використовувати ПЗ автомобілів та інших пристроїв, для визначення промовлених голосових команд людиною для подальшого перетворення їх в зрозумілі для СКС формати. Це в свою чергу набуває великої популярності через те, що механізми мають високу

ефективність і з кожним роком набувають високої точності розпізнавання голосу, і дозволяють користувачам чітко ставити команди для їхнього виконання.

Системи з голосовим керуванням «Apple CarPlay»[27] і «Android Auto»[28] використовують широкий спектр різних команд та функцій, детальніше було описано у розділі 2, див. 2.1. Виробники цих систем докладають багато зусиль для їхнього захисту від кібератак та зловмисників.

Рисунок 2.7 – Схема СГК з прийому голосових команд та подальшого їхнього виконання

Хоч ці системи є надійними, проте вони є недосконалими і тому за допомогою прихованих голосових команд, які незрозумілі звичайним користувачам, але зрозумілі системі та інтерпретуються нею як командами можуть піддаватися кібератаці [57].

Основна більшість цифрових пристроїв які мають підтримку аудіо форматів приймають частоти дискретизації звуку менше ніж 44 кГц і застосовують низькі частоти фільтрів для знешкодження сигналів 20 кГц [58].

Для того, щоб зрозуміти як звук який не чути людині може бути зрозумілим для систем розпізнавання мови, необхідно врахувати, що навіть коли ультразвук приймається і правильно реалізується апаратним компонентами, СРМ не може

розпізнати сигнали, які не відповідають тональності користувача, і в такому випадку команди не можуть бути інтерпретовані.

Одним з кроків для реалізації порушення безпеки систем голосового керування це є їхня активація. Інколи СКГ використовують функцію аутентифікації користувача, це означає, що їх можна активувати за допомогою певних слів. Користувач може вважати, що випадкова голосова команда не зможе пройти розпізнавання голосу, але це не є зовсім так просто. Для того, щоб краще зрозуміти принцип кібератаки ультразвуковими (нечутними) командами використовуємо наступну модель загрози.

Ціль злочинця — вводити голосові команди в системи голосового керування, без відома власників та виконувати різні дії, що можуть нашкодити користувачеві системи. Допустимо, що злочинці не мають прямого доступу до цільового пристрою, власного обладнання, яке передає акустичні сигнали та не можуть вимагати від користувача виконання будь-яких завдань. В таблиці 2.4 описано ситуації та можливі наслідки для виконання кібератаки.

Таблиця 2.4 – Ситуації та можливі наслідки для виконання кібератаки

Можлива ситуація	Аналіз ситуації
Атакувальне обладнання.	Допустимо, що злочинці можуть придбати як колонки, призначені для передачі ультразвуку, так і товарні пристрої для відтворення звукових сигналів. Атакуючий динамік знаходиться поблизу системи голосового керування цільового пристроїв. Наприклад, злочинець може таємно залишити динамік з дистанційним керуванням під автомобілем.

Кінець таблиці 2.4 – Ситуації та можливі наслідки для виконання кібератаки

Немає доступу до цільового пристрою користувача.	Допустимо, що злочинець може націлюватися на систему голосового керування, на свій вибір, але вона не має прямого доступу до цільових пристрої та не може фізично доторкнутися до них, змінити налаштування пристрою чи встановити зловмисне програмне забезпечення. Проте допустимо, що система повністю обізнана з характеристиками цільових пристроїв. Такі знання можна отримати, спочатку придбавши модель пристрою, а потім проаналізувавши пристрій тієї ж моделі перед запуском атак.
Немає взаємодії з користувача.	Допустимо, що цільові пристрої системи можуть перебувати поблизу користувача, але можуть не використовуватися і не привертати уваги. Крім того, система голосового керування може залишатися без нагляду, що може статися, коли користувач тимчасово відсутній (наприклад, залишивши автомобіль та піти по справах). Тим не менш, злочинець не може вимагати від користувача виконання команди активації.

Нехай можливість реалізації загрози розраховується за формулою:

$$M = \frac{M_1 + M_2}{20}, \quad (2.1)$$

де M_1 – числовий коефіцієнт на основі степеню вихідної захищеності;

M_2 – числовий коефіцієнт на основі ймовірної оцінки реалізації конкретної загрози безпеки для даної системи голосового керування.

Тоді можливість реалізації загрози буде вважатися:

– низькою, якщо $0 \leq M \leq 0.3$;

– середньою, якщо $0.3 \leq M \leq 0.6$;

– висока, якщо $0.6 \leq M \leq 0.8$;

– дуже висока, якщо $0.8 \leq M$.

Приклад розрахунку загроз кібератаки на основі введення ультразвукових голосових команд наведено у таблиці 2.5

Таблиця 2.5 – Розрахунок загроз кібератаки на основі введення ультразвукових голосових команд

Загроза	Вихідна захищеність	Ймовірна оцінка	Вірогідність реалізації загрози
Введення фальшивої інформації.	Низька	Середня	Висока
Відвідування шкідливих сайтів.	Низька	Низька	Середня
Здійснення збоїв в обслуговуванні автомобіля.	Низька	Висока	Дуже висока
Проведення шпигунства.	Низька	Висока	Дуже висока

Проблеми з голосовою аутентифікацією у розділі 2, див. 2.2 і 2.3, в системах голосового керування «Android Auto[26]» та «Apple CarPlay[42]», крім кібератак на основі введення нечутних (ультразвукових) команд для систем голосового керування, також дають можливість проведення атак з введенням сигналу на мікрофони пристроїв користувачів методом перетворення світла у звук. У роботі [58] показано, що атака за допомогою світлових команд підтверджує феномен оптичного зв'язку мікрофона голосової системи керування. Тобто після того, як оптичні сили, що перевищує певний поріг, аналогова вхідна напруга мікрофону має лінійну позитивну кореляцію з інтенсивністю світла.

Це своєю черго означає, що мікрофон системи голосового керування, може перетворювати оптичний сигнал атаки в електричний, так само як і звуковий, отже злочинцем можуть бути введені певні шкідливі команди в цільовий мікрофон методом модуляції інтенсивності лазера. Для вдалої світлової атаки командами, потрібно забезпечити ефективний світловий шлях, тобто, щоб лазерний промінь попадав прямо на порт мікрофону і був під невеликим кутом.

Також у роботі [58] сказано, що атака світловими командами – це новий клас атак введення сигналу, який базується на фото акустичному ефекті, а це означає, що мікрофон який використовує система голосового керування автомобілем має можливість перетворювати світло у звук, за допомогою амплітудної модуляції світла при введенні голосової команди на мікрофони. Він своєю чергою може виводити вихідну голосову команду, коли фактичний акустичний сигнал не приймається. Атаки за допомогою світлових команд можуть проходити на далекі відстані, та проникати через вікна автомобіля, навіть якщо вони за тоновані.

Після вдалої атаки світловими командами, злочинець може отримати доступ до різних даних з можливістю їхнього пошкодження, розголошувати конференційну інформацію, маніпулювати системою ідентифікації, встановлювати шкідливе програмне забезпечення, прослуховувати або перехоплювати дзвінки, встановлювати шкідливе програмне забезпечення та інше.

Для проведення атаки світловими командами, необхідний спеціальний пристрій (рисунок 2.8), який може випромінювати промінь світла і мати малий діаметр на великих дистанціях з можливістю фокусування в тісному місці.

Рисунок 2.8 – Спеціальний пристрій (лазер) для проведення атаки світловими командами [59]

Для дослідження атаки світловими командами у роботі [59] використовують лазерні діоди, тому що інтенсивність світла яка випромінюється лазерним діодом, пропорційна струму дії діоду, завдяки цьому можна легко проводити кодування аналогових сигналів через інтенсивність променя лазера за допомогою драйверу амплітудної модуляції.

2.5 Висновки

Проведено аналіз зарубіжних аналогів систем голосового керування автомобілем «Apple CarPlay» та «Android Auto». Проведено аналіз недоліків та

уразливостей систем голосового керування, в результаті якого були сформульовані основні загрози для системи голосової аутентифікації автомобіля. Розроблено модель виявлення небезпек сучасних способів кібератак на системи голосового керування автомобілем. Удосконалено засоби забезпечення надійності голосових помічників «Siri» та «Google Assistant» автомобільних систем, а саме вирішено проблеми з відмовою та коректністю роботи, недоступністю в регіоні використання та несправністю голосового керування

3 АЛГОРИТМИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ВІД СУЧАСНИХ СПОСОБІВ КІБЕРАТАК НА СИСТЕМИ ГОЛОСОВОГО КЕРУВАННЯ АВТОМОБІЛЯ

3.1 Дослідження та оцінка впливу кібератак ультразвуковими та світловими командами

За допомогою кібератаки ультразвукових команд або «DolphinAttack» [56], можна послати голосову команду яку звичайний користувач не почує, але аудіо приймач пристрою який піддався кібератаці її зрозуміє. Можна зробити висновок, що за допомогою кібератаки «DolphinAttack» можна реалізувати кібератаку на системи голосового керування та СРМ.

Існує загально прийняте рішення, що за допомогою ультразвукових команд, злодії можуть тільки пробувати маніпулювати системам розпізнавання голосу, а також легко можуть виявити себе, але насправді завдяки кібератаці «DolphinAttack» можна виконувати різні типи кібератак в тому числі на СКС голосового керування автомобілем, за допомогою ультразвукових голосових команд. Їхні приклади наведені в таблиці 3.1.

Таблиця 3.1 – Можливості кібератак ультразвуковими командами та їхні наслідки

Ультразвукова кібератака:	Наслідки вдалої кібератаки:
введення фальшивої інформації;	Можливість на пристрої жертви, надсилати фальшиві текстові повідомлення, змінювати маршрути навігатора, додавати різні події в календар та інше;
відвідування сайтів;	СКС автоматично відкриває шкідливі сайти, з небезпечними файлами;

Кінець таблиці 3.1 – Можливості кібератак ультразвуковими командами та їхні наслідки

проведення шпигунства;	Зловмисник може прослуховувати телефонні дзвінки користувача, стежити за його маршрутом, віддалено читати повідомлення, та використовувати відео файли, користуватися конференційною інформацією;
здійснення збоїв в обслуговуванні автомобіля;	Можливість віддаленого керування різних режимів пристроїв (автомобіля), в тому числі їхнього повного або часткового відключення чи виведення з ладу.

Провівши аналіз можна зробити висновок, що злодії можуть використовувати кібератаки за допомогою ультразвукових послідовних команд на спеціалізовані комп'ютерні системи різних цифрових пристроїв з підтримкою систем голосового керування (автомобілів), та виконувати різні шкідливі команди описані в таблиці 3.1 та інші. Також в кібератаці «DolphinAttack» можуть використовуватися для найсучасніших і на думку користувачів найбезпечніших системах.

Для визначення методів та засобів забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобіля в тому числі та захисту від кібератаки «DolphinAttack», потрібно більш детально розібрати систему голосового керування, та її компоненти, далі виконаємо кількісну оцінку впливу різних факторів на СГК і розглянемо методи захисту від даної кібератаки.

У розділі 1, див. 1.2, раніше було описано загальний принцип робити СКС голосового керування автомобілем, далі будемо більш детально розбирати роботу основних підсистем.

Система голосового керування складається з трьох головних підсистем, таких як захоплення мовлення, виконання заданих команд і розпізнавання голосу. Захоплення мовлення записує вхідні голосові команди, далі вони передаються на підсистему розпізнавання голосу далі цифрові сигнали, спочатку обробляються, для того, щоб вилучити частоти, які не підходять для звукового діапазону. Потім оброблені сигнали попадають в систему розпізнавання голосу.

В більшості система розпізнавання голосу працює у двох режимах. У режимі активації система не може приймати будь-яку голосову команду, але чекає на активацію спеціального слова або натиснення кнопки.

Наприклад в спеціалізованій комп'ютерній системі голосового керування автомобілем «Apple CarPlay» [27], необхідно натиснути спеціальну кнопку на кермі [28] або промовити «Привіт, Siri». Після активації система голосового керування, підходить до розпізнавання команди та використовує спеціальні алгоритми задані ПЗ для перетворення вказаної голосової команди на зрозумілу пристрою.

Необхідно розуміти, що система голосового керування яка залежить напряму від мовника, виконується локально, а не залежна СГК виконується через хмарний сервіс [60].

Коли користувач використовує хмарний сервіс, сигнали які були попередньо оброблені, направляються на сервери, де ці сигнали будуть розпізнані за допомогою машинних алгоритмів. Якщо СКС розпізнає команду, вона запустить програму для того, щоб виконати операцію. Всі команди та дії є залежними від системи та визначені.

Спеціалізовані комп'ютерні системи голосового керування автомобілем мають великий набір функцій та голосових команд як є доволі важкими для активації. Більшість досліджень безпеки для систем голосового керування зосереджуються на кібератаках, алгоритмах розпізнавання голосу, або шкідливому програмному забезпеченні [61].

Наступним кроком для визначення методів та засобів забезпечення надійності СКС побудуємо модель загрози.

Основна мета злодія полягає в тому, щоб вводити голосові команди, в системи голосового керування без відома власника для спричинення певної шкоди користувачу. Оскільки злодій не має повного доступу до основного пристрою який передає акустичні сигнали, він може вибирати будь-які системи голосового керування на свій розсуд і можливості. Хоч ці системи не можуть встановлювати шкідливе програмне забезпечення, але вони можуть містити інформацію про характеристики пристрою для аналізу та підготовки перед атакою.

Для вдалої кібератаки необхідне спеціальне обладнання, для цього злодій може використовувати пристрої для передачі ультразвуку або для відтворення різних звукових сигналів. Наприклад можна залишити пристрій поблизу, або прикріпити його під автомобіль жертви та віддалено передавати відповідний сигнал. На рисунку 3.1 зображена схема модулів передавача для здійснення кібератак ультразвуковими командами.

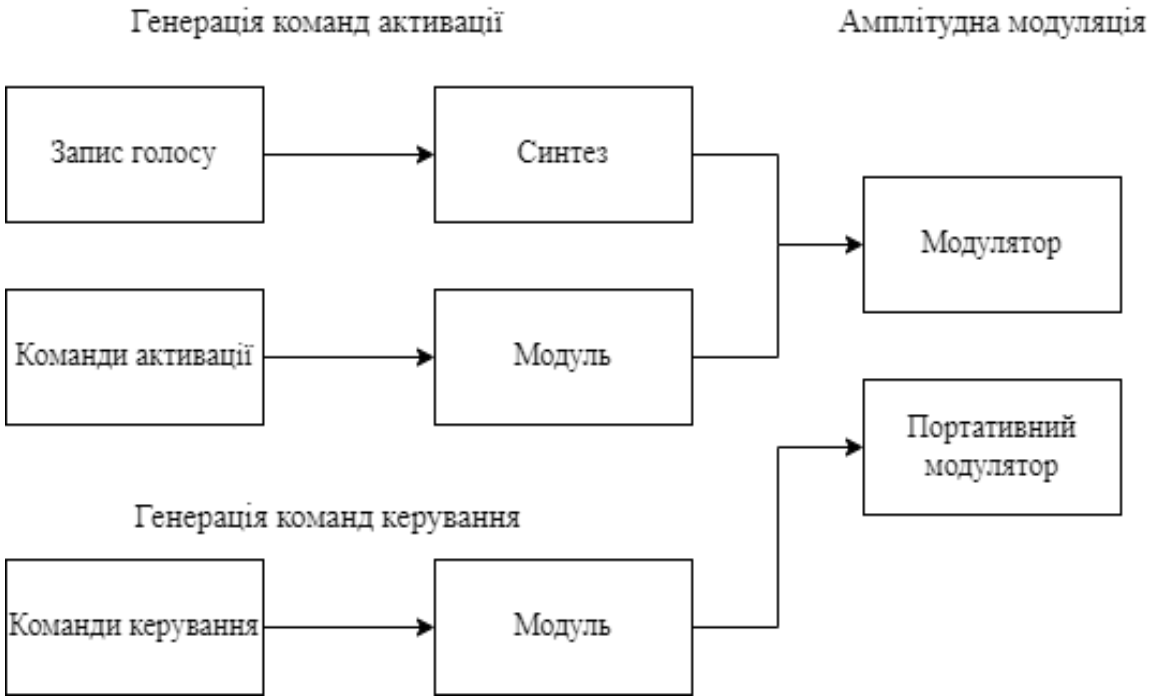


Рисунок 3.1 – Архітектурна схема модулів передавача

Як раніше було сказано, що основна мета це вводити голосові команди які важко виявити, найкраще для цього підходять, звуки які людське вухо не може відчути, тобто ультразвук його діапазону менш як 20 кГц.

В «DolphinAttack» використовуються голосові команди які не чути для керування системою голосового керування. Зазвичай злодій мало може контролювати СГК, успішність кібератаки полягає у створенні ультразвукових голосових команд на атакувальний передавач.

Отже, в цих кібератаках мають генеруватися сигнали для основної смуги голосових команд як для фази розпізнавання системи голосового керування, так і для активації, модулювати сигнали основної смуги, для того, щоб мати можливість ефективно де модулювати на систему голосового керування та проектувати їх на передавач, котрий зможе запускати «DolphinAttack» у будь-якому доступному місці.

Для того, щоб отримати доступ до контролю системи голосового керування, кібератака «DolphinAttack» повинно згенерувати команди активації, перед загальним введенням голосових команд керування. Далі на прикладі голосового помічника «Siri» який працює в «Apple CarPlay» [28], як саме відбувається генерація голосових команд.

Голосовий помічник «Siri» працює у двох режимах, а саме активації та розпізнавання. Перед тим як виконувати голосові команди його потрібно активувати, таким чином слід генерувати два види голосових команд, для активації та основні команди керування.

Активація вважається успішною, якщо голосова команда задовольняє вимоги: має слова пробудження «Привіт, Siri» та імітує голос користувача під який голосовий помічник був навчений. Для злочинця створення команди активації є досить складним, якщо звичайно у нього немає можливості зробити запис слів активації користувача.

Генерація певного голосу в «Привіт, Siri» з використанням чинних методів мовлення та функцій, витягнутих із записів, надзвичайно важко, а інколи взагалі не можливо, через те, що незрозуміло, який саме набір функцій потрібно для

голосової ідентифікації [62]. Тому можна використати два методи для створення команд активації для голосового помічника.

Перший метод використовує синтез мови, для перероблення тексту в голос, отже навіть якщо злочинець не має доступу для запису голосу користувача, він може спробувати згенерувати певний набір команд активації, це зв'язано з тим, що два користувачі з однаковими темпами голосу, можуть активувати «Siri» голосовою командою.

В «DolphinAttack» можуть використовуватися різні набори активації голосових команд, з різною тональністю голосу, за допомогою систем синтезу мовлення.

Другий метод використовується коли злочинець, має можливість записати слова чи словосполучення користувача, з можливістю подальшого їх розбиття на фонеми та з'єднування їх в різні слова, в тому числі і необхідні для активації.

Після проходження активації злочинець, може мати доступ до загальних команд голосового керування. з'являється можливість вибирати текст команди керування та створювати її за допомогою систем синтезу мови. Система розпізнавання голосу не перевіряє ідентичність команд керування.

Для забезпечення надійності голосового керування автомобілем, від ультразвукової (нечутної) кібератаки, застосовуємо новий метод захисту, що використовує апаратні компоненти та містити пристрій для подальшого використання, для більшого розуміння методу використаємо модель загрози у розділі 2, див. 2.4.

Як раніше було у розділі 2, див. 2.2 і 2.3. у спеціалізованих комп'ютерних системах голосового керування «Android Auto» [27] та «Apple Car Play» [28], є недоліки з голосовою аутентифікацією. Тобто злочинцю для вдалої кібератаки (DolphinAttack) спочатку потрібно віддалено послати нечутний (ультразвуковий) сигнал пробудження системи.

Такий сигнал, злочинець може отримати за допомогою запису голосу користувача, на пристрій якого направлена кібератака, для подальшого розбиття

сигналу на слова які необхідні для активації. Запропонований метод допоможе підвищити захист системи, на першому етапі підготовки для вдалої кібератаки.

Суть методу полягає у зниженні можливості злочинцю отримати запис голосу користувача. Для цього потрібно використати ультразвуковий блокатор запису для мікрофонів (рисунок 3.2).

Рисунок 3.2 – Ультразвуковий блокатор записів [63]

Сьогодні існує багато різних видів ультразвукових блокаторі запису, які мають різні характеристики та можливості. Для прикладу пристрій зображений на рисунку 3.2, може придушувати функцію запису для мікрофонів, на відстані до семи метрів, та з можливістю збільшення діапазону та ефективності при використанні зовнішніх додаткових ультразвукових динаміків.

Далі на рисунку 3.3, показано використання ультразвукового блокатора за допомогою алгоритму роботи даного пристрою.

За своїми розмірами пристрій досить невеликий та комфортний, а головне непомітний, що дає зручність встановлення в автомобільному салоні чи в будь-якому іншому місці.

Принцип роботи полягає в тому, що ультразвуковий блокатор запису, використовує подавляючий ультразвуковий сигнал, для виконання процесу глушіння сигналу мікрофону пристрою, що виконує запис. Після цього запис мікрофону неможливо, або досить важко буде розібрати.

Рисунок 3.3 – Алгоритм роботи ультразвукового блокатора записів

Наступним кроком, для успішної кібератаки на СГК є модуляція голосових команд. Після того як успішно згенерувалися основні сигнали голосових команд, їх потрібно модулювати на носіях (ультразвукових) так, щоб користувач їх не чув. Для цього використовується не лінійність мікрофонів.

Для її використання, «DolphinAttack» повинна використовуватися амплітудна модуляція. В кібератаці потрібно вибрати параметр коефіцієнту модуляції, оскільки він безпосередньо зв’язаний з ефектом не лінійності мікрофонів та їхнього подальшого використання.

Передавач голосових команд (ПГК) який використовується в «Dolphin Attack» для створення шкідливих дій в СКС голосового керування автомобілем, зазвичай повинен складатися з декількох компонентів. Далі наведено приклад найпростішого, але за функціоналом він нічим не є, гіршим за інші (рисунок 3.4). Отже, ПГК складається з таких компонентів як: джерела сигналу, динаміка, модулятора та підсилювача.

Джерело сигналу виробляє основні сигнали вихідних голосових команд, динамік в своєю чергою перетворює модульований сигнал, в хвилі, а модулятор модулює голосовий сигнал в хвилі.

Рисунок 3.4 – Блок-схема передавача голосових команд для здійснення «DolphinAttak»

Атака світловими командами відбувається прямо пропорційно на мікрофон. Він являє собою інтегровану реалізацію механічних компонентів на кристалі або чіпу. Завдяки такій будові він має невеликі розміри, має високу ефективність, та є досить дешевим та простим у використанні.

Такі мікрофони використовуються в смартфонах, автомобілях, та в іншій техніці, якій потрібне голосове керування [64]. На рисунку 3.5 зображена структурна схема роботи типового мікрофона.

Рисунок 3.5 – Структурна схема мікрофона

Зазвичай звичайний мікрофон складається з інтегральної схеми спеціального призначення ASIC та діафрагми, яка є тонкою мембраною, що вібрує даючи відповідь на акустичну хвилю.

Принцип роботи мікрофона полягає у тому що, діафрагма разом з нерухомою задньою панеллю пристрою виконує роль конденсатора з паралельними пластинами, в якому через механічні деформації змінюється ємність, коли діафрагма реагує на акустичний тиск. Далі схема ASIC, перетворює ємнісну зміну в сигнал напруги на виході мікрофону.

Для успішної атаки світловими командами необхідно визначити вимоги та критерії для атакуючого пристрою (лазеру). У таблиці 3.2 зображено вимоги до потужності лазера та критерії для проведення успішної атаки світловими командами.

Таблиця 3.2 – Вимоги та критерії для атакуючого пристрою (лазеру)

Вимоги та критерії	Способи реалізації
Вибір команди.	Потрібно визначити та вибрати, голосові команди, які можуть виконуватися системою голосового керування автомобілем.
Виконання генерації команд.	Потрібно створити аудіо записи вибраних команд для системи голосового керування, та додати до них команди активації.
Перевірка успішного введення світлової команди.	Перевірити вимоги для деяких команд, що використовують при підключенні до облікового запису, для правильного виконання в системі.
Налаштування голосу та безпеки.	Виконати налаштування конфігурації пристрою, визначити необхідну мінімальну потужність.

Кінець таблиці 3.2 – Вимоги та критерії для атакуючого пристрою (лазеру)

Експериментальне встановлення.	Направити лазерний промінь на порт мікрофону системи голосового керування, виконати фокусування променя лазера, щоб точно розмістити його на мікрофоні.

Отже, після дотримання та виконання всіх вимог та критеріїв, можна переходити до генерації команд, для подальшого виконання атаки. Для генерації команд можна використати запис голосу користувача, або скористатися спеціальним програмним забезпеченням для перетворення тексту в голосову команду, детальніше було описано у розділі 3, див. 3.1.

Сигнал атаки світловими командам надходить на перетворювач напруги в струм та використовуючи фото-акустичний ефект мікрофону, перетворений сигнал попадає на вхід мікрофону пристрою користувача, що знаходиться на звуковій карті. Далі за допомогою аналогово-цифрового перетворювача (АЦП), голосова команда перетворюється в текстову команду. На виході текстова команда використовуючи цифро-аналоговий перетворювач (ЦАП), формується в голосову команду та надходить на звукову карту пристрою користувача, що був атакований. Звукова карта передає сигнал голосової команди на аудіо вихід.

Для успішної атаки на системи голосового керування, потужність атакуючого пристрою (лазера), повинна бути не менше 60 мВт, цієї потужності достатньо для керування багатьма популярними в тому числі і автомобільними системами з голосовою активацією. Атаки світловими командами можуть проводитися на великі відстані, незалежно від прозорих вікон та іншого.

На рисунку 3.6 зображено структурна схема процесу виконання атаки світловими командами на систему голосового керування автомобілем. Після успішної світлової атаки на прикладі систем голосового керування, злодій зможе отримати доступ різних мультимедійних та навігаційних функцій автомобіля, отримання конференційної інформації користувача та інше.

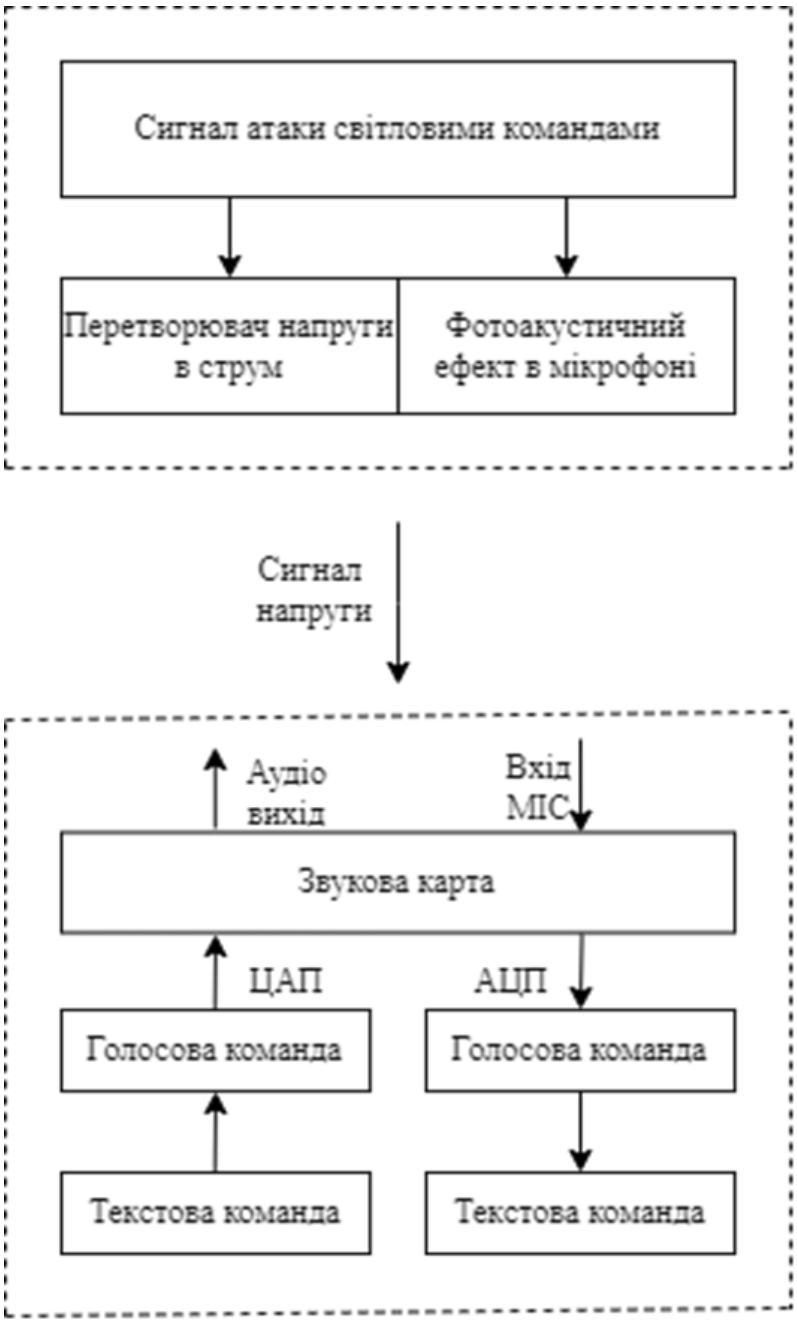


Рисунок 3.6 – Структурна схема процесу атаки світловими командами

3.2 Апаратні та програмні засоби захисту системи голосового керування від кібератак на основі ультразвукових та світлових команд

Наступним кроком оцінимо продуктивності впливу «DolphinAttack» на різні фактори методів та засобів захисту від них.

Для кібератаки, швидкість розпізнання різних видів мови голосових команд не буде відрізнятися. Голосові помічники такі як «Siri» чи «Google Assistant» в системах голосового керування автомобілем рекомендовано використовувати з мінімальним впливом фонового шуту, тому що СГК є чутливими та це може привести до неправильного аналізу та виконання голосової команди заданої користувачем.

Оскільки кібератака виконується дистанційно при збільшенні відстані збільшується і рівень фонових шумів, як раніше було описано - це може призвести до неправильного розпізнавання голосової команди.

Дистанція також впливає на швидкість розпізнавання. Оскільки швидкість розпізнавання голосової команди активації є більша через те, що вона має в собі меншу кількість слів, ніж команда керування, вона виконається швидше. Наприклад якщо виконати голосову команду активації «Привіт, Siri» і голосову команду керування «Siri, Проклади маршрут з точки А до точки Б» на однаковій відстані, в «DolphinAttack» швидкість виконання першої команди більша ніж другої.

Далі будуть оцінені методи та засоби захисту в кібератаки на систему голосового керування. Для захисту можна використовувати як апаратні, так і програмні методи.

Апаратний захист полягає в покращенні мікрофону СГК та його характеристик. Основна причина вдалої кібератаки в тому, що мікрофон може сприймати акустичні команди з частотою вище 20 кГц, хоча в ідеалі він не повинен.

В основному більшість мікрофонів допускають сигнали вище 20 кГц [отже мікрофон має бути розширений і призначеним, для приборкання акустичних сигналів, у яких частота знаходиться в діапазоні ультразвукових команд. На рисунку 3.7 показано метод скасування нечутної голосової команди.

В мікрофон можна додати модуль для фільтра низьких частот, з метою виявлення модульованих голосових команд та скасування основної смуги частот, використовуючи модульовані голосові команди [65]. Завдяки цьому можна

виявити сигнали в частоті діапазону ультразвуку, що показують характеристики модуляції та де модулювати ці сигнали для отримання основної смуги частот.

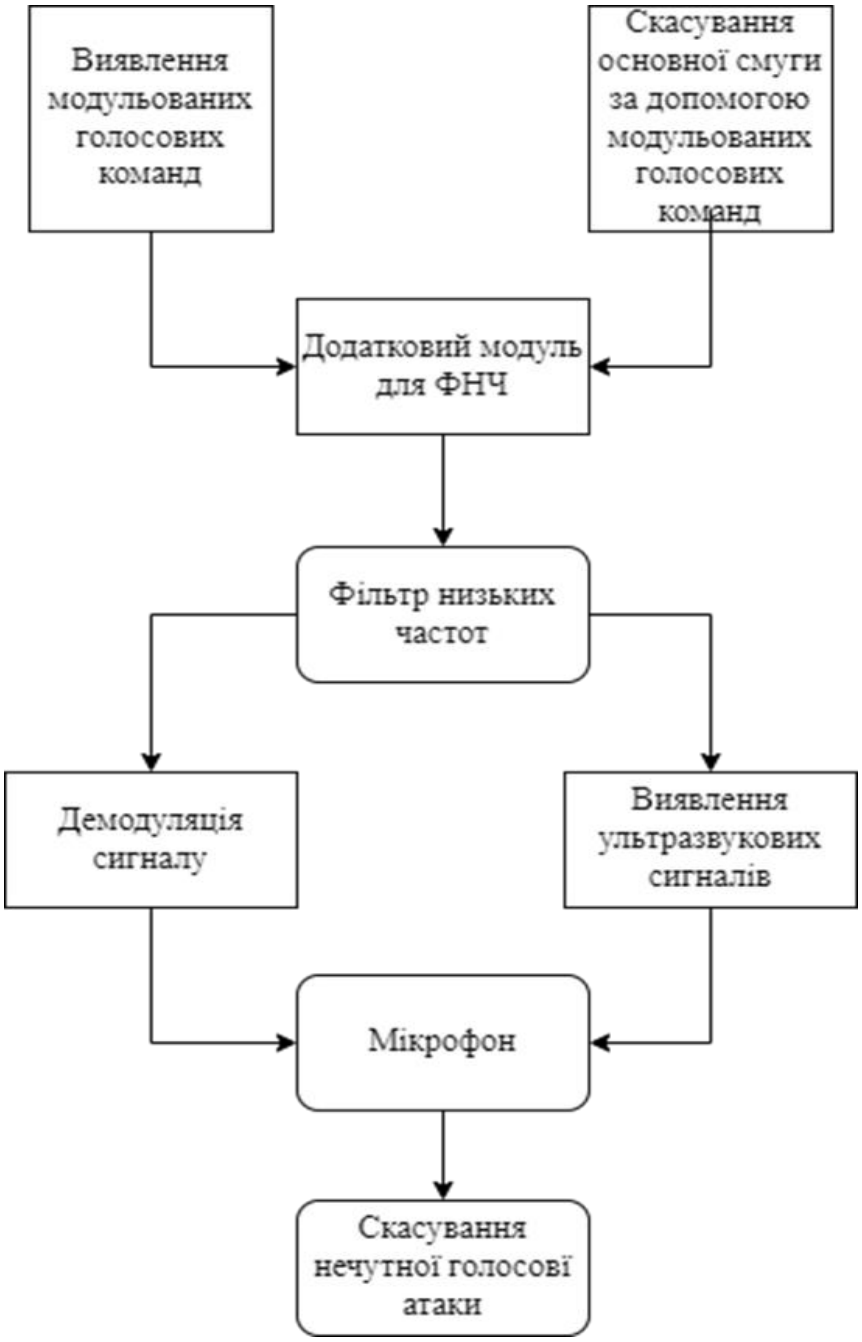


Рисунок 3.7 – Метод скасування нечутної голосової команди

Наприклад, при введенні ультразвукової команди, крім де модульованих сигналів основних смуг частоти $m(t)$, записані аналогові сигнали мають включати вихідний модульований сигнал. Нехай відомо, що:

$$v(t) = Am(t)\cos(2\pi f_c t) + \cos(2\pi f_c t), \quad (3.1)$$

де A – це коефіцієнт вхідного сигналу підсилення $m(t)$.

Виконуючи зниження $v(t)$ для отримання $Am(t)$ і регулюючи амплітуду, можна скасувати сигнал основної смуги частоти. Дана процедура скасування команд ніяк не впливає на нормальну роботу мікрофону, тому що не буде статистичного зв'язку між зловленими звуковими сигналами та шумами в ультразвуковому діапазоні.

Для забезпечення програмного захисту потрібно використовувати унікальні властивості голосових команд, які відрізняють їх від справжніх. На рисунку 3.7 показано демодульований сигнал кібератаки який відрізняється від вихідного сигналу і від записаного на високих частотах в діапазоні 800-2400 Гц.

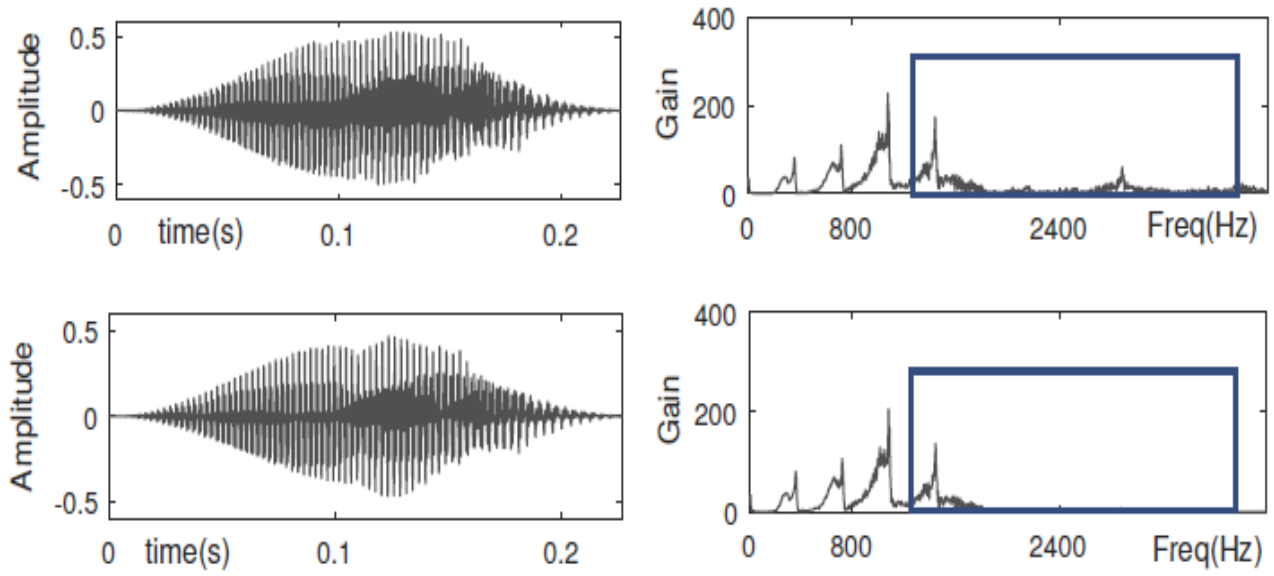


Рисунок 3.8 – Різниця демодульованого сигналу від вихідного [66]

Оригінальний сигнал який виробляється двигуном Google TTS, має частоту 25 кГц для модуляції, завдяки цьому є можливість виявити «DolphinAttack», виконавши аналіз частоти в діапазоні від 800 до 2400 Гц. Для підтвердження доцільності виявлення кібератаки, використовується метод опорних векторів в

ролі класифікатора та витягуванням з аудіо функцій у частотній та часовій області.

При використанні створених голосових команд «Привіт, Siri», за допомогою спеціальних програм перетворення тексту в голосову команду, були отримані по два зразки голосової команди, в яких один записувався, а інший відтворювався. Для того, щоб навчити класифікатор на методі опорних величин,для виявлення шкідливих голосових команд, необхідно використати декілька записаних аудіо зразків, інші зразки, можна використати, для тестування. Класифікатор може відрізнити відновлені аудіо записи від записаних з істинним плюсовим результатом і мінусовим показником на всі сто відсотків. Результат використання класифікатора, виконаного на методі опорних векторів, показує, даний програмний метод захисту, може бути виявлений, для шкідливих кібератак.

Наступний метод захисту від нечутної кібератаки полягає у пошуку та виявленню ознак не лінійності сигналу, які передаються на мікрофон СГК. Для цього потрібно зрозуміти чи можна виявити сліди не лінійності, від яких злочинець не зможе позбавитися. Але спочатку потрібно зрозуміти як саме працює акустична не лінійність. В цілому мікрофони та динаміки розроблені як лінійні системи, це означає, що вихідні сигнали є лінійними комбінаціями вхідних сигналів. У підсилювачі потужності який використовується в мікрофонах і динаміках, вхідний звуковий сигнал дорівнює $s(t)$, тоді вихідний сигнал в ідеальному має бути:

$$S_{out}(t) = A_1 s(t), \tag{3.2}$$

де A_1 – коефіцієнт підсилення підсилювача.

На практиці зазвичай компоненти в мікрофонах можуть бути лінійними тільки в чутних діапазонах частот, тобто більшими за 20 кГц. В ультразвукових смугах де частота менша як 25 кГц, вони показують не лінійність [67]. Звідси виходить, що для ультразвукових сигналів вихід підсилювача розраховується:

$$s_{out}(t) = \sum_{i=1}^{\infty} A_i s^i(t) = A_1 s(t) + A_2 S^2(t) + A_3 S^3 \cdots$$
$$\approx A_1 s(t) + A_2 S^2(t), \quad (3.3)$$

В роботі [65] показано як можна відтворювати ультразвукові сигнали, які можна записати мікрофоном, але для людини вони будуть нечутними. В ультразвуковому динаміку є можливість відтворення двох нечутних тонів:

$$s_1(t) = \cos(2\pi f_1 t), \quad (3.4)$$

З частотою $f_1 = 38$ кГц і $s_2(t) = \cos(2\pi f_2 t)$ на $f_1 = 40$ кГц. Коли комбінований сигнал проходить через нелінійний мікрофон на виході він стає:

$$s_{out}(t) = A_1 s_{hi}(t) + A_2 s_{hi}^2(t) = A_1\big(s_1(t) + s_2(t)\big) + A_2(s_1(t) + s_2(t))^2$$
$$= A_1 \cos(2\pi f_1 t) + A_1 \cos(2\pi f_2 t) + A_2\, cos^2(2\pi f_1 t) + A_2\, cos^2(2\pi f_2 t)$$
$$+2A_2 \cos(2\pi f_1 t)\cos(2\pi f_2 t), \quad (3.5)$$

Наведений сигнал має компоненти частоти $f_1,\ f_2,\ 2f_1, 2f_2, f_2 + f_1$ і $f_2 - f_1$. Мікрофон перед, цифровою обробкою і записом використовує фільтр низьких частот для видалення компонентів вищих 24 кГц. Отже, частоти $f_1, f_2, 2f_1, 2f_2\ i\ f_1 + f_2$ всі більші як 24 кГц, тоді залишається прийнятий сигнал:

$$s_{low}(t) = A_2 + A_2 \cos(2\pi(f_2 - f_2)t), \quad (3.6)$$

В цілому, $f_2 - f_1 = 2$ кГц записаний мікрофоном, це показує властивість, яка дає змогу надіслати нечутний сигнал, з можливістю генерувати копію звуку в середині мікрофону.

Таким чином позначимо сигнал голосової команди: «Siri, проклади маршрут…», яку вимовив користувач - $v(t)$, коли він промовлятиме цю команду, буде виконуватися вираз:

$$s_h = v(t) + n(t), \tag{3.7}$$

де $n(t)$- шум мікрофону.

Нехай злочинець відтворює цю голосову команду за допомогою ультразвуку, записаний сигнал s_{atk} буде мати вигляд:

$$s_{atk} = \frac{A_2}{2}\left(1 + 2v(t) + v^2(t)\right) + n(t). \tag{3.8}$$

На рисунку 3.8 показано спектрограму голосової команди для сигналів s_h та s_{atk}, як видно ці сигнали майже схожі за своєю структурою, а це означає, що конвертор тексту виводить однаковий текст для сигналів s_h та s_{atk}.

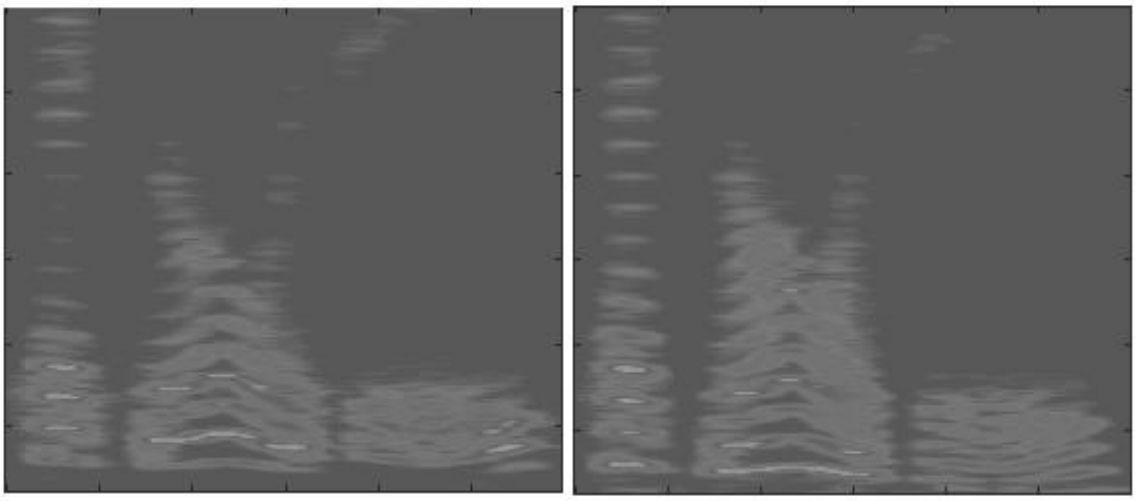


Рисунок 3.9 – Спектрограма для сигналу s_h та s_{atk}, голосової команди «Siri, проклади маршрут…» [68]

Виходячи з цього, можна зробити висновок, що для захисту потрібно перевіряти будь-який сигнал (вхідний) і визначати чи є він низькочастотним заданим користувачем, або копією високочастотної кібератаки.

Для прикладу можна використати еліптичний класифікатор «LipRead» [68], для пошуку та виявлення кібератак він використовує функції потужності, перекіс

амплітуди та коефіцієнт кореляції. Поводячи аналіз коефіцієнту помилкового прийняття та коефіцієнту помилкового відхилення, використовується основа еліпсоїдної техніки поділу. Щоб визначити оптимальну межу вирішення, обчислюється коефіцієнт помилкового прийняття та коефіцієнт помилкового відхилення (для кожного еліпсоїда. Його задача полягає у виборі параметрів еліпса, які мінімізують коефіцієнти. Оскільки він орієнтований на введення голосових команд, цей класифікатор розроблено автономно і його не потрібно навчати для кожного пристрою чи окремої людини.

Для забезпечення захисту та підвищення надійності від атак світловими командами в автомобільних системах голосового керування «Android Auto» [27] та «Apple CarPlay» [28] можна використовувати наступні програмні та апаратні методи захисту.

Програмний метод захисту полягає у застосуванні додаткового рівня аутентифікації для системи голосового керування. У роботі [58] автори використовують додатковий крок аутентифікації користувача, цим самим намагаючись захиститися від виконання несанкціонованих конференційних команд. Метод полягає у використанні додаткового кроку аутентифікації перед виконанням критичних команд та зменшення спроб неправильного введення паролю, якщо система підтримує таку функцію.

Цей метод може допомогти також у випадку коли злочинець не має змоги почути відповідь системи голосового керування, тому що знаходиться далеко від атакованого пристрою. Наприклад система задасть будь-яке випадкове запитання перед виконанням голосової команди, на яке злочинець не зможе дати відповідь, цим самим зупинивши атаку.

Наступний метод захисту полягає у використанні роботи датчиків, та використанні методів їхнього злиття для виявлення команд введених на основі світла [69]. Голосові помічники часто мають та використовують декілька мікрофонів. Суть методу полягає у тому, що злочинець використовує один спеціальний пристрій (лазер) для проведення атаки світловими командами і для цього використовується лише один мікрофон який отримує сигнал, в той час,

коли інші мікрофони нічого не отримують. Отже, можна спробувати виявити атаку, використавши порівняння сигналів від кількох мікрофонів, ігноруючи голосові команди, які вводяться за допомогою одного спеціального пристрою (лазера). Цей метод може бути ефективним, тільки тоді коли виконується один атакувальний пристрій.

Апаратний метод захисту полягає в покращенні структури мікрофону, тобто для блокування світлових команд можна використати спеціальні непрозорі перешкоди які можна встановити на мікрофон, тільки лишаючи невеликі зазори для можливості проходження звукових хвиль. Тобто зменшити кількість світла, яка досягає діафрагми мікрофона. На рисунку 3.10 зображено захист мікрофона.

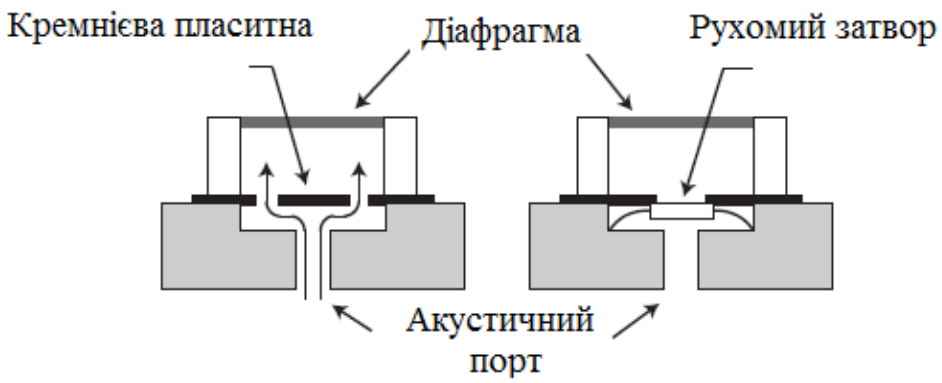


Рисунок 3.10 – Захист мікрофону за допомогою спеціальних бар’єрів [70]

Конструкція зображена на (рисунку 3.10) має кремнієву пластину та рухомий затвор, за допомогою яких усувається пряма видимість діафрагми мікрофона.

3.3 Метод вирішення задачі підвищення надійності системи голосового керування автомобіля

Підвищення рівня безпеки та надійності автомобільного транспортного засобу є одним з важливих аспектів сучасного суспільства. Недосконалість

спеціалізованих комп’ютерних систем з голосовим керуванням автомобіля, а саме з проблемою аутентифікації користувача або ж відсутністю її в цілому, у розділі 2, див. 2.2 і 2.3, дозволяють злочинцям отримати доступ до різних функцій та можливостей автомобіля. Використовуючи для цього різні види кібератак, наприклад атаки світловими командами [58], або введенням нечутних (ультразвукових) команд «DolphinAttack» [56], за допомогою спеціальних пристроїв, які направлені на мікрофони голосового керування автомобілем, дозволять злочинцям обходити недосконалість системи аутентифікації водіїв.

Описані раніше методи захисту, у розділі 3, див. 3.2 і дозволяють забезпечити надійність систем голосового керування автомобіля, досить ефективно, але не максимально. В результаті проведеного огляду першоджерел системи аутентифікації різних автомобілів, був отриманий матеріал, аналіз якого дозволив зробити висновок, що для максимального забезпечення надійності системи голосового керування автомобіля, потрібно використовувати додаткову систему аутентифікації, яка дозволить лише водію, або довіреним особам використовувати весь функціонал транспортного засобу, виконувати керування системами та інше.

Для розв’язання проблеми з додатковою аутентифікацією створена автономна система безпеки, з можливістю аутентифікації користувача за допомогою відбитків пальців власника автомобіля, або довірених осіб. Основними компонентами системи біометричної аутентифікації водія будуть такі компоненти: плата Arduino UNO, сканер відбитків пальців, LCD- дисплей, сервомотор для запуску системи автомобіля та додаткові апаратні пристрої.

Для програмування плати Arduino UNO та завантаження коду, будемо використовувати середовище розробки Arduino IDE. Для даного середовища будуть використані спеціальні бібліотеки для підключення основних компонентів системи (див. додаток А). На рисунку 3.11 зображено схему методу роботи системи біометричної аутентифікації, де показано основні етапи проходження перевірки користувача

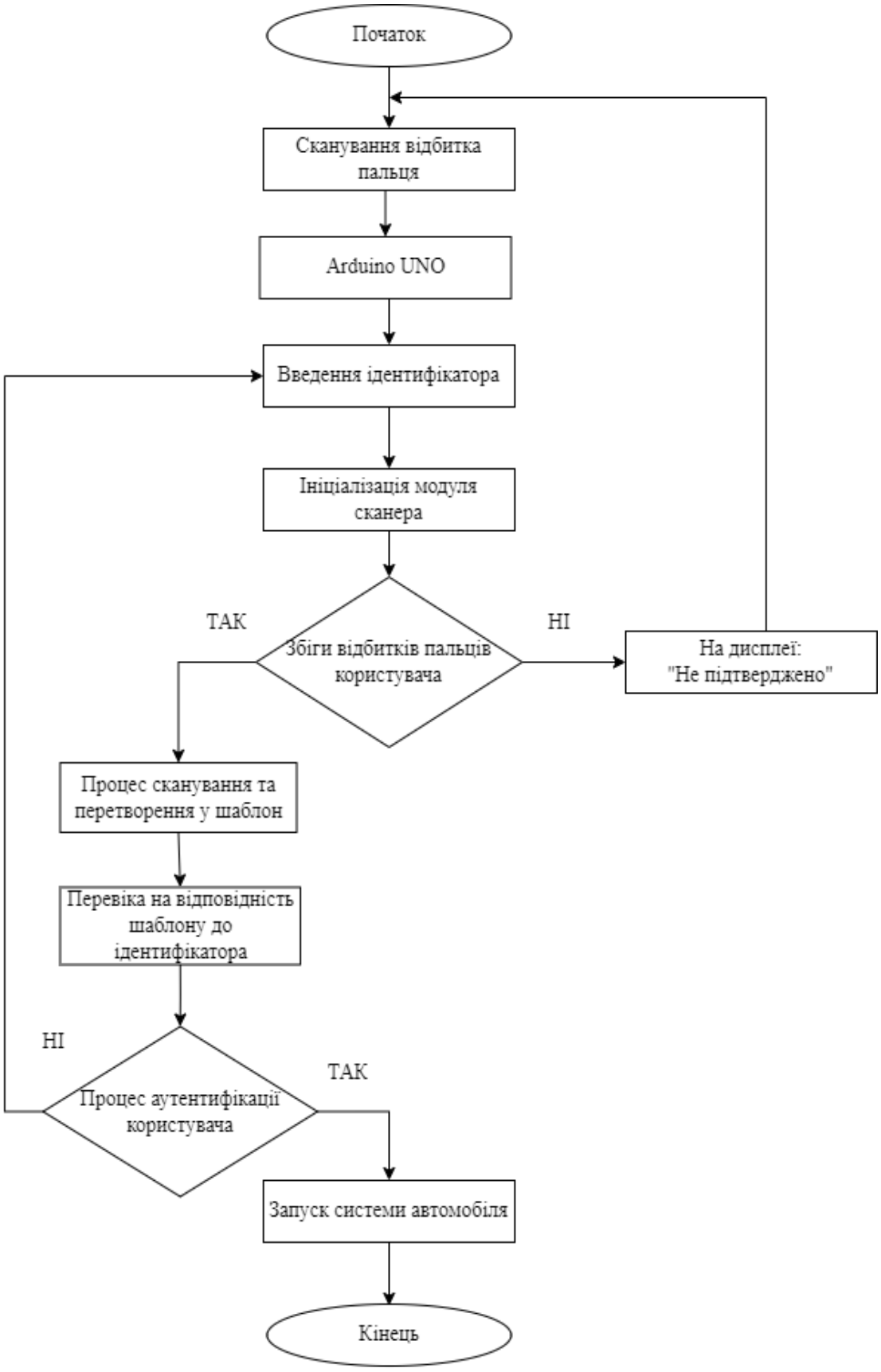


Рисунок 3.11– Блок-схема алгоритму роботи методу системи біометричної аутентифікації

3.4 Висновки

В даному розділі було описано та запропоновано методи та засоби для забезпечення надійності спеціалізованих комп’ютерних систем голосового керування автомобілем «Android Auto» та «Apple CarPlay» на основі захисту голосової аутентифікації систем від кібератак.

Проведено аналіз методу виявлення кібератаки за допомогою ультразвукових команд «DolphinAttack», визначено можливі наслідки та створена схема модулів, запропоновано новий метод забезпечення надійності для захисту від таких типів кібератак.

Визначено оцінку впливу на систему голосового керування автомобілем, та запропоновано апаратні та програмні методи забезпечення надійності спеціалізованих комп’ютерних систем «Android Auto» та «Apple CarPlay» від кібератак.

Запропоновано метод, що дозволяє вирішити задачу забезпечення надійності голосового керування, використовуючи метод додаткової біометричної аутентифікації користувача.

4 ДОДАТКОВА БІОМЕТРИЧНА СИСТЕМА АУТИНТЕФІКАЦІЇ КОРИСТУВАЧА ДЛЯ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ВІД КІБЕРАТАК

4.1 Вибір типу архітектури апаратно-програмного пристрою для біометричної аутентифікації водія

Технологія біометричної системи розпізнавання відбитків пальців це новий та сучасний метод для забезпечення надійності та захисту для систем безпеки. Цей метод використовує фізичну присутність користувача для аутентифікації користувача. Розпізнавання відбитків пальців сьогодні широко використовується в різних біометричних системах, наприклад в телефонах, в пристроях розумних будинків, біометричних замках, банківських розрахунках та інше [71]. Використання біометричної аутентифікації як персонального коду, в якості персонального коду вважається традиційним методом. Використання даної системи біометричної аутентифікації є досить надійним і дозволить користувачу забезпечувати надійність для спеціалізованих комп’ютерних систем автомобіля, та заблокує доступ злочинцеві до системи голосового керування, що у свою чергу унеможливить виконання різних способів проведення кібератак розділі 3, див. 3.1.

Відомі підходи до вирішення поставленого завдання засновані на роботі [72], в якій сказано, що біометричні технології безпеки являються одними з найефективніших систем захисту, та все більше стають повсякденними атрибутами в житті звичайних людей. В останні роки ці системи набули великого поширення у виробництві мобільних технологій, тобто у смартфони вбудовуються сканери відбитків пальців, розпізнавання голосу та інше.

Особлива увага до проблеми аутентифікації, пов’язана з розробкою методів та засобів для забезпечення надійності для СКС автомобіля. Тобто завдяки процесу аутентифікації особи, використовуючи порівняння її характеристик з характеристиками, які були раніше введені в систему, надається можливість максимально точно визначити, чи даний користувач має відповідний доступ до запитуваної інформації чи ні. Це дає можливість забезпечити надійність актуальній проблемі захисту інформації.

Важливим моментом для проведення досліджень в автомобільних системах аутентифікації є положення про те, що у сучасному світі існує високий попит на надійні та максимально безпечні системи в транспортних засобах. Отже, проектування та розробка апаратно-програмної біометричної системи безпеки з застосуванням технології відбитків пальців для запобігання несанкціонованого доступу до автомобіля є простим і корисним у використанні.

Апаратно-програмна реалізація системи використовує в собі додатковий спосіб аутентифікації користувача, що базується на можливості запуску системи запалювання автомобіля, що своєю чергою дозволить використовувати його функціонал, та унеможливить його використання, при неправильній біометричній аутентифікації за допомогою відбитку пальця.

Датчик відбитків пальців, надає можливість погодження малюнку відбитку користувача з тим, що зберігається в системній пам’яті датчика. Програма дослідження спрямована на інструменті для отримання відповідей та виконання інструкцій відповідно до отриманих результатів, використовуючи мікроконтролер Arduino Uno і включає наступні питання системи безпеки. Які використовують аналіз отриманих результатів та перевіряють чиї саме відбитки пальців можуть отримати права доступу для включення спеціалізованої комп’ютерної системи автомобіля.

4.1.1 Архітектура додаткової автомобільної системи аутентифікації

Провівши аналіз методів та вимог до додаткової автомобільної біометричної системи аутентифікації, можна зробити висновок, що потрібно створити проект архітектури та метод функціонування даної системи. Кожний апаратний компонент даної системи, має використовувати СПЗ, яке виконується за допомогою Arduino UNO. На рисунку 4.1 зображено архітектуру біометричної системи аутентифікації.

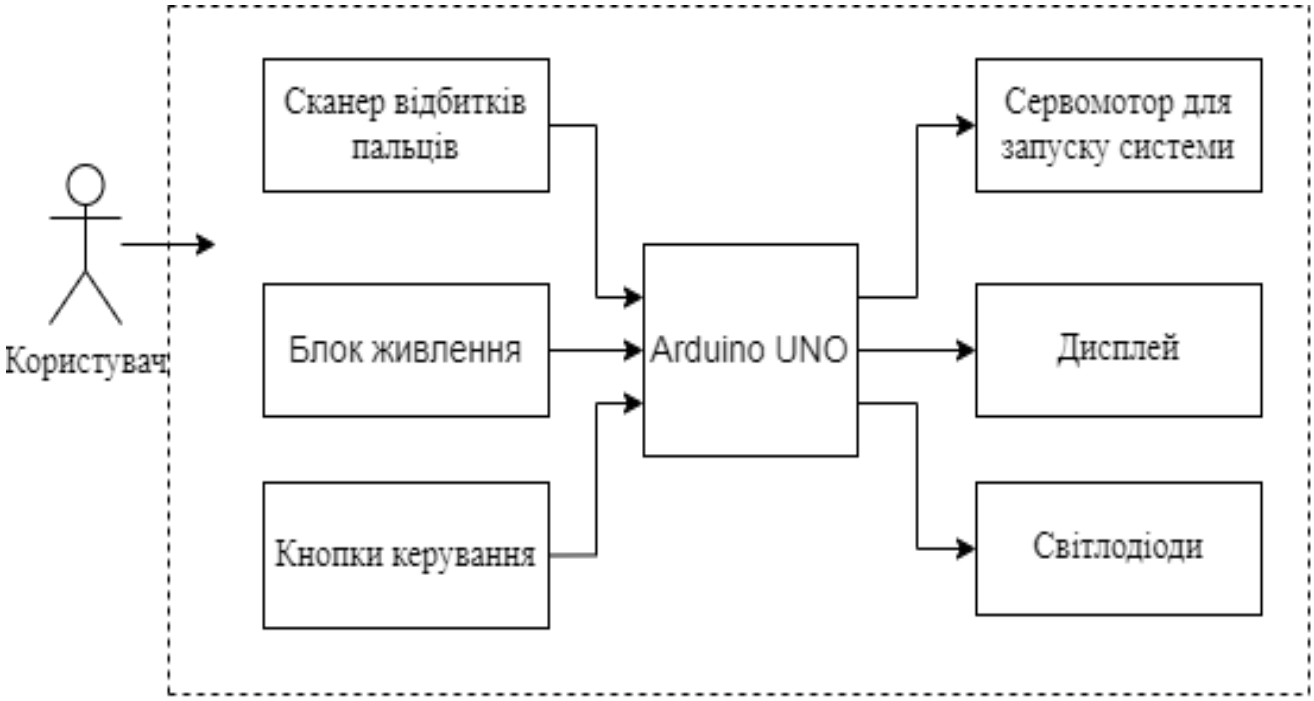


Рисунок 4.1– Апаратна архітектура автомобільної системи аутентифікації користувача за відбитком пальця

Апаратна складова автомобільної системи біометричної аутентифікації, складається, з сукупності апаратних пристроїв, своєю чергою здійснюють зчитування відбитку пальця користувача і виконують функції керування даних.

Структура апаратної системи біометричної аутентифікації охоплює в собі наступні пристрої:

- модуль сканера відбитків пальців;
- кнопки керування системою;
- LED-індикатори;
- сервомотор для запуску системи;
- LCD-дисплей;
- двоканальне реле;
- системна плата Arduino UNO.

Спочатку користувач повинен зареєструватися в базі даних системи біометричної аутентифікації, цей процес відбувається коли сканер отримує відбиток пальця вперше. Далі датчик відбитків пальців використовується, для

підтвердження особи користувача, використовуючи Arduino UNO як мікроконтролер, далі двоканальні релейні модулі використовуються як електронні перемикачі, виконують керування електричними пристроями. Далі релейні модулі будуть підключатися до колекторного контакту напруги на двигуні системи запуску автомобіля.

LCD-дисплей та LED-індикатори виконують функцію відображення повідомлення про результат виконання аутентифікації користувача за його відбитками пальців.

Програмна складова автомобільної системи біометричної аутентифікації (рисунок 4.2) містить в собі програмне забезпечення для:

– бази даних, яка використовується для зберігання та накопичення зображень відбитків пальців користувача, та інших довірених осіб і містить інформацію про них;

– програмне забезпечення для аналізу і класифікації розпізнавання збережених даних системи біометричної аутентифікації;

За допомогою програмного забезпечення біометричний пристрій зчитує відбиток пальця користувача або іншої довіреної особи, для того, щоб в подальшому його можна було визначити та конвертувати в цифровий формат для аутентифікації. Система розрізняє введення відбитку пальців в базу даних і показує результат.

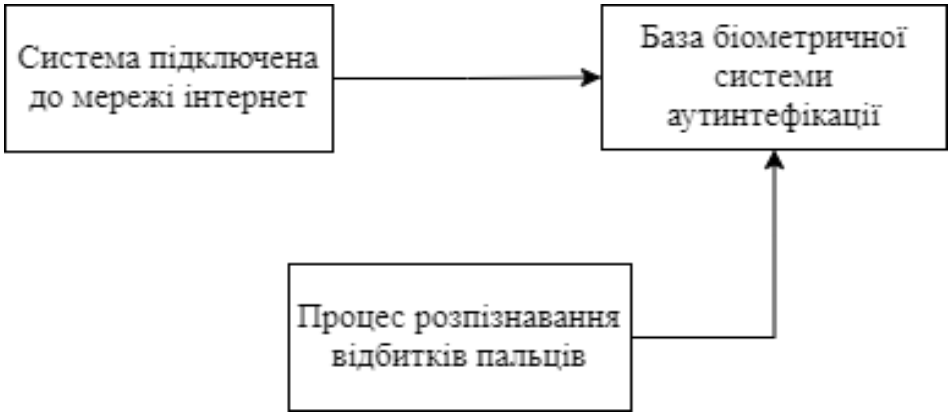


Рисунок 4.2 – Програмна складова автомобільної системи біометричної аутентифікації

4.1.2 Обґрунтування вибору та аналіз технічних характеристик системи біометричної аутентифікації автомобіля

Щоб обґрунтувати вибір апаратно-програмного забезпечення пристрою біометричної аутентифікації, необхідно, перш за все, з’ясувати технічні характеристики основних компонентів системи.

Одним з компонентів системи є апаратно-програмний комплекс Arduino UNO (рисунок 4.3). Він є чудовим інструментом для користувачів, з будь-яким рівнем можливостей. Системна плата Arduino UNO має можливість підключення різних периферійних пристроїв, та не потребує окремого апаратного забезпечення для завантаження нового коду, оскільки використовує для цього USB – кабель.

Середовище Arduino IDE використовується для програмування плати Arduino, та використовує мову C++, щоб зробити програму для вивчення невимогливою [73]. Це своєю чергою створює умови, щоб практично будь-який користувач мав можливість створити корисний і цікавий пристрій.

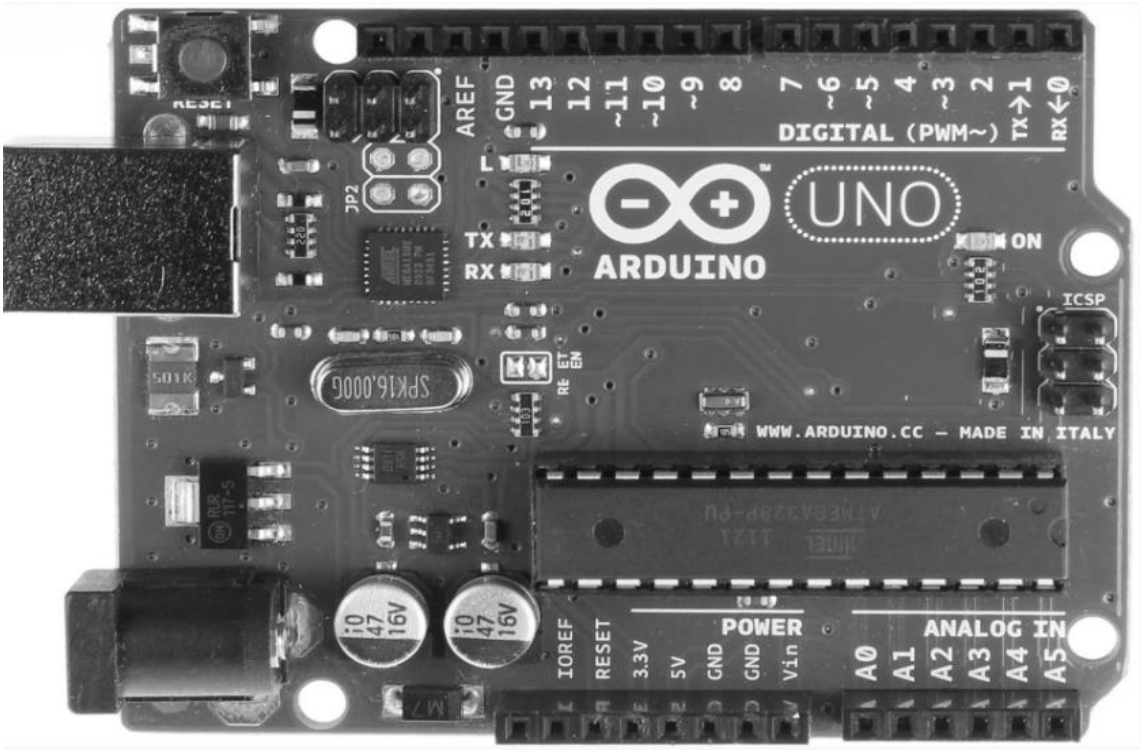


Рисунок 4.3 – Вигляд апаратно-програмного комплексу Arduino UNO [74]

Виявлення специфічних особливостей Arduino UNO є тим підґрунтям, на якому будуються всі інші аспекти дослідження системи біометричної аутентифікації, тому що даний апаратно-програмний комплекс є основним компонентом системи. За основу в Arduino UNO взято мікроконтролер ATMEGA328. Основні технічні характеристики даного пристрою, показано у таблиці 4.1.

Таблиця 4.1 – Переваги та недоліки системи голосового керування

Характеристики	Мікроконтролер
Електрична напруга роботи	5 В
Вхідна рекомендована напруга	7-15 В
Допустимі межі вхідної напруги	6-19 В
Цифрові контакти	14
Аналогові контакти входу	6
Постійний струм для контакту 3.3	150 мА
Постійний струм на контакти	40 мА
Статична пам'ять SRAM	2 КБ
Flash пам'ять	32 КБ
Швидкість тактової частоти	17 мГц
Енергонезалежна пам'ять	1 КБ

Мікроконтролер має кварцовий генератор, швидкість якого становить 16 мГц, 6 аналогових входів та 14 цифрових входів/виходів, 6 з яких можна використовувати в якості виходів широтно-імпульсної модуляції, роз’єм: живлення, програматора, USB, скидання налаштувань. Підключення відбувається за допомогою USB інтерфейсу, або акумулятора.

Плата Arduino UNO має вбудований стабілізатор, який надає можливість автоматично підбирати джерело для живлення, а також вирівнювати напругу до

необхідних для роботи контролера. Для зовнішнього живлення може використовуватися USB- порт.

На вхід потрібно подавати напругу в діапазоні від 7 до 15 Вольтів, для того, щоб знизити ризик перегріву стабілізатора і подальшого його функціонування. Якщо плата отримує живлення від будь-якого іншого джерела, можна отримати стабільну напругу 5 Вольтів. Контакт GND використовується для заземлення і повинен бути виведений як мінус, інакше живлення подаватися не буде.

Мікроконтролер ATmega328, має Flash, SRAM і енергонезалежну пам'ять, характеристики яких показано у таблиці 4.1.

Наступним важливим компонентом біометричної системи аутентифікації автомобіля є сканер відбитків пальців. Для даної системи був обраний сканер FPM10A (рисунок 4.4), тому що, ця модель підтримує алгоритми шифрування даних, та має вбудовану пам'ять. Що дозволяє створювати базу даних відбитків пальців користувачів у внутрішній пам’яті.

Рисунок 4.4 – Сканер відбитків пальців FPM10A [75]

Сканер є сумісним з різними мікроконтролерами, також має низьке енергоспоживання, а час обробки зображення займає не більше 1 секунди. Процес аутентифікації за допомогою відбиту пальця користувача відбувається коли система виконує та порівнює знімок відбитку за шаблоном чи раніше надрукованими знімками у базі даних. Основні технічні характеристики сканера відбитків пальців FPM10A наведено у таблиці 4.2. На рисунку 4.5 зображено схему підключення сканера відбитків пальців FPM10A до Arduino UNO.

Таблиця 4.2 – Параметри сканера відбитків пальців FPM10A

Характеристики	Значення характеристик
Напруга живлення	3.6 – 6.0 В
Робочий струм	120 мА
Час обробки зображення відбитка пальця	менше 1.0 сек.
Вид сенсора	Оптичний
Розмір сенсора	14x18 мм
Розмір сигнатури	256 байтів
Розмір шаблону	512 байтів
Місткість	до 300 комірок
Рівні безпеки	1-5
Вид інтерфейсу	UART TTL
Швидкість передачі	57600
Робоча температура	-15 ° C - +45 C
Рівень вологості повітря	45% - 80% RH
Розміри	47 x 25 x 20 мм
Вага пристрою	14 грам

Функціональне призначення провідників (рисунку 4.4), показує, що за живлення відповідає червоний провідник, зелений та білий провідники

відповідають за вихідні/вхідні дані відповідно, чорний відповідає за заземлення.

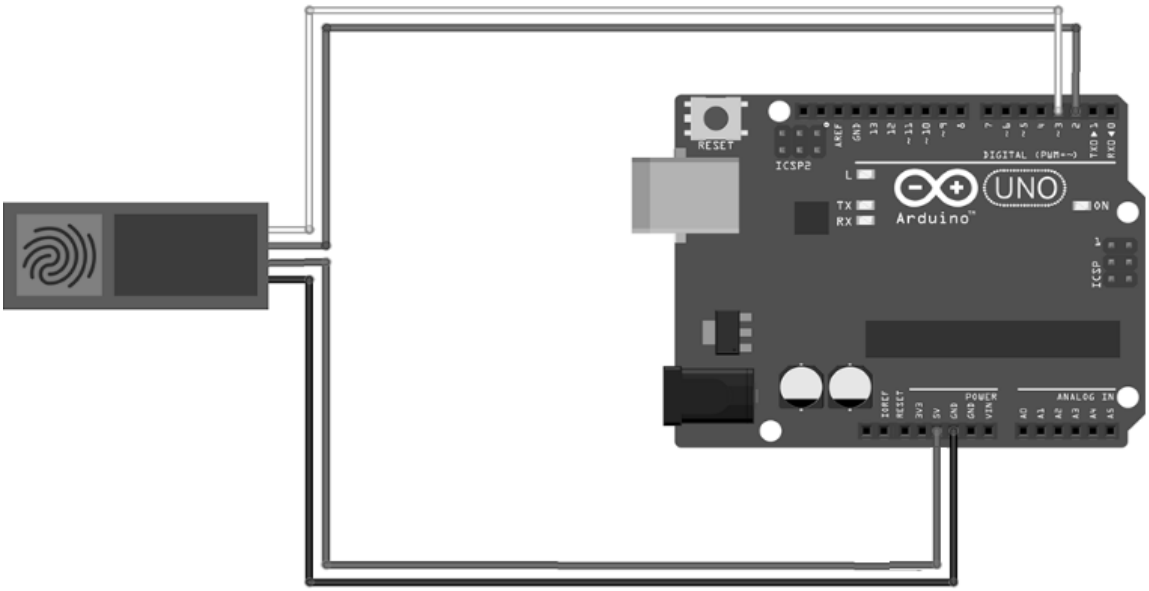


Рисунок 4.5 – Схема підключення сканера FPM10A до Arduino UNO

Для зображення результатів роботи біометричної аутентифікації використовується LCD QA1602A дисплей. Цей дисплей використовуватися для зображення буквено-цифрових символів.

Він має два рядки, які складаються з 16 символів відповідно. Для роботи використовує бібліотеку LiquidCrystal в Arduino IDE. Основні технічні характеристики наведено у таблиці 4.3.

Таблиця 4.3 – Характеристики дисплею LCD QA1602A

Характеристики	Значення характеристик
Розміри дисплею	82 x 37 мм
Температура роботи	0 – 40 °C
Колір підсвічування	темно-синій
Колір зображення символів	білий
Розмір зображення символів	4.39 x 2.97 мм
Формфактор	16 x 2
Розміри крапок	0.5 x 0.5 мм

Кінець таблиці 4.3 – Характеристики дисплею LCD QA1602A

Напруга живлення	5 В
Використаний інтерфейс	HD44780

Дисплей LCD QA1602A (рисунок 4.5), отримуватиме код від мікроконтролера Arduino UNO та показуватиме його в оперативній пам’яті, далі коди символу будуть перетворюватись в шаблони та показуватися на LCD дисплеї.

Також дисплей зображає та використовує функцію додавання нового користувача та видалення інформації про зареєстрованого користувача біометричної аутентифікації автомобіля, та показувати статус вдалої аутентифікації. Контактні Pin модулі та їхній опис функціоналу для LCD дисплею наведено у таблиці 4.4.

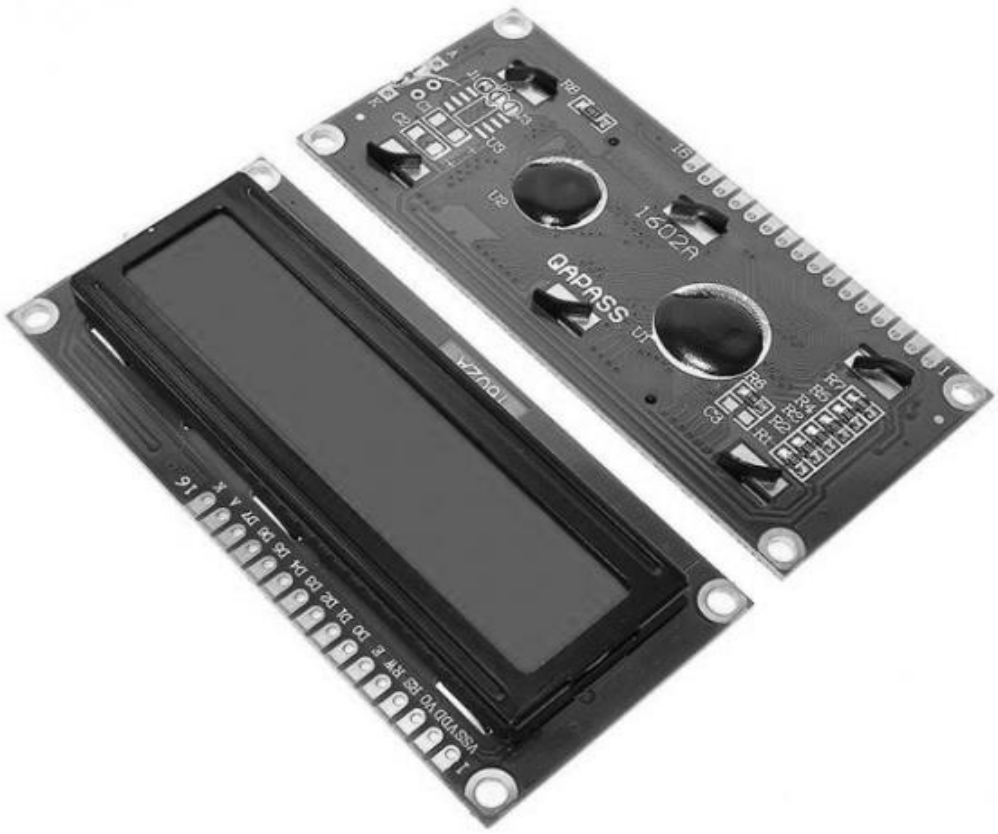


Рисунок 4.5 – LCD дисплей QA1602A [76]

Таблиця 4.4 – Pin модулі та їхні функції LCD QA1602A

№ виводу	Контактні модулі	Опис функціоналу
1	Data Pin 1	Підключається до VDD.
2	Data Pin 2	Підключається до джерела живлення пристрою.
3	Data Pin 3	Використовується для регулювання контрасту LCD дисплея.
4	Data Pin 4	Вибір реєстру.
5	Data Pin 5	Вибір сигналу читання або запису.
6	Data Pin 6	Ввімкнення сигналу.
7	Data Pin 7 to in 14	Шина даних.
8	Data Pin 15	Збільшення підсвічування.
9	Data Pin 16	Зменшення підсвічування.

Провівши аналіз технічних характеристик, та виконавши обґрунтований вибір основних компоненті апаратного забезпечення автомобільної системи додаткової біометричної аутентифікації користувача, можна перейти до проектування схеми взаємодії між компонентами системи.

Для того, щоб спроектувати схему потрібно використати такі апаратні компоненти:

- плата Arduino UNO;
- сканер відбитків пальців FPM10A;
- LCD дисплей QA1602A;
- з’єднувальні провідники;
- LED світло-діоди;
- резистори 1 кОм;
- резистор 2.2 кОм;
- джерело живлення;

– кнопки керування.

Кнопки керування використовуються для взаємодії з автомобільною системою біометричної аутентифікації. Кнопка реєстрації, використовується для реєстрації нового відбитку сканування пальця користувача та з можливістю повернення назад. Наступна кнопка дозволяє вибирати ідентифікатор або місцеположення, а також для видалення сканованого зображення, інші кнопки виконують функції переміщення і зіставлення відбитків пальців. LED світло діоди використовуються як індикатори та показують, що система біометричної аутентифікації готова для зчитування відбитків пальців. На рисунку 4.6 наведено створену схему апаратних компонентів автомобільної системи біометричної аутентифікації користувача.

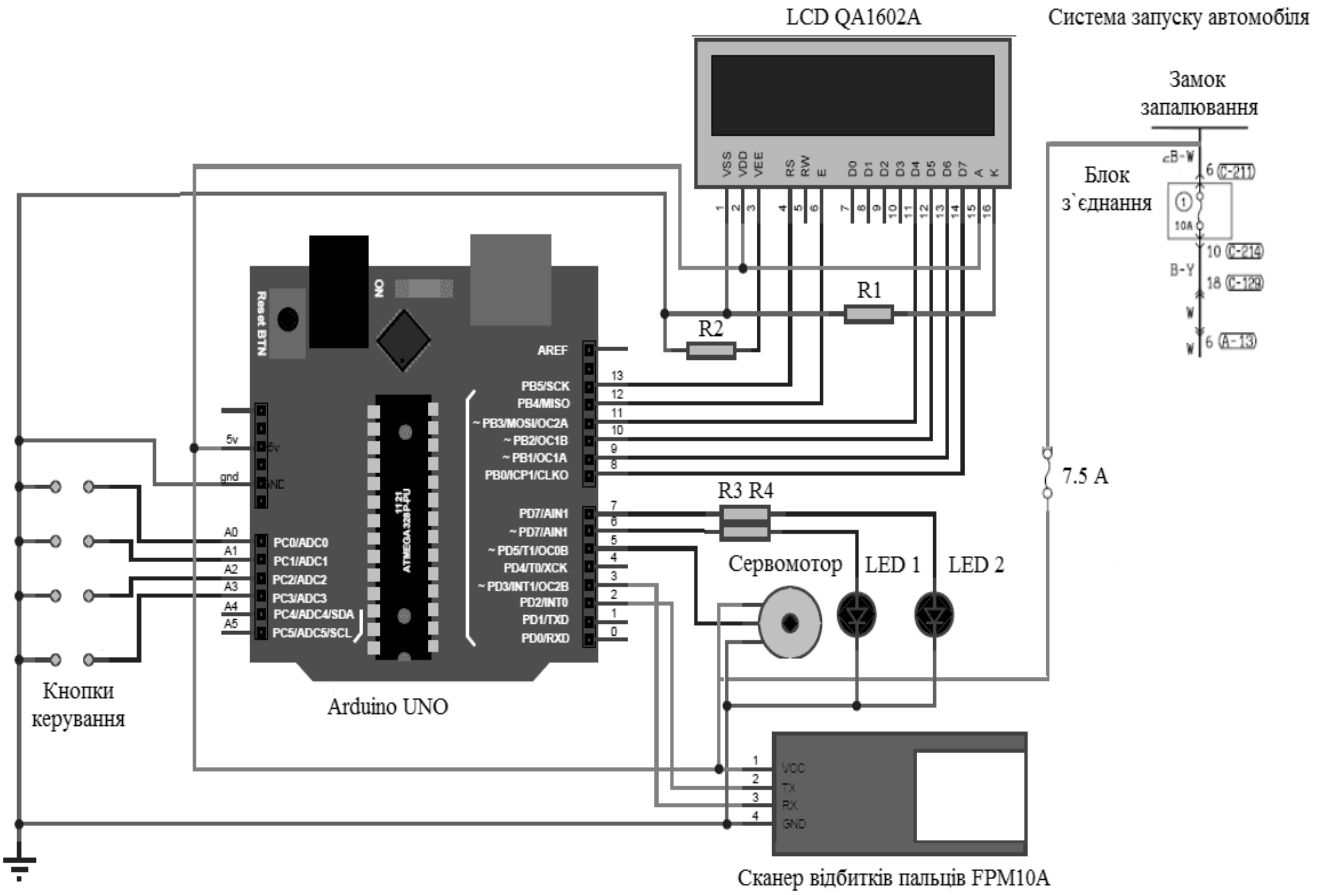


Рисунок 4.6 – Схема автомобільної системи біометричної аутентифікації

Плата Arduino UNO виконує керування всіма процесами схеми (рисунок 4.6), а саме зчитує натискання кнопок, відображає інформацію на дисплеї та приймає інформацію від сканера, коли користувач проходить аутентифікацію, виконує запуск автомобіля.

4.2 Програмна (апаратно-програмна реалізація) автомобільної системи біометричної аутентифікації

Текст Для реалізації програмної частини автомобільної системи біометричної аутентифікації необхідно встановити додаткові бібліотеки для роботи:

– Adefruit Fingerprin Library для роботи з модулем сканера відбитків пальців FPM10A;

– Liquid Crystal Library 2CV112 для роботи з LCD дисплей QA1602A;

– Wire та SoftwareSerial, що входять в стандартний набір середовища розробки IDE Arduino для програмування Arduino UNO;

Приєднавши Arduino UNO до порту комп’ютера за допомогою USB, на першому етапі за допомогою бібліотеки Adefruit Fingerprin необхідно виконати наступні кроки реєстрації нового відбитка пальця (рисунок 4.7).

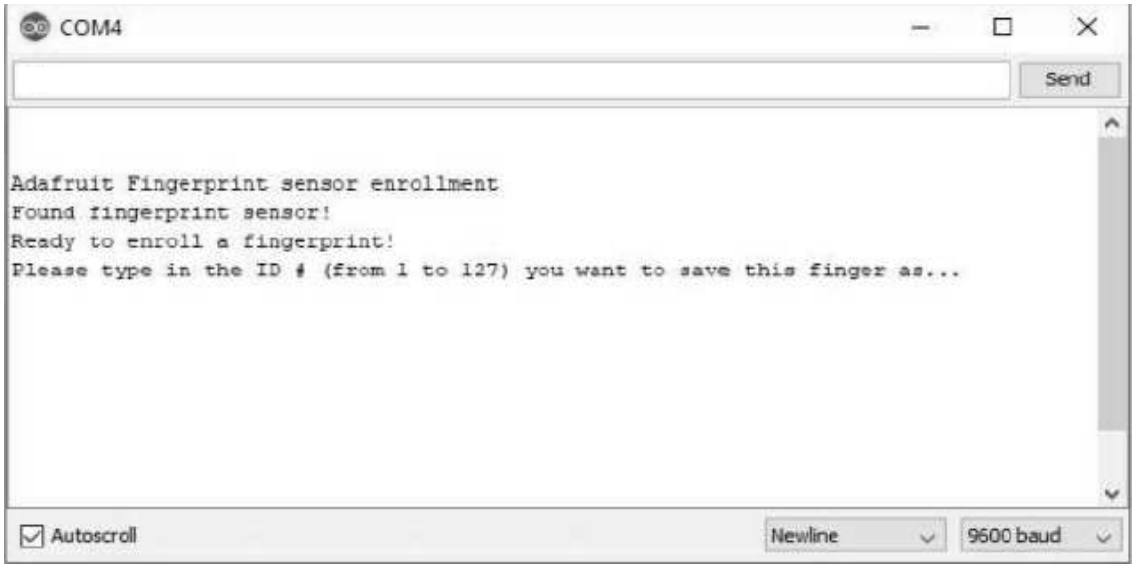


Рисунок 4.7 – Реєстрація нового відбитка користувача

Далі потрібно повторити процедуру, та двічі помістити той самий палець на сканер і повторювати процес до того часу, коли отримаєте повідомлення про те що відбитки збігаються. Це означатиме, що відбиток успішно збережено.

Далі показано вікно (рисунок 4.8), з тим що є декілька відбитків користувача, як збережені на різних ідентифікаторах.

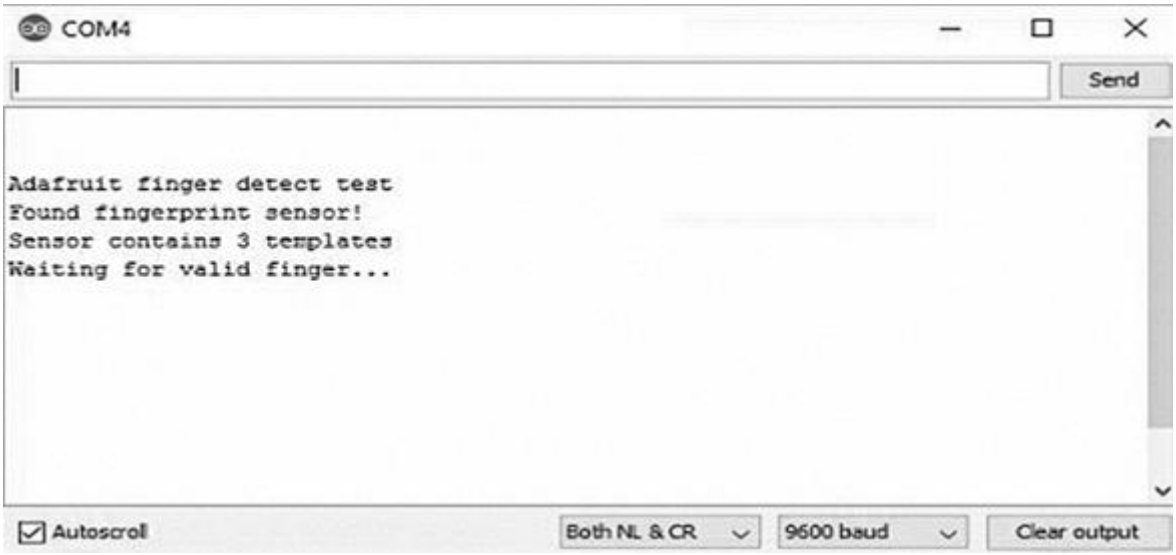


Рисунок 4.8 – Зображення декількох відбитків користувача

Наступним кроком є сканування для ідентифікованого користувача. На екрані показано ідентифікатор, що відповідає відбитку користувача. Він показує вірогідність чим більша вірогідність тим більша схожість з відбитком пальця користувача. Для зчитування в автомобільній системі біометричної аутентифікації відбитка пальця користувача та виконання певних дій (запуску системи автомобіля) використовується наступний фрагмент коду:

```
for (int i = 0; i <5; i ++)
  {
    lcd.clear ();
    lcd.print ("Put your finger");
    delay (1900);
```

```
int result = getFingerprintIDez ();
if (result> = 0)
   digitalWrite (openLight, HIGH);
   digitalWrite (closeLight, LOW);
   lcd.clear ();
   lcd.print ("Confirmed");
   lcd.setCursor (0,1);
   lcd.print ("Start System");
   motServo.write (0);
   delay (5000);
   motServo.write (150);
   digitalWrite (closeLight, HIGH);
   digitalWrite (openLight, LOW);
   lcd.setCursor (0,1);
   lcd.print ("Start the car system");
```

Також у додатковій автомобільній системі біометричної аутентифікації користувача, використано різні функції для коректної роботи компонентів.

4.3 Результати експерименту та аналіз додаткової системи аутентифікації користувача

Перевірку доступу в автомобільній біометричній системі аутентифікації, можна вважати успішною, якщо користувач увімкне автомобільну систему за допомогою власного відбитка пальця, що зареєстрований у пам’яті пристрою. Якщо зареєстрований у системі користувач не в змозі цього зробити, систему можна вважати несправною. Результат роботи функцій, що використовуються в системі додаткової біометричної аутентифікації наведено у таблиці 4.5

Таблиця 4.5 – Функції програмної реалізації біометричної аутентифікації

Назва функції	Реалізація функції
void checkKeys()	Використовується для перевірки натискання кнопок.
deleteFingerprint()	Надає можливість видалення запису з вибраним ідентифікатором системи.
delet()	Введення ідентифікатора пальця користувача, який необхідно видалити з системи, та використовується для виклику функції, що видаляє запис із вибраними ідентифікаторами з системи
getFingerprintEnroll()	Збереження та конвертування відбитка пальця у шаблон з вибраним ідентифікатором в пам'ять модуля датчика відбитка пальця користувача.

Проведення експерименту відбувається, шляхом виявлення відбитків пальців для системи, спрямованих на пошук значення відсотку успіху інших відбитків пальців, які не були введені в базу даних сканера. Експеримент виконується шляхом встановлення відбитка пальця користувача, а потім продовження встановлення відбитка пальця другого користувача. Для визначення відсоткових значень будуть перевірені зміни десяти правих відбитків пальців користувачів, які були використані за допомогою зразка сканування іншої особи, що не була зареєстрована у сканері датчика відбитку пальця.

Важливим моментом для проведення дослідження є положення про те, що сканер дуже чутливий до розміщення відбитків пальців користувача. Розташування відбитка пальця має бути точно на шарі скла сканера, щоб відбиток читався чітко та відповідно до введеного і зберігався в системі. Результати дослідження модуля відбитків пальця наведено у таблиці 4.6.

Таблиця 4.6 – Дослідження сканування відбитків пальця користувача біометричної системи автомобіля

Відбиток пальця	Позитивний (справжній)	Негативний (справжній)	Хибно-позитивний	Помилково-негативний	Автомобільна система
1	1	0	0	0	включена
2	1	0	0	0	включена
3	1	0	0	1	виключена
4	1	0	0	0	включена
5	1	0	0	0	включена
6	1	0	0	0	включена
7	1	0	0	1	виключена
8	1	0	0	0	включена
9	1	0	0	0	включена
10	1	0	0	0	включена

У таблиці 4.6 показано матрицю результатів тесту. Матриця показує фактичну та неправильну кількість прогнозів у даних тесту матриці. Вхідні дані матриці мають такі значення:

– позитивний (справжній) - це кількість відбитків пальців користувачів за допомогою сканера;

– негативний (справжній) для кількості відбитків інших користувачів, що виявлені неправильно;

– хибно-позитивний результати відбитків пальців іншого користувача, якого вводять, перевірені та правильні;

– помилково-негативний коли модуль сканера відбитків пальців вказує, що не вдалось отримати доступ до системи запуску автомобіля.

Виходячи з наведених вище результатів можна зробити висновок, що відсоток успішності відбитка пальця користувача який може отримати доступ до автомобіля становить 90 відсотків.

В наступному дослідженні брали участь дев’ять користувачів, ідея полягала в тестуванні функції перевірки відбитків пальців системи, тобто самого режиму роботи. Кожний користувач робив близько тридцяти спроб перевірити свій відбиток пальця, який був збережений системою раніше. В результаті дослідження було виявлено, що час для виконання перевірки відбитка пальця користувача становить менше однієї секунди, результати дослідження наведено у таблиці 4.7

Таблиця 4.6 – Результати тестування системи

Користувач	Кількість спроб	Підтверджено	Невдала спроба	Відсоток підтверджених спроб
1	35	33	2	93.3 %
2	35	34	1	96.6 %
3	35	33	2	93.3 %
4	35	32	3	90 %
5	35	34	1	96.6 %
6	35	31	4	87.7 %
7	35	33	2	93.3 %
8	35	34	1	96.6 %
9	35	34	1	96.6 %

Результати дослідження показують, що додаткова система біометричної аутентифікації користувача досить ефективна, більша кількість спроб аутентифікації користувачів були вдалими та виконувалися за призначенням. Невдалі спроби розпізнавання відбитка пальця, можуть бути пов’язані з неправильним розміщенням користувачем на сканері пальців, або іншими несуттєвими проблемами.

4.4 Оцінка ефективності моделей та методів для розв’язання задачі

Особливість запропонованого підходу полягає в тому, що спочатку, змінний стум подається на трансформатор 0-12 Вольт, який є підвищуючим трансформатором. Відомо що, трансформатор, у якого вихідна напруга перевищує вхідну напругу, називається підвищуючим трансформатором.

Підвищувальний трансформатор зменшує вихідний струм для підтримки вхідної та вихідної потужності системи. Далі LCD - дисплей зображує систему запалювання автомобіля. LCD - дисплей розміром 16x2 означає, що він може показувати 16 символів на рядок.

На цьому LCD - дисплеї кожен символ зображується в матриці 5x7 пікселів і здатний відображати 224 різних символи та символи. Дисплей має два регістри, а саме команди та даних.

В системі біометричної аутентифікації використовується чотири кнопки: UP/DOWN, ENROLL, D/T, OK. За допомогою цих кнопок надається можливість зберігати та видаляти відбитки пальців користувачів. Для цього натисніть кнопку UP/DOWN, потім натисніть OK, щоб встановити розташування відбитка пальця/

Після того, як встановили розташування, натисніть кнопку D/T, тоді з’явиться повідомлення: «Будь ласка, зачекайте» і після цього він покаже місце пальця на сканері відбитків пальців FPM10A. Модуль датчика відбитків пальців фіксує зображення пальця, а потім перетворює його в еквівалентний шаблон і зберігає його у своїй пам’яті за вибраним ідентифікатором Arduino UNO.

Усім процесом керує Arduino UNO, наприклад, знімати відбиток пальця, перетворювати його в шаблони, зберігати місце розташування тощо. А потім він зображатиме зроблене зображення, а потім знімає палець і знову поміщає палець. Після розміщення пальця він показує, що користувач пройшов аутентифікацію, а це своєю чергою означає, що автомобіль запускається. Запуск автомобіля здійснюється сервомотором. Сервомотор - це поворотний або лінійний привод, який дозволяє точно керувати кутовим або лінійним положенням, швидкістю та прискоренням.

Результат роботи системи біометричної аутентифікації полягає в тому, що автомобіль запуститься лише тоді, коли затверджений користувач зможе відсканувати свій палець на модулі відбитків пальців. Біометрична система запалювання призначена для забезпечення транспортного засобу високого рівня безпеки та захисту. Керувати ланцюгом запалювання будуть лише схвалені відбитки пальців користувача які запрограмовані на запалювання автомобіля. Система перевіряє та розблокує ланцюг запалювання за 0,3 секунди, що робить систему надійною.

4.5 Висновки

В результаті узагальнення літератури для забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем, виявлено низку проблем, основними з яких є недосконаліть системи аутентифікації користувача.

Для реалізації вирішення даної проблеми було створено та розроблено апаратно-програмний продукт додаткової біометричної автомобільної системи аутентифікації користувача. Система створена для забезпечення надійності від кібератак на систему голосового керування.

В результаті проведеного експерименту з системою біометричної аутентифікації, було виявлено, що успішність для зареєстрованого в системі відбитка пальця користувача, який може отримати доступ до автомобіля становить дев'яносто відсотків.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено додаткову біометричну систему аутентифікації користувача для підвищення надійності голосового керування автомобілем, та захисту від сучасних методів кібератак.

У першому розділі розглянуто основні поняття та концепції спеціалізованих комп'ютерних систем автомобіля. Також здійснено комплексний огляд системи голосового керування автомобілем та способи взаємодії даної системи з користувачем. Проведено аналіз засобів для забезпечення та підвищення надійності, в результаті якого можна сформулювати комплекс методів підвищення надійності голосового керування автомобілем. В перше поставлено та вирішено питання принципу роботи спеціалізованих автомобільних систем «Android Auto» та «Apple CarPlay».

У другому розділі проведено аналіз в результаті якого були сформовані концепції зарубіжних аналогів спеціалізованих комп'ютерних систем голосового керування автомобілем «Android Auto» та «Apple CarPlay». Проведено дослідження основних недоліків та вразливостей голосових помічників для даних систем, в результаті якого сформульовано загрози для системи голосової аутентифікації автомобіля.

Запропоновано модель виявлення загроз та забезпечення надійності голосових помічників «Siri» та «Google Assistant», що дозволяє удосконалити засоби які потрібно використовувати для підвищення надійності спеціалізованих комп'ютерних систем автомобіля. Проведена порівняльна оцінка моделі виявлення сучасних способів кібератак, яка показала можливості проведення атак ультразвуковими та світловими командами на систему голосового керування автомобілем.

У третьому розділі проведено дослідження оцінки впливу та запропоновано нову класифікацію існуючих методів та засобів для забезпечення надійності спеціалізованих комп'ютерних систем голосового керування автомобілем

«Android Auto» та «Apple CarPlay» на основі захисту системи голосової аутентифікації систем від кібератак ультразвуковими та світловими командами.

Проведено аналіз методу виявлення кібератаки за допомогою ультразвукових команд «DolphinAttack», визначено можливі наслідки та створена схема модулів, розроблений метод підвищення безпеки, що дозволяє на підготовчому етапі проведення кібератаки попередити та унеможливити її виконання.

В результаті дослідження запропоновано апаратні та програмні методи забезпечення надійності спеціалізованих комп'ютерних систем «Android Auto» та «Apple CarPlay» від кібератак на основі проведення ультразвуковими та світловими командами. Запропоновано метод, що дозволяє вирішити задачу забезпечення надійності голосового керування, використовуючи метод додаткової біометричної аутентифікації користувача.

У четвертому розділі досліджено проблему недосконалості голосової аутентифікації користувача, та для вирішення даної проблеми було розроблено та реалізовано апаратно-програмний продукт додаткової біометричної автомобільної системи аутентифікації користувача. Виконано комплексну оцінку ефективності використаних моделей та методів для вирішення поставленої задачі.

Проведено вибір типу архітектури та основних компонентів системи для апаратно-програмного пристрою додаткової біометричної системи користувача. Здійснено обґрунтування та аналіз основних технічних характеристик даної системи. Проведено експериментальне дослідження системи на різних користувачах, в результаті якого було встановлено, що система справно виконує всі задані функції.

Практична цінність отриманих результатів. В результаті виконаного наукового дослідження запропоновано апаратні та програмні методи забезпечення надійності спеціалізованих комп'ютерних систем «Android Auto» та «Apple CarPlay» від кібератак на основі проведення ультразвуковими та світловими командами. Виконано комплексну оцінку ефективності використаних моделей та методів для вирішення поставленої задачі. Проведено експериментальне

дослідження системи на різних користувачах, в результаті якого було встановлено, що система справно виконує всі задані функції.

За темою магістерської роботи подано статтю «RESEARCH OF METHODS AND MEANS OF ENSURING THE RELIABILITY OF A SPECIALIZED COMPUTER VOICE VEHICLE CONTROL SYSTEM» у фахове наукове видання Computer systems and information technologies (м.Хмельницький) [2].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Що таке комп'ютерна система?: технопедія. URL: https://uk.theastrologypage.com/computer-system (дата звернення 06.11.2021).

2. Башук В.Ю., Гнатчук Є.Г. RESEARCH OF METHODS AND MEANS OF ENSURING THE RELIABILITY OF A SPECIALIZED COMPUTER VOICE VEHICLE CONTROL SYSTEM. *Міжнародний науковий журнал «Журнал комп'ютерних систем та інформаційних технологій».* 2022. № 1. С. 54–61.

3. Sukhorukova I.V., Chistyakova N. A. Methodological aspects of teaching actuarial mathematics. *Astra Salvensis - overview of history and culture*. 2018. Vol. 15, No special. P. 847-858.

4. Stoimenov D., Petrov P. System for voice control of car modules with communication through CAN network: bachelor's thesis in Technical University Sofia, Bulgaria, 2016. P. 93-98.

5. Heisterkamp P. Linguatronic: Product-Level Speech System for Mercedes-Benz Cars: Proceedings of the First International Conference on Human Language Technology Research., San Diego, 2016. P. 124-126.

6. Mann S., Berton A., Ehrlich U. How to Access Audio Files of Large Data Bases Using: In-car Speech Dialogue Systems: DaimlerChrysler AG, *Group Research & Advanced Engineering.* Antwerp, August 22. 2017. P. 49.

7. Continental Automotive :Advanced Driver Assistance Systems. URL: http://www.continentalautomotive.com/www/automotive_de_en/themes/passenger_cars /chassis_safety/ada s (дата звернення 07.11.2021).

8. Juliussen E., Carlson J. Not If, but When: Autonomous Driving and the Future of Transit. *Journal of Public Transportation*. 2018. Vol. 21, No 1. P. 92-103.

9. Nissan's Autonomous Self Driving Car: Nissan USA. URL: http://www.nissanusa.com/blog/autonomous-drive-car (дата звернення 07.11.2021).

10. Model S Autopilot Press Kit:Tesla Motors. URL: https://www.teslamotors.com/presskit/autopilot (дата звернення 07.11.2021).

11. Ching Y. C. Advancements, prospects, and impacts of automated driving systems. *International Journal of Transportation Science and Technology*. September 2017. Vol. 6, No 3. P. 208-216.

12. Bansal P., Kockelman K. M. Are we ready to embrace connected and self-driving vehicles? A case study of Texans: Transportation 45., Austin, TX, USA, 19 November 2018. P. 641–675.

13. Smith S. Digital signal processing: A practical guide for engineers and researchers. California: Dodeka-XXI, 2016. P. 720.

14. Суприган О. І., Ваховська Л.М. Комбінування генетичних алгоритмів в елементах штучної нейронної мережі. Опт-ел. інф-енерг. техн. 2019. 14 листоп. №37. С. 5-10.

15. Chang W. T., Matthieu H., Forestier G., Webb G. I. Efficient search of the best warping window for Dynamic Time Warping: *proceedings of the SIAM International Conference on Data Mining (SDM).*, Melbourne, April 27. 2018. Australia. P. 225-233.

16. Qin A., Hu Q., Zhang Q., Lv Y. Concurrent Fault Diagnosis Based on Bayesian Discriminating Analysis and Time Series Analysis With Dimensionless Parameters. *IEEE Sensors Journal*. 2019. 15 March. Vol. 19, No 6. P. 2254-2265.

17. Narasimhan V., Danecek P., Scally A., Xue Y., Tyler-Smith C., Durbin R. BCFtools/RoH: a hidden Markov model approach for detecting autozygosity from next-generation sequencing data. *Bioinformatics.* 2016. 1 June. Vol. 32, No 11. P. 1749-1751.

18. Pocketsphinx як окрема програма на пристроях Android. URL: https://cmusphinx.github.io/2017/03/pocketsphinx-as-standaloneapp-on-android-wearables/ (дата звернення: 10.11.2021).

19. Accord. NET Framework: Machine Learning Framework. URL: http://accord-framework.ne (дата звернення: 10.11.2021).

20. Голосове керування магнітолою з кнопок на кермі: інструкція. URL: https://caraudio.in.ua/blog/golosovoe-upravlenie-magnitoloy-s-knopok-na-rule/ (дата звернення: 10.11.2021).

21. Pandora: Автомобільна сигналізація. URL: https://pandora.com.ua/products/avtosignalizaciya-pandora-dxl-5000-s (дата звернення: 10.11.2021).

22. Voice Recognition: System. URL: http://webmanual.hyundai.com/STD_GEN5_WIDE/AVNT/EU/voicerecognitionsystem.html (дата звернення: 13.11.2021).

23. Muhammad B.A., Fatima A.N. A comparative study on radio frequency identification system and its various applications. *International Journal of Advances in Applied Sciences (IJAAS)*. 2018. 6 December. Vol. 10, No 4. P. 392-398.

24. Технології розпізнавання голосу: посібник. URL: http://www.sciencemag.org (дата звернення: 21.11.2021).

25. Theology voice control. URL: http://tehnology.com (дата звернення: 22.11.2021).

26. Mohith S., Santhanalakshmi S., Sudhakaren M. Gesture and Voice Controlled Robotic Car using Arduino. *NTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E – ISSN*. 2018. April 24. Vol. 4, No 2. P. 3392-3399.

27. Що таке Android Auto? І як воно працює: інструкція користувача. URL: http://www.rcd330.com.ua/ chto-takoe-android-auto (дата звернення: 05.12.2021).

28. Apple : Apple CarPlay The ultimate copilot. URL: https://www.apple.com/ios/carplay/ (дата звернення 05.12.2021).

29. Google: Android AUTO. URL: https://www.android.com/auto/ (дата звернення 07.12.2021).

30. Ramnath R., Kinnear N., Chowdhury S., Hyatt T. Interacting with Android Auto and Apple CarPlay when driving. *TRL The Future of Transport*. 2020. № 3. P. 12-17. URL: https://trl.co.uk/uploads/trl/documents/PPR948-_IAM-RoadSmart---infotainment-sim-study.pdf (дата звернення 03.01.2022).

31. Mandal A.K., Cortesi A., Ferrara P., Spoto F., Panarotto F. Vulnerability analysis of Android auto infotainment apps. Association for Computing Machinery:

proceedings of the 15th ACM International Conference on Computing Frontiers., (New York, NY, USA, May 08, 2018). Ischia, 2018. P. 183-190.

32. Grocke D. Staying ahead of evolving cyber security threats. *Bulletin*. 2016. Vol. 38, No 9. P 16-18.

33. Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., Savage S., Koscher S., Czeskis A., Roesner F., Kohno T. Comprehensive Experimental. *Analyses of Automotive Attack Surfaces*: 20 USENIX Security Symposium., San Francisco, 10-12 Aug. 2016. P.214-219.

34. Miller C., Valasek C. Remote Exploitation of an Unaltered Passenger Vehicle.2015. № 5. P. 25-29. URL: https://illmatics.com/Remote%20Car%-20Hacking.pdf (дата звернення 14.01.2022).

35. Ramon de Graaff. Controlling your connected car enforcing privacy on telematics data using cryptographic techniques. Eindhoven University of Technology. 2015. № 3. P. 15-21. URL: https://pure.tue.nl/ws/portalfiles/portal/47037140 (дата звернення 15.01.2022).

36. Yunhan J.J., Zhao D., Chen Q.A., Mao M.Z. Towards secure and safe appified automated vehicles. IEEE Intelligent Vehicles Symposium (IV). 2017. T.1, P. 705-711. DOI: 10.1109/IVS.2017.7995800.

37. Cortesi A., Ferrara P., Pistoia M., Tripp O. DatacentricSemantics for Verification of Privacy Policy Compliance by MobileApplications. *VMCAI 2015* : 16th International Conference on Verification, Model Checking, and Abstract Interpretation., Mumbai, Jan. 12-14. 2015. P.61-79.

38. Spoto F. The Julia Static Analyzer for Java. *Conference*: International Static Analysis Symposium., Indonesia, Sept. 16-18. 2016. P.39-57.

39. Що таке Apple CarPlay? Як це працює?: короткий Посібник. URL: https://www.dz-techs.com/apple-carplay-guide#lwptoc2 (дата звернення: 16.01.2022).

40. Sonnenberg J. Service and user interface transfer from nomadic devices to car infotainment systems. *Automotive User Interfaces and Interactive Vehicular Applications*: Proceedings of the 2nd International Conference., Pittsburgh, 11-12 Nov. 2016. Pittsburgh, 2017. P. 162-165.

41. Bose R., Brakensiek J., Park K.Y. Terminal mode: transforming mobile devices into automotive application platforms: *Automotive User Interfaces and Interactive Vehicular Applications:* Proceedings of the 2nd International Conference., Pittsburgh, 11-12 Nov. 2016. Pittsburgh, 2017. P. 148-155.

42. Jegadeesan R., Sankar R. N. Energy Consumption Power Aware Data Delivery in Wireless Network. Circuits and Systems. 2016. Vol. 7, No 10. P. 2829-2836.

43. AppleCarPlay: Quick Start Guide. URL:https://www.dztechs.com/apple-carplay (дата звернення: 18.01.2022).

44. Petridis S., Stafylakis T., Ma P., Tzimiropoulos G., Pantic M. Audio-Visual Speech Recognition with a Hybrid CTC/Attention Architecture. *IEEE Spoken Language Technology Workshop (SLT).* 2018. P. 512-520. DOI: 10.1109/SLT.2018.8639643.

45. Das T.K., Khalid M.O., A Voice Identification System using Hidden Markov Model. *Indian Journal of Science and Technology*. 2016. Vol. 9, No 4. P. 1-6.

46. Як налаштувати Apple CarPlay у своєму автомобілі : керівництво. URL: https://uk.vemprarua.org/how-setup-apple-carplay-your-car (дата звернення: 01.02.2022).

47. Shmatkov V.N., Bonkowski P., Golendukhin V.S. Interaction with Internet of Things devices by voice control. *Technical Journal of Information Technologies*. 2019. Vol. 6, No 2. P. 714-721.

48. WI-FI modem: photo insert. URL: https://3g-digger.com/wifi-v-mashynu (дата звернення: 04.02.2022).

49. Bose introduces quiet comfort road noise control: definition. URL: https://www.bose.com/en_us/pressroom/archive/2019/bose-introduces-quietcomfort-road-noise-control.html (дата звернення: 15.02.2022).

50. Lin J., Niu S., Wijngaarden A J., McClendon J.L., Smith M.C., Wang K.C. Improved Speech Enhancement Using a Time-Domain GAN with Mask Learning. *Proc. Interspeech*. 2020. № 6. P. 3286-3290. URL: https://www.isca-speech.org/archive_v0/Interspeech_2020/pdfs/1946.pdf . (дата звернення: 15.02.2022).

51. Carlini N., Mishra P., Vaidya T., Zhang Y., Sherr M., Wagner D., Zhou W. Hidden Voice Commands. *USENIX Association*: 25th USENIX Security Symposium (USENIX Security 16)., Austin, Aug 10-12, 2016, Austin, 2017. P. 513-530.

52. Центр стратегічних досліджень Національного університету оборони України імені Івана Черняховського: зб. наук. пр. / редкол.: О. М. Загорка ЗАГОРКА та ін. Київ: НУО України імені Івана Черняховського, 2018. 149 с.

53. Feng F., Fawaz K., Kang G. Continuous Authentication for Voice Assistants: *University of Michigan MobiCom'17.* Snowbird, 2017. № 3. P. 6-10.

54. Як використовувати Асистента в режимі "На автомобілі": інструкція користувача. URL: https://support.google.com/assistant/answer/10217503?hl=ru&-ref_topic=10217595 (дата звернення: 10.02.2022).

55. В Android Auto зявиться більше програм: фотовиставка. URL: https://ww w.ajudandroid.com.br/android-auto-novidades-2022/ (дата звернення: 16.02.2022).

56. Що таке атака Дельфінів: експертне пояснення URL: https://fraud watch.com/what-is-a-dolphin-attack (дата звернення: 15.02.2022).

57. Приховані голосові команди: мануал. URL: https://www.usenix.org/usen ixsecurity16/technical-sessions/presentation/carlini (дата звернення: 17.02.2022).

58. Sugawara T., Cyr B., Rampazzi S. Genkin D., Fu K. Light commands: laser-based audio injection attacks on voice-controllable systems. *USENIX Association*: 29th USENIX Security Symposium (USENIX Security 20)., Austin, Aug 17-20, 2019, Austin, 2020. P. 2631-2648.

59. Hei X., Xiaoiiang D. Security, Data Analytics, and Energy-Aware Solutions in the IoT: methodologies. Pennsylvania: IGI Global, 2021 p. 218 c.

60. Kasmi C., Lopes E. J. IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones. *IEEE Transactions on Electromagnetic Compatibility.* 2015. Vol. 57, No 6. P. 1752-1755.

61. Wang G., Martin M.V. SegmentPerturb: *Effective Black-Box Hidden Voice Attack on Commercial ASR Systems via Selective Deletion*: 18th International Conference on Privacy, Security and Trust (PST)., Auckland, 13-15 Dec. 2021. P 1-12.

62. Mukhopadhyay D., Shirvanian M., Saxena N. All your voices are belong to us. *Stealing voices to fool humans and machines*: Proceedings of the European Symposium on Research in Computer Security., Berlin, 18-21 Jan. Berlin, 2018. P 599-621.

63. Ultrasonic Audio Recording Blocker. White Noise Generator: Powerful Microphone Suppressor Device. URL: https://www.amazon.com/Ultrasonic-Recording-Blocker-Generator-BugHunter/dp/B075MBND1N (дата звернення: 01.03.2022).

64. Mehta S.K., Angira M. Selection of Piezoelectric Material for MEMS Technology based Microphone. *Using MCDM Methods*: 2021 International Conference on Intelligent Technologies (CONIT)., Hubli, 25-27 June. 2021. Hubli, 2021. P. 1-5.

65. Wood G.S. Design and Characterization of a Micro-Fabricated Graphene-Based MEMS Microphone. *IEEE Sensors Journal. 2019.* Vol. 19, No 17. P. 7234-7242.

66. He Y., Bian J., Tong X., Qian Z., Zhu W., Tian X., Wang X. Canceling Inaudible Voice Commands. Against Voice Control Systems. *Association for Computing Machiner*: The 25th Annual International Conference on Mobile Computing and Networking., New York, 11 Oct. 2019. New York, 2019. P. 1-15.

67. Dobrucka A. Nonlinear distortions in electroacoustic devices. *Archives of Acoustics* 2011 Vol. 36, No 2. P. 437-460.

68. Nirupam R.., Sheng S., Hassanieh H., Romit R. Inaudible Voice Commands: The {Long-Range}. Attack and Defense. *USENIX Association*: 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18., Renton, Apr. 9-11, 2018, Renton, 2018. P. 547-560.

69. Davidson D., Wu H., Jellinek R., Ristenpart T., Singh V. Controlling UAVs with Sensor Input Spoofing Attacks. *USENIX Association*: 10th USENIX Workshop on Offensive Technologies (WOOT 16)., Austin, Aug 8-9, 2016, Austin, 2016. P. 438-469.

70. Wang Z., Zou Q., Song Q., Tao J. The era of silicon MEMS microphone and look beyond, International Conference on Solid-State Sensors. *Micromachines.* 2020. Vol. 11, No 5. P. 1-26.

71. Himanshu P., Hardik M. Fingerprint Based Vehicle Ignition System. *Fuzzy Systems*. 2018. Vol. 10, No 3. P. 64-67.

72. Trainys T., Venčkauskas A. Encryption Keys Generation Based on Bio-Cryptography Finger Vein Method. *CEUR Workshop Proceedings*:International Conference on Information Technologies., Kaunas, Apr. 27. 2018. Kaunas, 2018. P. 106-111.

73. Rajan C., Megala B., Nandhini A., Priya C. Comparative Analysis of Arduino Micro Controllers in Robotic Car. *International Journal of Mechanical and Materials Engineering*. 2015. Vol. 9, No 2. P.371-380.

74. Arduino UNO: photo print. URL: https://doc.arduino.ua/hardware/Uno (дата звернення:07.04.2022).

75. Сканер відбитка пальця: фотовиставка. URL: https://www.robo store.com.ua/otladochnye-platy/esp-moduli/skaner-otpechatka-palca-fpm10a/ (дата звернення: 08.04.2022).

76. LCD 1602 символьний дисплей 16x2(синій). URL: https://arduino.ua/prod169-lcd-1602-simvolnii-displei-16x2-sinii (дата звернення: 10.04.2022).

ДОДАТОК А
(обов'язковий)

ЛІСТИНГ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДОДАТКОВОЇ АВТОМОБІЛЬНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ВОДІЯ

Підключення бібліотек:

```
#include <Wire.h>  // Бібліотека роботи з шиною;
#include <LiquidCrystal_I2C.h>LiquidCrystal_I2C lcd(0x27,16,2) //Для
роботи з LCD дисплеєм 16x2;
#include <Adafruit_Fingerprint.h> // Для сканера відбитків пальця
FPM10A;
#include <SoftwareSerial.h>  // Бібліотека для UART;
SoftwareSerial  mySerial(3, 4);    // Визначаємо об'єкт
SoftwareSerial для роботи з бібліотекою;
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);  //
Визначаємо об'єкт для бібліотеки;
#include<Servo.h> // Бібліотека для роботи з сервомотором;
Servo motServo; // Присвоєння імені сервомотору;
```

Модуль « Зчитування в автомобільній системі біометричної аутентифікації відбитка пальця користувача та виконання певних дій (запуску системи автомобіля)».

```
for (int i = 0; i <5; i ++)
   {
      lcd.clear ();
      lcd.print ("Put your finger");
      delay (1900);
      int result = getFingerprintIDez ();
      if (result> = 0)
          digitalWrite (openLight, HIGH);
          digitalWrite (closeLight, LOW);
          lcd.clear ();
```

```
        lcd.print ("Confirmed");
        lcd.setCursor (0,1);
        lcd.print ("Start System");
        motServo.write (0);
        delay (5000);
        motServo.write (150);
        digitalWrite (closeLight, HIGH);
        digitalWrite (openLight, LOW);
        lcd.setCursor (0,1);
        lcd.print ("Start the car system”)
```

Модуль «Зчитування відбитка пальця, конвертування його в шаблон та збереження його з вибраним індикатором у пам'ять модуля датчиків відбитків пальців»

```
    int p = -1;
    lcd.clear ();
    lcd.print (ID: ");
    lcd.print (id);
    lcd.setCursor (0,1);
    lcd.print ("Put your finger");
    delay (2000);
    while (p! = FINGERPRINT_OK)
    {
      p = finger.getImage ();
```

Модуль «Видалення запису вибраного ідентифікатора з системи».

```
{
    unit5_t p = -1;
    lcd.clear ();
    lcd.print ("Wait");
    p = finger.deleteModel (id);
    if (p == FINGERPRINT_OK)
    {
      Serial.println ("Deleted");
      lcd.clear ();
      lcd.print ("Finger Scan Removed");
      lcd.setCursor (0,1);
      lcd.print ("Done");
      delay(600);
```

Вихідний код додаткової автомобільної системи біометричної аутентифікації водія:

```
#define enroll 14
#define del 15
#define up 16
#define down 17
#define openLight 6
#define closeLight 7
#define servoPin 5
void setup()
{
    delay(600);
    motServo.attach(servoPin);
    motServo.write(150);
    pinMode(enroll, INPUT_PULLUP);
    pinMode(up, INPUT_PULLUP);
    pinMode(down, INPUT_PULLUP);
    pinMode(del, INPUT_PULLUP);
    pinMode(openLight, OUTPUT);
    pinMode(closeLight, OUTPUT);
    lcd.begin(16,2);
    lcd.print("Driver Safety System");
    lcd.setCursor(0,1);
    lcd.print("behind the finger scan");
    delay(1500);
    lcd.clear();
    finger.begin(57600);
    Serial.begin(9600);
    lcd.clear();
    lcd.print("Search sensor module ");
    lcd.setCursor(0,1);
    delay(600);
    if (finger.verifyPassword())
    {
```

```
      Serial.println("Scanner Sensor Module Found// модуль сканера
відбитків пальців знайдено
      lcd.clear();
      lcd.print("Scanner Found");
      delay(600);
    }
}
void loop()
{
 lcd.setCursor(0,0);
 lcd.print(""Press up or down ");
 lcd.setCursor(0,1);
 lcd.print("to run");
 digitalWrite(closeLight, HIGH);
 if(digitalRead(up)==0 || digitalRead(down)==0)
 {
  for(int i=0;i<5;i++)
  {
    lcd.clear();
    lcd.print("Put your finger to the scanner"");
    delay(1500);
    int result=getFingerprintIDez();
    if(result>=0)
    {
        digitalWrite(openLight, HIGH);
        digitalWrite(closeLight, LOW);
        lcd.clear();
        lcd.print("Passed");
        lcd.setCursor(0,1);
        lcd.print("Start system   ");
        motServo.write(0);
        delay(4900);
        motServo.write(150);
        return;
     }
```

```
    }
  }
  checkKeys();
  delay(600);
}
void checkKeys()
{
    if(digitalRead(enroll) == 0)
    {
     lcd.clear();
     lcd.print("You have to wait");
     delay(600);
     while(digitalRead(enroll) == 0);
     Enroll();
    }
    else if(digitalRead(del) == 0)
    {
     lcd.clear();
     lcd.print("You have to wait");
     delay(600);
     delet();
    }
}
void Enroll()
{
    int count=0;
    lcd.clear();
    lcd.print("Register a finger in the system    ");
    lcd.setCursor(0,1);
    lcd.print("Location for scanning:");
    while(1)
    {
      lcd.setCursor(9,1);
      lcd.print(count);
      if(digitalRead(up) == 0)
```

```
      {
        count++;
        if(count>25)
        count=0;
        delay(400);
      }
      else if(digitalRead(down) == 0)
      {
        count--;
        if(count<0)
        count=25;
        delay(400);
      }
      else if(digitalRead(del) == 0)
      {
           id=count;
           getFingerprintEnroll();
           return;
      }
        else if(digitalRead(enroll) == 0)
      {
           return;
      }
 }
}
void delet()
{
   int count=0;
   lcd.clear();
   lcd.print("Remove the fingerprint ");
   lcd.setCursor(0,1);
   lcd.print("Location for scanning:");
   while(1)
   {
     lcd.setCursor(9,1);
```

```
      lcd.print(count);
      if(digitalRead(up) == 0)
      {
        count++;
        if(count>25)
        count=0;
        delay(400);
      }
      else if(digitalRead(down) == 0)
      {
        count--;
        if(count<0)
        count=25;
        delay(400);
      }
      else if(digitalRead(del) == 0)
      {
           id=count;
           deleteFingerprint(id);
           return;
      }
        else if(digitalRead(enroll) == 0)
      {
           return;
      }
 }
}
unit5_t getFingerprintEnroll()
{
  int p = -1;
  lcd.clear();
  lcd.print("Identeficator:");
  lcd.print(id);
  lcd.setCursor(0,1);
  lcd.print("Put your finger ");
```

```
  delay(1500);
  while (p != FINGERPRINT_OK)
  {
    p = finger.getImage();
    switch (p)
    {
    case FINGERPRINT_OK:
      Serial.println("Image created"); // Зображення сканування
відбитка пальця захоплено
      lcd.clear();
      lcd.print("Image created");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.println("Not found"); // Зображення сканування не
знайдено
      lcd.clear();
      lcd.print("Not found");
      break;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Error""); // Помилка сканування зображення
відбитка пальця
      lcd.clear();
      lcd.print("Error");
      break;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Scan error");
      lcd.clear();
      lcd.print("Scan error"); // Помилка сканування зображення
  }
  p = finger.image2Tz(1);
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Finger scan transformed "); // Зображення
перетворено
      lcd.clear();
```

```
      lcd.print("Finger scan transformed ");
      break;
    case FINGERPRINT_IMAGEMESS:
      Serial.println("The fingerprint is contaminated "); //
Зображення відбитка пальця брудне
       lcd.clear();
       lcd.print("The fingerprint is contaminated ");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Error");
      lcd.clear();
      lcd.print("Error");
      return p;
    case FINGERPRINT_FEATUREFAIL:
      Serial.println("Functions not found "); // Функції відбитків
пальців не знайдено
      lcd.clear();
      lcd.print("Functions not found ");
      return p;
    case FINGERPRINT_INVALIDIMAGE:
      Serial.println("Functions not found ");
      lcd.clear();
      lcd.print("Not found ");
      return p;
  }

  Serial.println("Remove finger"); // Видаленн відбитка пальців
користувача
  lcd.clear();
  lcd.print("Remove Finger"); // Заберіть палець з сканера відбитків
пальців
  delay(1500);
  p = 0;
  while (p != FINGERPRINT_NOFINGER) {
    p = finger.getImage();
```

```
  }
  Serial.print("ID "); Serial.println(id);
  p = -1;
  Serial.println("Put your finger back "); // Покладіть той самий
палець на сканер
   lcd.clear();
      lcd.print("Place Finger");
      lcd.setCursor(0,1);
      lcd.print("   Back");
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image created "); // Зображення сканування
захоплено
      break;
    case FINGERPRINT_NOFINGER:
      Serial.print(".");
      break;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Error");
      return;
    }
  }
  p = finger.image2Tz(2);
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image redesigned");
      break;
    case FINGERPRINT_IMAGEMESS:
      Serial.println("Contaminated image");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Error");
      return p;
```

```
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Scan function not found");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Find fingerprint features");
    return p;
  default:
    Serial.println("ERROR");
    return p;
}

Serial.print("Creating model for #");  Serial.println(id);

p = finger.createModel();
if (p == FINGERPRINT_OK) {
  Serial.println("The scan matches");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("ERROR");
  return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
  Serial.println("Scans do not match ");
  return p;
} else {
  Serial.println("ERROR");
  return p;
}

unit5_t p = finger.getImage();

if (p != FINGERPRINT_OK)
return -1;
p = finger.image2Tz();
if (p != FINGERPRINT_OK)
return -1;
p = finger.fingerFastSearch();
```

```
  if (p != FINGERPRINT_OK)
  {
   lcd.clear();
   lcd.print("The scanner did not find a finger ");
   lcd.setCursor(0,1);
   lcd.print("Again");
   delay(1500);
  return -1;
  }
  // found a match!
  Serial.print("id #");
  Serial.print(finger.fingerID);
  return finger.fingerID;
}
unit5_t deleteFingerprint(unit5_t id)
{
  unit5_t p = -1;
  lcd.clear();
  lcd.print("Wait"); // Потрібно зачекати
  p = finger.deleteModel(id);
  if (p == FINGERPRINT_OK)
  {
    Serial.println("Removed scan!");
    lcd.clear();
    lcd.print("Removed scan "); // Палець видалено
    lcd.setCursor(0,1);
    lcd.print("OK"); //
    delay(600);
  }
}
```

ДОДАТОК Б
(обов'язковий)

ПУБЛІКАЦІЯ У ФАХОВОМУ ЖУРНАЛІ

Є.Г.ГНАТЧУК, В.Ю. БАШУК, Д.С. КВАСНІЦЬКИЙ

Хмельницький національний університет

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ СПЕЦІАЛІЗОВАНОЇ КОМПЮТЕРНОЇ СИСТЕМИ ГОЛОСОВОГО КЕРУВАННЯ АВТОМОБІЛЕМ

В роботі досліджено методи та засоби захисту забезпечення надійності в сучасних спеціалізованих комп'ютерних системах голосового керування автомобілем. Проведена оцінка характеристик та властивостей системи. Розглянуто основні принципи роботи та різні можливості конструкцій голосового керування автомобілем. Показано моделі і методи виявлення небезпек, і визначено недоліки та вразливості автомобільних систем «Android Auto» та «Apple CarPlay» щодо впливу зловмисного програмного забезпечення на основі сучасних способів кібератак. Проведено аналіз роботи та показано підготовку для здійснення кібератаки ультразвуковими та світловими командами на системи голосового керування автомобілем. Запропоновано методи та засоби для підвищення ступеня захисту системи голосової аутинтефікації спеціалізованих комп'ютерних систем «Android Auto» та «Apple CarPlay». Окремо представлено кожний метод його кроками. Створено та показано алгоритми роботи програмних та апаратних методів забезпечення надійності від кібератак. В результаті узагальнення літератури для забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем, виявлено низку проблем, основними з яких є недосконалість системи аутентифікації користувача.

Для реалізації вирішення даної проблеми було створено та розроблено апаратно-програмний продукт додаткової біометричної автомобільної системи аутентифікації користувача. Система була створена для забезпечення надійності від кібератак на систему голосового керування.

Проведені експериментальні дослідження підтверджують ефективність системи біометричної аутентифікації як запропонованого рішення щодо забезпечення додаткового методу захисту.

Ключові слова: системи голосового керування, метод, захист, ультразвукові атаки

YELYZAVETA HNATCHUK, VITALII BASHUK, DENYS KVASNITSKYI

Khmelnytskyi National University

RESEARCH OF METHODS AND MEANS OF ENSURING THE RELIABILITY OF A SPECIALIZED COMPUTER VOICE VEHICLE CONTROL SYSTEM

The methods and means of protection of reliability in modern specialized computer systems of voice control of the car are investigated in the work. The evaluation of the characteristics and properties of the system is carried out. The basic principles of work and various possibilities of constructions of voice control of the car are considered. Models and methods of hazard detection are shown, and the shortcomings and vulnerabilities of Android Auto and Apple CarPlay car systems to the impact of malicious software based on modern methods of cyber attacks are identified. The analysis of work is carried out and preparation for carrying out cyber attack by ultrasonic and light commands on systems of voice control of the car is shown. Methods and means to increase the level of protection of the voice authentication system of specialized computer systems "Android Auto" and "Apple CarPlay" are proposed. Each method is presented separately by its steps. Algorithms of work of software and hardware methods of ensuring reliability from cyberattacks are created and shown. As a result of summarizing the literature to ensure the reliability of a specialized computer voice control system, a number of problems have been identified, the main of which is the imperfection of the user authentication system.

To implement the solution to this problem, a hardware and software product of an additional biometric automotive user authentication system was created and developed. The system was created to ensure the reliability of cyber attacks on the voice control system.

Experimental studies confirm the effectiveness of the biometric authentication system as a proposed solution to provide an additional method of protection.

Keywords: voice control systems, method, protection, ultrasonic attacks

Introduction

Today, information technology is evolving widely and progressively every day in all directions, and it affects each of us. One of the important aspects is the possibility of voice control. Voice-controlled systems are widely used in various industries, including automotive engineering. The urgency of the work is to develop methods and hardware and software to ensure the reliability of voice control of the car.

When designing a system, it is necessary to take into account and use the features of the tasks assigned to them, which can be performed under the influence of modern methods of cyber attacks. In this regard, the necessary scientific task is to develop a special hardware and software that will provide opportunities to increase the reliability and protection against criminal cyber attacks on the voice control system.

Subject area analysis and relevant decisions

Problems solved in computer information systems have a number of characteristic features that affect the technology of automated data processing.

The computer system has the ability to integrate with other engineering technologies, expand capabilities and create a unified management environment, using the diversity and unification of computer equipment [1].

Dedicated computer voice control system helps you with voice commands to control functions such as navigating the route in the navigator, using climate control and its functionality, controlling the multimedia system, it also has the ability to interact with the user. With the help of voice assistants, the system can respond to voice commands and display various information on the screen of the driver's multimedia device.

In modern cars, voice control is performed by uttering the appropriate commands, which by undergoing certain transformations are converted into control signals for the respective systems. Today, you can use voice control to control the following systems in the car (Table 1).

Table 1 - Voice control systems

System type	Виконання функції
Climate control	With the help of the climate control system, the user can change the temperature, turn on the seat heating, change the fan speed and more.
Multimedia	Provides the ability to receive, transmit, video and audio information.
Navigation	Perform voice control of the car navigation system
On-board computer	Determining the parameters of the car

In the voice control system, one of the main functions is voice recognition, which allows you to control the mobile phone connected to it, use the various features of the multimedia system, use the radio, navigation system and much more.

Entering voice commands greatly reduces your time and control, which in turn helps you focus on the road and driving. It is also possible to use voice commands to interact with navigation systems, ie paving or changing routes, etc. Voice control systems support a variety of languages, including the unpopular ones.

The process of voice recognition in specialized computer voice control systems (Figure 1) takes place in several stages. At each stage, a number of different methods are used to process the material signal. The process of voice recognition can be divided into three stages:

- receiving a voice signal and processing commands;

- recognition of phonemes and words;

- understanding of the voice command.

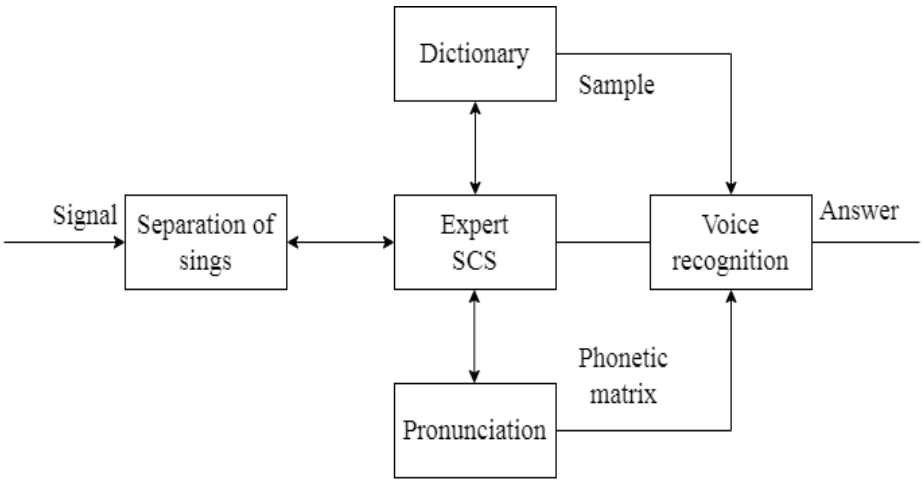


Figure 1. Scheme of the voice recognition process

The process of automatic determination of "who speaks" is performed on the basis of individual information input to the voice signal [2]. When driving a vehicle, human voice and gesture commands are entered as input data of the vehicle [3].

Today, the most popular car voice control systems are Android Auto [4] and Apple CarPlay [5]. To use the car's voice control functions, these systems use voice assistants.

After analyzing the operation of the car system "Android Auto", we can conclude that one of the problems is the voice control system - it's voice authentication. Due to this problem, criminals can perform cyber attacks, so-called inaudible or ultrasonic commands (DolphinAttak), on voice control systems.

To ensure the reliability of this system, you can use the method of "Hidden Markov model" [6]. There are two ways to send a voice signal to your device. They use the phonetic and whole word approach. The method is to identify the speaker and authorize it next to the voice database. First, the system learns with the help of certain voices, then it is tested with an unknown voice and then the system recognizes the user who owns the unknown voice. The recognition system is divided into two subsystems, such as text-dependent and text-independent.

Also, the car system "Android Auto" with voice control is vulnerable to other types of cyberattacks, such as attack by light commands performed by, giving a light command to the microphone of the voice control system with a special device for example, tinting car windows and more.

Analyzing the work of the car system "Apple CarPlay", we can conclude that the problem of voice assistant is often cloud data processing and dependence on the quality of Internet connection. So you need a quality and fast internet connection to ensure the reliability of your voice control system. To do this, you can buy a 3G / 4G WI-FI raster in the car, which will ensure the speed of your system with cloud data processing. The router can be connected to the car's cigarette lighter, to the USB port of your car, depending on your choice and characteristics of the car. But we should not forget that it is impossible to connect and configure devices from other manufacturers often enough, or they will work with limited functionality [7].

High-quality and stable Internet connection will also help to solve another shortcoming of the use of voice control, namely the malfunction, various system failures due to untimely software updates. To resolve this issue, you need to update your device to the latest available software version.

Another very serious problem that is often encountered with the voice assistant in the system "Apple CarPlay" is that it can read voice commands that were not assigned to it, ie respond to different types of noise, also due to noise voice control system may misunderstand and perform your voice team. To solve this problem, you can use the development of a system from Bose.

The company has developed a "QuietComfort Road Noise Control" system that can be installed in your car to reduce noise levels, which will ensure reliable voice control. The system consists of microphones and a set of accelerators, using acoustics installed in the car, filtering background noise, the system increases the clarity of voice commands and expands the possibilities of voice control.

You can also use the method of speech enhancement integrates the display of characteristics, time domain in a unified structure using the GAN network, it processes voice command waves and separates speech and noise signals coming into two one-dimensional layers of Fourier transform convolution, which reflect signal shapes in speech and noise

spectrograms, which in turn are used to calculate losses. This method is superior to methods for improving voice commands, based on the DNN neural network.

One of the significant shortcomings of automotive systems is the voice authentication mechanism, for example, a criminal can bypass the security function of the voice assistant by pretending to be the owner by attacking light commands, thereby gaining unauthorized access to the vehicle. The study clearly demonstrated [8] how you can secretly and remotely enter voice commands with your own voice, in various ways without even attracting the attention of users.

To ensure reliability, you can use the method of dynamic time scale transformation (DTW) [9]. This method allows you to find the proximity, for two measurement sequences, in a certain period of time. It can be used to recognize a voice command if two speech signals represent the same output voice command, even at different speeds and lengths. One of the advantages of this method is ease of implementation.

Apple CarPlay, like Android Auto, is also vulnerable to cyberattacks, such as light commands. Next, the example of the threat model will show how such an attack occurs. The purpose of the thief is to remotely enter commands that pose a threat to the user's device, using a special device (laser). For example, an offender does not have physical access to a user's device, so he cannot change settings that are not available by voice, but he can gain remote access to the target device and its microphone by entering light commands. It should also be noted that remote access to the target device allows you to monitor the LEDs of the device, which in turn shows him how they react (light up) after recognizing the voice command and allows remote use as feedback. to determine the success of the attack attempt. To protect the reliability of the voice control device in the car as protection, you can use both hardware and software protection.

Methods of ensuring the reliability and protection against modern methods of cyber attacks on the voice control system

Today, Apple's Siri or Google Assistant voice assistants, used for voice control on Apple CarPlay [4] and Andoid Auto [5], respectively, are becoming popular. the method of human interaction with the car through voice control. With the advent of these systems, there has also been a need to provide protection for them. As previously described, these systems have a common vulnerability to the voice authentication system.

Next, we will discuss the methods of protection and reliability against cyber attacks by ultrasonic and light commands on a specialized computer system of voice control of the car. It should be understood that the voice control system, which depends directly on the speaker, is performed locally, and not the dependent voice control system is performed through the cloud service [10].

When a user uses a cloud service, signals that have been pre-processed are sent to servers where these signals will be recognized by machine algorithms. If the SCS recognizes the command, it will run the program to perform the operation. All commands and actions are system dependent and defined. Dedicated computer voice control systems have a wide range of functions and voice commands that are quite difficult to activate. Most security research for voice control systems focuses on cyberattacks, voice recognition algorithms [11], or malicious software.

In order to have access to control of the voice control system, Dolphin Attack must generate activation commands before the general introduction of voice control commands. Next, on the example of the voice assistant "Siri" who works in "Apple CarPlay" [4], how exactly is the generation of voice commands. Siri Voice Assistant works in two modes, namely activation and recognition. Before executing voice commands, you need to activate it, so you need to generate two types of voice commands, for activation and basic control commands. Activation is considered successful if the voice command meets the requirements: has wake-up words "Hello, Siri" and mimics the user's voice under which the

voice assistant was trained. For a thief, creating an activation team is quite difficult, unless of course he is able to record the words of the user's activation.

Generating a certain voice in "Hello, Siri" using the current speech methods and functions extracted from the recordings [12] is extremely difficult, and sometimes not possible at all, because it is unclear what set of functions is required for voice identification. Therefore, you can use two methods to create activation commands for the voice assistant.

DolphinAttax can use different voice command activation kits, with different voice tones, using speech synthesis systems. The method is used when the offender has the ability to write words or phrases of the user, with the possibility of further breaking them into phonemes and combining them into different words, including those necessary for activation.

After undergoing activation, the offender may have access to general voice control commands. it is possible to select the text of the control command and create it using language synthesis systems. The voice recognition system does not verify the identity of the control commands.

To ensure the reliability of voice control of the car, from ultrasonic (inaudible) cyber attack, I want to offer my own method of protection, which will use hardware protection and contain a device for future use.

The specialized computer voice control systems "Android Auto" [5] and "Apple Car Play" [4] have shortcomings with voice authentication. That is, the criminal for a successful cyber attack (DolphinAttack) must first remotely send an inaudible (ultrasonic) signal to wake up the system.

Such a signal, the offender can receive by recording the voice of the user on whose device the cyberattack will be directed, to further break the signal into words that are necessary for activation. The proposed method will help increase the protection of the system in the first stage of preparation for a successful cyber attack.

The essence of the method is to reduce the possibility of the offender to obtain a recording of the user's voice. To do this, use an ultrasonic microphone recording blocker. To date, there are many different types, with different characteristics and capabilities .. Next (Figure 2), will show the use of an ultrasonic blocker using the algorithm of this device.

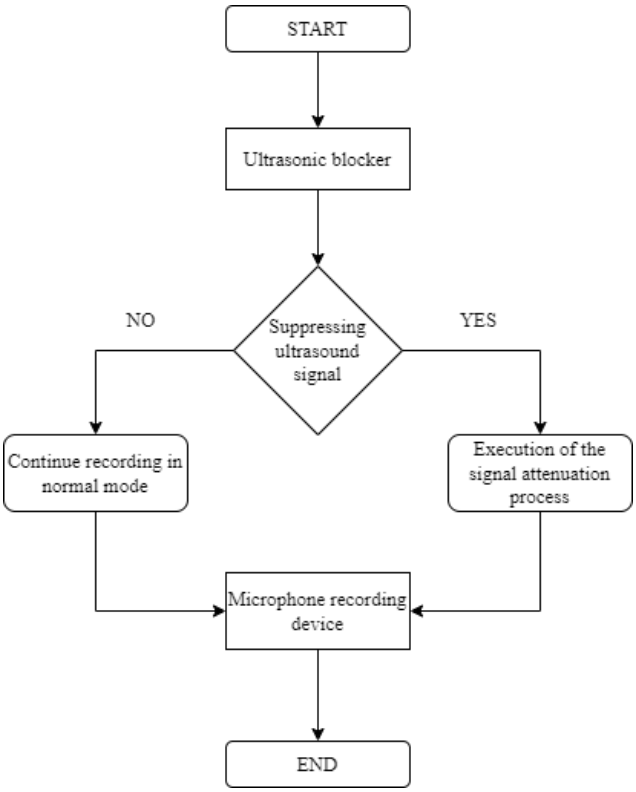


Figure 2. Scheme of the algorithm of ultrasonic recording blocker

The size of the device is quite small and comfortable, and most importantly invisible, which makes it easy to install in the car showroom or anywhere else.

The next step will be to assess the effectiveness of Dolphin Attack's impact on various factors and methods of protection for them. For a cyberattack, the speed of recognition of different types of voice commands will not differ. Voice assistants such as Siri or Google Assistant are recommended for use in car voice control systems with minimal background noise, as SGCs are sensitive and can lead to incorrect analysis and execution of user-defined voice commands.

As the cyberattack is performed remotely, the level of background noise increases as the distance increases, as previously described, which can lead to incorrect recognition of the voice command. Next, the methods and means of protection in cyber attacks on the voice control system will be evaluated. Both hardware and software methods can be used for protection.

Hardware protection is to improve the SGC microphone and its characteristics. The main reason for a successful cyber attack is that the microphone can receive acoustic commands above 20 kHz, although ideally it should not.

In general, most microphones allow signals above 20 kHz [13], so the microphone should be extended and designed to curb acoustic signals in which the frequency is in the range of ultrasonic commands.

You can add a low-pass filter module to the microphone to detect modulated voice commands and cancel the bandwidth using modulated voice commands. This allows you to detect signals in the frequency range of the ultrasound, showing the modulation characteristics and where to modulate these signals to obtain the main frequency band.

To provide software, you need to use the unique properties of voice commands that distinguish them from the real thing. Figure 3 shows a demodulated cyberattack signal that differs from the original signal and that recorded at high frequencies in the range of 800-2400 Hz.

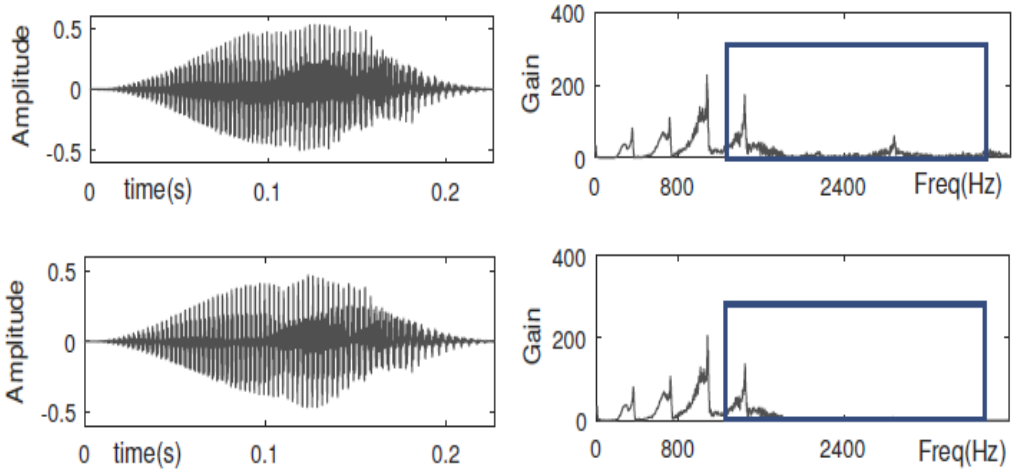


Figure 3. Difference of demodulated signal from original [14]

The original signal produced by the Google TTS engine has a frequency of 25 kHz for modulation, so it is possible to detect "Dolphin Attack" by performing a frequency analysis in the range from 800 to 2400 Hz. To confirm the feasibility of detecting a cyber attack, the method of reference vectors as a classifier and extraction from audio functions in the frequency and time domain.

Using the created voice commands "Hello, Siri", with the help of special programs for converting text into a voice command, two samples of voice commands were obtained, in which one was recorded and the other was played. In order to teach the classifier on the method of reference values, to detect malicious voice commands, it is necessary to use several recorded audio samples, other samples can be used for testing. The classifier can distinguish restored audio recordings from those recorded with a true positive result and a negative value of one hundred percent.

The result of using a classifier made by the method of reference vectors, shows that this software method of protection can be detected for malicious cyberattacks.

The next method of protection against inaudible cyberattacks will be to search for and detect signs of non-linearity of the signal that is transmitted to the microphone of the voice control system. To do this, you need to understand whether it is possible to identify traces of non-linearity, which the offender will not be able to get rid of. But first you need to understand exactly how acoustic nonlinearity works.

In general, microphones and speakers are designed as linear systems, which means that the output signals are linear combinations of input signals. In the power amplifier used in microphones and speakers, the input audio signal is s (t), then the output signal should ideally be:

$$S_{out}(t) = A_1 s(t)\,, \tag{1}$$

where A1 is the gain of the amplifier;

In practice, components in microphones can usually be linear only in audible frequency ranges, ie greater than 20 kHz. In ultrasonic bands where the frequency is less than 25 kHz, they do not show linearity [15]. It follows that for ultrasonic signals the output of the amplifier is calculated:

$$s_{out}(t) = \sum_{i=1}^{\infty} A_i s^i(t) = A_1 s(t) + A_2 S^2(t) + A_3 S^3 \cdots \approx A_1 s(t) + A_2 S^2(t) \quad (2)$$

[16] shows how it is possible to reproduce ultrasonic signals that can be recorded by a microphone, but they will be inaudible to humans. In the ultrasonic speaker there is a possibility of reproduction of two inaudible tones:

$s_1(t) = \cos(2\pi f_1 t)$ with frequency $f_1 = 38$ kHz i $s_2(t) = \cos(2\pi f_2 t)$ with $f_1 = 40$ kHz.

When the combined signal passes through a nonlinear microphone at the output it becomes:

$$s_{out}(t) = A_1 s_{hi}(t) + A_2 s_{hi}^2(t) = A_1\big(s_1(t) + s_2(t)\big) + A_2(s_1(t) + s_2(t))^2$$

$$= A_1 \cos(2\pi f_1 t) + A_1 \cos(2\pi f_2 t) + A_2 \cos^2(2\pi f_1 t) + A_2 \cos^2(2\pi f_2 t)$$

$$+2A_2 \cos(2\pi f_1 t)\cos(2\pi f_2 t), \quad (3)$$

This signal has frequency componentsv f_1, f_2, $2f_1$, $2f_2$, $f_2 + f_1$ and $f_2 - f_1$. The microphone before, digital processing and recording uses a low-pass filter to remove components higher than 24 kHz. So frequencies

$$s_{low}(t) = A_2 + A_2 \cos(2\pi(f_2 - f_2)t), \quad (4)$$

In general,, $f_2 - f_1 = 2$ kHz з recorded by the microphone, this shows a property that allows you to send an inaudible signal, with the ability to generate a copy of the sound in the middle of the microphone.

Thus we mark the signal of the voice command: "Siri, pave the route…", which was pronounced by the user - $v(t)$, when he will say this command, the expression will be executed:

$$s_h = v(t) + n(t), \quad (5)$$

where $n(t)$- microphone noise;

Let the offender reproduce this voice command using ultrasound, recorded signal s_{atk} look like:

$$s_{atk} = \frac{A_2}{2}(1 + 2v(t) + v^2(t)) + n(t), \quad (6)$$

Figure 4 shows the spectrum of the voice command for the s_h and s_{atk}, as these signals are almost similar in structure, which means that the text converter outputs the same text for the s_h and s_{atk}.

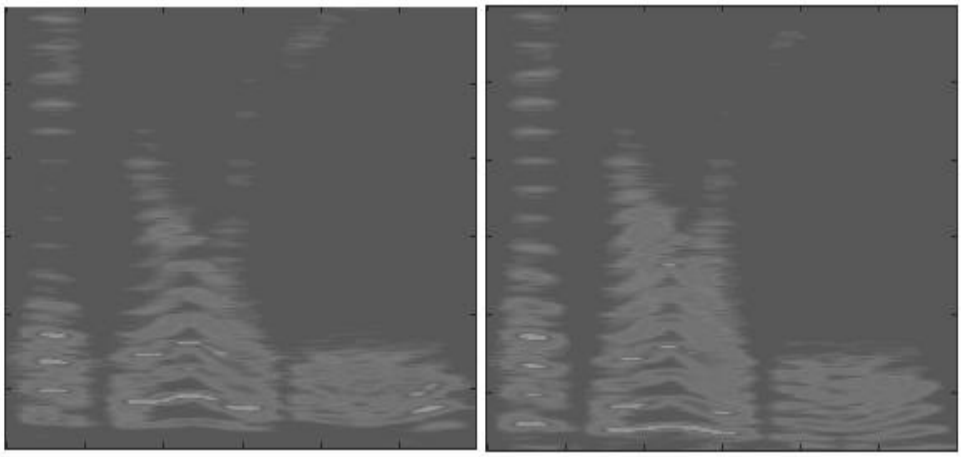


Figure 4. Spectrogram for signal s_h and s_{atk}k, voice command "Siri, pave route…"

Based on this, we can conclude that for protection you need to check any signal (input) and determine whether it is a low-frequency user-specified, or a copy of the high-frequency cyber attack.

Attack by light commands is similar to cyberattacks by ultrasonic commands, the difference is that it uses a special device (laser) to attack. Hardware and software protection methods are used to protect against this type of attack. The software method of protection is to apply an additional level of authentication to the voice control system. In [17], the authors use an additional step of user authentication, thus trying to protect against the execution of unauthorized conference commands. The method is to use an additional authentication step before executing critical commands and reduce attempts to enter the wrong password if the system supports this feature.

This method can also help if the offender is unable to hear the response of the voice control system because it is far from the attacked device. For example, the system will ask any random question before executing a voice command, to which the offender will not be able to answer, thus stopping the attack.

The next method of protection is to use the operation of sensor algorithms, and use methods of merging them to detect commands entered on the basis of light [18]. Voice assistants often have and use multiple microphones. The essence of the method is that the offender uses one special device (laser) to attack light commands and uses only one microphone that receives the signal, while other microphones do not receive anything. So you can try to detect the attack using comparisons of signals from multiple microphones, ignoring voice commands that are entered using a special device (laser). This method can be effective only when one attacking device is running.

The imperfections of specialized computer systems with voice control of the car, namely with the problems of authentication or lack thereof in general, allow criminals to access various functions and capabilities of the car. Using various types of cyberattacks, such as attacks by light commands, or the introduction of inaudible (ultrasonic) commands,

with the help of special devices aimed at microphones of voice control of the car, will allow criminals to bypass the imperfections of the driver authentication system.

The previously described protection methods allow to ensure the reliability of the car's voice control systems, quite effectively, but not as much as possible. As a result of the review of the original sources of the authentication system of different cars, the material obtained, the analysis of which led to the conclusion that to ensure the reliability of the car voice control system, you need to use an additional authentication system that will allow only the driver or proxies. system management and more. To solve the problem of additional authentication, an autonomous security system will be created, with the possibility of direct authentication using the fingerprints of the car owner or proxies. The main components of the system will be the Arduino UNO board, fingerprint scanner, LCD display, servomotor. The Arduino IDE will be used to download code and program the Arduino UNO board. The algorithm of the system (Figure 5) shows that if the user is not authenticated correctly, the system will not be able to provide access to the car's functions.

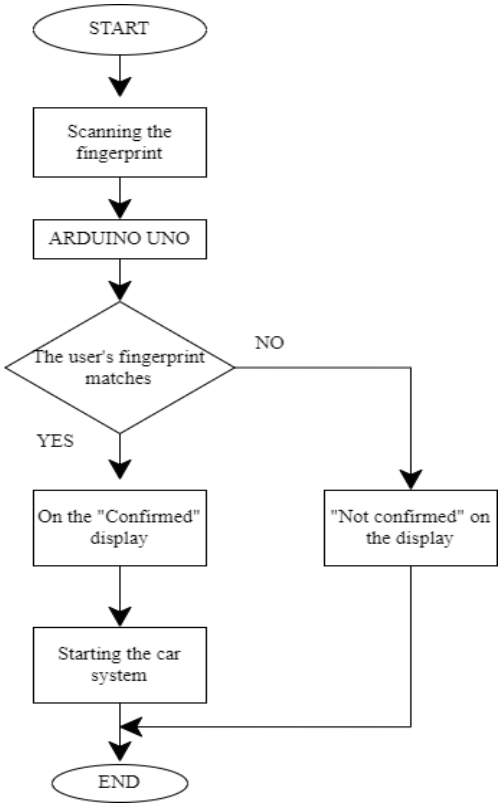


Figure 5. Block diagram of the biometric authentication system algorithm

Biometric fingerprint recognition technology is a new and modern method for ensuring reliability and protection for security systems. This method uses the physical presence of the user to authenticate the user. Today, fingerprint recognition is widely used in various biometric systems, such as telephones, smart devices, biometric locks, bank payments and more [19]. The use of biometric authentication as a personal code as a personal code is considered a traditional method.

The use of this biometric authentication system will be quite reliable and will allow the user to provide reliability for specialized computer systems of the car, and block the criminal's access to the voice control system, which in turn will prevent various methods of cyberattacks

Known approaches to solving this problem are based on the work [20], which states that biometric security technologies are one of the most effective protection systems, and are increasingly becoming everyday attributes in the lives of ordinary people. In recent years, these systems have become widespread in the production of mobile technology, ie smartphones are built-in fingerprint scanners, voice recognition and more.

Particular attention is paid to the problem of authentication, related to the development of methods and tools to ensure the reliability of the car's SCS. That is, through the process of authentication of a person, using the comparison of its characteristics with the characteristics that were previously entered into the system, it is possible to determine as accurately as possible whether the user has appropriate access to the requested information or not. This makes it possible to ensure the reliability of the current problem of information security.

An important point for research in automotive authentication systems is the fact that in today's world there is a high demand for reliable and safest systems in vehicles. Thus, the design and development of hardware and software biometric security system using fingerprint technology to prevent unauthorized access to the car is simple and useful to use. The hardware and software implementation of the system will use an additional method of user authentication, which will be based on the ability to start the car's ignition system, which in turn will use its functionality and prevent its use in case of incorrect biometric authentication with fingerprint.

Fingerprint sensor, allows you to match the image of the user's fingerprint with what is stored in the system memory of the sensor. The research program focuses on a tool to obtain answers and follow instructions according to the results obtained, using the Android Uno microcontroller and includes the following security issues. Who use the analysis of the obtained results and check whose fingerprints can get access rights to turn on a specialized computer system of the car.

Experimental results and analysis of an additional user authentication system

Checking access to the car's biometric authentication system can be considered successful if the user turns on the car's system using their own fingerprint, which is registered in the device's memory. If the user registered in the system is unable to do so, the system may be considered defective.

The experiment is performed by detecting fingerprints for the system, aimed at finding the value of the success rate of other fingerprints that have not been entered into the scanner database. The experiment is performed by setting the fingerprint of the user, and then continuing to establish the fingerprint of the second user. To determine the percentages, changes in the ten right fingerprints of users that were used using another person's scan pattern that was not registered in the fingerprint sensor scanner will be checked.

An important point for the study is the position that the scanner is very sensitive to the placement of the user's fingerprints. The location of the fingerprint should be exactly on the layer of the scanner glass so that the fingerprint is read clearly and in accordance with the input and stored in the system. The results of the study of the fingerprint module are shown in table 2.

Table 2 - Study of the fingerprint scan of the user of the car's biometric system

Fingerprint	Positive (real)	Negative (real)	False-positive	False-negative	Car system
1	1	0	0	0	included
2	1	0	0	0	included
3	1	0	0	1	excluded
4	1	0	0	0	included
5	1	0	0	0	included
6	1	0	0	0	included
7	1	0	0	1	excluded
8	1	0	0	0	included
9	1	0	0	0	included
10	1	0	0	0	included

Table 2 shows the matrix of test results. The matrix displays the actual and incorrect number of predictions in the matrix test data. The input data of the matrix have the following values:

- positive (true) - is the number of fingerprints of users using a scanner;

- negative (true) for the number of prints of other users that are detected incorrectly;

- false-positive fingerprint results of another user being entered, verified and correct;

- false-negative when the fingerprint scanner module indicates that the car startup system could not be accessed.

Based on the above results, it can be concluded that the success rate of the fingerprint of the user who can access the car is 90 percent.

Similar works

There are many articles on this topic, for example, a scientific article [21] presented the results of user interaction with a specialized computer system "Android Auto". The study examined the interaction of drivers with the functions of the voice control system and the safety of their control on the road. The results of the study showed that using the "Android Auto" system is quite safe.

McAfee and its partners have published a report called "Precautionary Software" [22], in which they analyzed the new threats and risks in the automotive specialized computer system that are present in modern cars. In [23-24], the authors show a comprehensive approach to show that the safety of modern cars may be compromised due to interference and interference with the passage of Bluetooth and Wi-Fi signals. In some articles, such as [25], security and privacy issues in car voice control systems are solved using different cryptographic methods, or using different secure development environments [26].

Conclusions

As a result of summarizing the literature to ensure the reliability of a specialized computer voice control system, a number of problems have been identified, the main of which is the imperfection of the user authentication system.

To implement the solution to this problem, a hardware and software product of an additional biometric automotive user authentication system was created and developed. The system was created to ensure the reliability of cyber attacks on the voice control system.

An experiment with a biometric authentication system found that the success rate for a registered fingerprint user who can access the car is ninety percent.

Literature

1. What is a computer system? - definition from technopedia. URL: https://uk.theastrologypage.com/computer-system (Accessed on: 06.11.2021).
2. Theology voice control. URL: http://tehnology.com (Accessed on: 22.11.2021).
3. S.Mohith., S.Santhanalakshmi., M.Sudhakaren. Gesture and Voice Controlled Robotic Car using Arduino.2018., pp 3392-3396.
4. What is Android Auto? And how it works. URL: http://www.rcd330.com.ua/ chto-takoe-android-auto (Accessed on: 05.12.2021).
5. How to set up Apple CarPlay in your car (manual). URL: https://uk.vemprarua.org/how-setup-apple-carplay-your-car (Accessed on: 15.12.2021).
6. A Voice Identification System using Hidden Markov Model T. K. Das., Khalid M.O., Nahar SITE, VIT University, Vellore – 632014, Tamil Nadu, India; Department of Computer Science, Yarmouk University, Irbid – 21163, Jordan.
7. V. N. Shmatkov, P. Bonkowski, D. S. Medvedev [et al.] Interact with IOT devices using the voice interface // Scientific and technical Bulletin of information technologies, mechanics and optics, 2019
8. Nicholas Carlini., Pratyush Mishra., Tavish Vaidya., Yuankai Zhang., Micah Sherr.,Clay Shields., DavidWagner.,Wenchao Zhou. 2016. Hidden Voice Commands. In 25th USENIX Security Symposium (USENIX Security 16). USENIX Association, Austin, TX, 513–530.

9. Збірник наукових праць.Центру стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2018. № 3(64). С. 149.
10. Chaouki Kasmi and Jose Lopes Esteves. 2015. IEMI threats for information security: Remote command injection on modern smartphone
11. Nicholas Carlini, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. 2016. Hidden voice commands. In Proceedings of the USENIX Security Symposium.
12. Dibya Mukhopadhyay, Maliheh Shirvanian, and Nitesh Saxena. 2015. All your voices are belong to us: Stealing voices to fool humans and machines. In Proceedings of the European Symposium on Research in Computer Security. Springer, 599–621.
13. STMicroelectronics. 2016. MP34DB02 MEMS audio sensor omnidirectional digital microphone. http://www.mouser.com/ds/2/389/mp34db02-955149.pdf. (2016).
14. Yitao He, Junyu Bian, Xinyu Tong, Zihui Qian, Wei Zhu, Xiaohua Tian, Xinbing Wang. Canceling Inaudible Voice Commands Against Voice Control Systems. 2019 Article No.: 28Pages 1-15
15. DOBRUCKI, A. Nonlinear distortions in electroacoustic devices. Archives of Acoustics 36, 2 (2011), 437–460.
16. Nirupam Roy, Sheng Shen, Haitham Hassanieh, Romit Roy Choudhury University of Illinois at Urbana-Champaign. Inaudible Voice Commands: The Long-Range Attack and Defense.
17. Takeshi Sugawara, The University of Electro-Communications; Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu, University of Michigan. Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems August 12–14, 2020
18. D. Davidson, H. Wu, R. Jellinek, T. Ristenpart, and V. Singh, “Controlling UAVs with sensor input spoofing attacks,” in USENIX WOOT, 2016.
19. Omidiora E. O., Fakolujo O. A., Arulogun O. T., Aborisade D. O. 2011. A Prototype of a Fingerprint Based Ignition Systems in Vehicles. 62(2): 164-171.
20. Tomas Trainys, Algimantas Venčkauskas. Encryption Keys Generation Based on Bio- Cryptography Finger Vein Method. CEUR Workshop Proceedings 2145 (2018) 106-111
21. R Ramnath., N Kinnear., S Chowdhury., THyatt. Interacting with Android Auto and Apple CarPlay when driving: The effect on driver performance.2020. pp 12-17.
22. Stuart McClure. Caution: malware ahead. Vision Zero International. 2013.
23. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. 2016.
24. Charlie Miller., Chris Valasek. Remote exploitation of an unaltered passenger vehicle. Black Hat. 2015.
25. Ramon de Graaff. 2015. Controlling your Connected Car. 2015.
26. Yunhan Jack Jia., Ding Zhao., Qi Alfred Chen.,Z Morley Mao.Towards Secure and Safe Appified Automated Vehicles. 2017.

ДОДАТОК В
(обов’язковий)

ПРЕЗЕНТАЦІЯ ДОПОВІДІ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Кафедра комп'ютерної інженерії та інформаційних систем

Магістерська робота
На тему: Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем

Студента II курсу, групи КІ2м-20-1
Башука Віталія Юрійовича
Науковий керівник: к.т.н, доцент
Гнатчук Єлизавета Геннадіївна

Хмельницький 2022

1

Мета: дослідження та оцінка ефективності методів та засобів забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем.

Об'єкт дослідження: надійність спеціалізованої комп'ютерної системи голосового керування автомобілем.

Предмет дослідження: спеціалізована комп'ютерна система голосового керування автомобілем.

2

Актуальність роботи

Системи голосового керування стають дедалі популярнішими в різних сферах застосування, в тому числі і в галузях машинобудування. Ними все частіше користуються люди різного віку, тому що вони є досить простими в експлуатації, а головне дієвими тому, що використовують різноманітні функції для вирішення різних типів задач.

По-друге голосові помічники систем голосового керування допомагають виконувати різноманітні типи задач для користувачів завдяки широкому функціоналу.

З одного боку, сучасні алгоритми розпізнавання голосових команд, є ще не зовсім досконалими, та не завжди чітко розуміють задану команду користувача і можуть піддаватися різним типам кібератак, але з іншого боку, завдяки розвитку технологій нейромереж і хмарних обчислень, та використання сучасних апаратних та програмних засобів або методів для забезпечення надійності, цю проблему можна звести до мінімуму.

Отже, дослідження та оцінка ефективності методів та засобів забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем є актуальною задачею.

3

Постановка задачі

Для вирішення поставленої задачі необхідно:

- дослідити методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем. Для вирішення цієї задачі необхідно розглянути основні концепції та оцінити ефективність використання зарубіжних спеціалізованих комп'ютерних системах таких як: «Android Auto» та «Apple CarPlay». Розробити моделі виявлення та алгоритми підвищення надійності голосового керування. Також виявити існуючі небезпеки та недоліки в користуванні даними системами. Провести аналіз відомих характеристик методів та засобів для забезпечення надійності.

- виконати моделювання процесу надійності та безпеки в спеціалізованих комп'ютерних системах голосового керування автомобілем,

- розглянути сучасні способи проведення кібератак на автомобільні системи.

- запропонувати апаратні та програмні методи підвищення надійності від сучасних кібератак.

4

Наукова новизна отриманих результатів:

1. Розроблений метод підвищення безпеки системи голосового керування автомобілем, що дозволяє на підготовчому етапі проведення кібератаки попередити та унеможливити її виконання за рахунок блокування ультразвукових коливань пристрою, що проводить записування вхідного сигналу.

2. Запропоновано метод, що дозволяє вирішити задачу забезпечення надійності голосового керування автомобілем, використовуючи засоби додаткової біометричної аутентифікації користувача.

5

Аналіз характеристик системи голосового керування автомобілем

У сучасних автомобілях голосове керування здійснюється шляхом вимови належних команд, які шляхом проходження певних перетворень перетворюються в сигнали керування для відповідних систем. При створенні систем голосового керування повинні враховувати проблеми пов'язані з фоновими шумами, відмінності у вимові, акценти, розмір словника, початку і кінця промови. Проблеми пов'язані з шумами вирішуються за допомогою якісних мікрофонів і методів фільтрації .

Для розв'язання проблем пов'язаних з відмінності у вимові, акцентами, словниковим запасом застосовуються такі типи рішення:

- потрібно забезпечувати інтервал між окремими словами, якщо система розпізнає мову, користувач може вимовляти фрази в природному вигляді, не роблячи проміжків між словами;

- використовувати ступінь деталізації при застосуванні еталонів голосових команд. В системі голосового керування, однією з основних функцій є розпізнавання голосу, що надає можливість, керувати мобільним телефоном, підключеним до неї, користуватися різними можливостями мультимедійної системи, використовувати радіо, навігаційну систему та багато іншого.

6

Переваги та недоліки голосового керування

Переваги	Недоліки
Зручність користування функціями системи та її компонентами.	Не кожна система голосового керування може розпізнати голос користувача та команду.
Наявність голосових помічників, які суттєво полегшують роботу з системою.	Недосконалість системи аутентифікації, що може привести до отримання несанкціонованого доступу та проведення шкідливих дій.
Можливість виконувати телефонні дзвінки, та користуватися мультимедійною системою вашого автомобіля, відправляти або прослуховувати голосові повідомлення, та інше.	Наявність шумів та інших завад, що погіршують розпізнавання системою голосових команд сказаних користувачем.

7

Системи з голосовим керуванням «Android Auto» «Apple CarPlay»

«Android Auto» - це спеціалізована комп'ютерна система, створена компанією «Google» для автомобіля з можливістю голосового керування. Система дозволяє забезпечувати зв'язок з додатками вашого смартфону та функціями автомобіля, використовуючи голосові команди за допомогою помічника «Google Assistant»

Компанія «Apple» випустила інноваційну систему «Apple CarPlay», яка надає можливість користуватися iPhone підключивши його до вашого автомобіля та використовувати голосове керування для різних задач. Система розміщує голосовий помічник «Siri» голосового керування з можливістю бистрого запуску на кермі.

8

Методи забезпечення надійності голосового керування

В результаті узагальнення літератури про основні недоліки та вразливості систем «Android Auto» та «Apple CarPlay», однією з проблем є недосконалість системи аутентифікації користувача та реакція на різні види шумів. Завдяки цій проблемі, злочинці можуть виконувати кібератаки ультразвуковими та світловими командами, вразі успішності кібератаки, вони можуть обійти функцію безпеки голосового помічника видавши себе за власника цим самим отримати несанкціонований доступ до системи транспортного засобу. Для підвищення безпеки та надійності можна використовувати дані методи:

- Метод прихованої Марківської моделі: суть методу полягає в ідентифікації динаміка та авторизації його з базою даних голосів.

- Метод динамічного трансформатування часової шкали: дозволяє знаходити близькість, для двох послідовностей вимірювання, в певний проміжок часу.

- Метод безперервної аутентифікації: використовує сукупність вібрацій голосу користувача та порівнює їх з голосовою командою отриманою з мікрофона системи.

- Метод покращення мовлення: дозволяє оброблювати частоту хвилі голосової команди та виконує розподілення сигналу мовлення від шуму.

Для вирішенні інших проблем та недоліків, що трапляються в системах, зображено структурну схему засобів для підвищення надійності. Для використання голосового керування в системі, потрібно промовити слова пробудження або натиснути кнопку мікрофона, але коли трапляється, що голосове керування не відповідає, для виправлення і коректної роботи, використовують такі засоби.

Апаратні методи захисту

У спеціалізованих комп'ютерних системах голосового керування «Android Auto» та «Apple CarPlay», є недоліки з голосовою аутентифікацією. Для вдалої кібератаки (DolphinAttack) спочатку потрібно віддалено послати нечутний (ультразвуковий) сигнал пробудження системи. Такий сигнал, злочинець може отримати за допомогою запису голосу користувача, на пристрій якого направлена кібератака, для подальшого розбиття сигналу на слова які необхідні для активації.

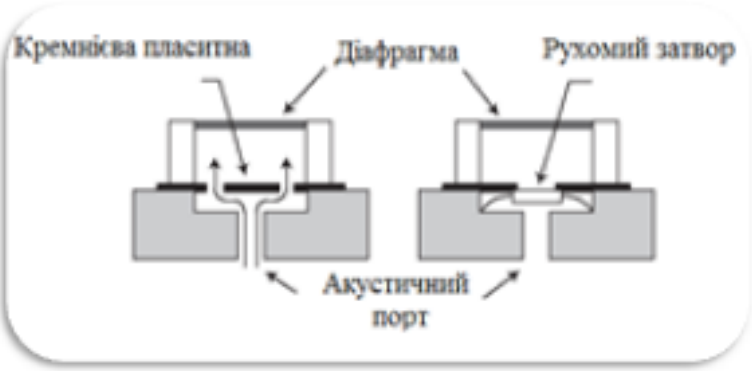
Метод ультразвукового блокування, що використовує апаратний пристрій допоможе підвищити захист системи, на першому етапі підготовки для вдалої кібератаки. Суть методу полягає у зниженні можливості злочинцю отримати запис голосу користувача

11

Метод удосконалення мікрофону системи голосового керування та її характеристик. Основна причина вдалої кібератаки в тому, що мікрофон може сприймати акустичні команди з частотою вище 20 кГц, хоча в ідеалі він не повинен. Суть методу полягає в можна додаванні модуля для фільтра низьких частот, з метою виявлення модульованих голосових команд та скасування основної смуги частот, використовуючи модульовані голосові команди. Завдяки цьому можна виявити сигнали в частоті діапазону ультразвуку, що показують характеристики модуляції та демодулювати ці сигнали для отримання основної смуги частот.

12

Метод покращенні структури мікрофону, тобто для блокування світлових команд можна використати спеціальні непрозорі перешкоди які можна встановити на мікрофон, залишаючи невеликі зазори для можливості проходження звукових хвиль. Тобто зменшити кількість світла, яка досягає діафрагми мікрофона.

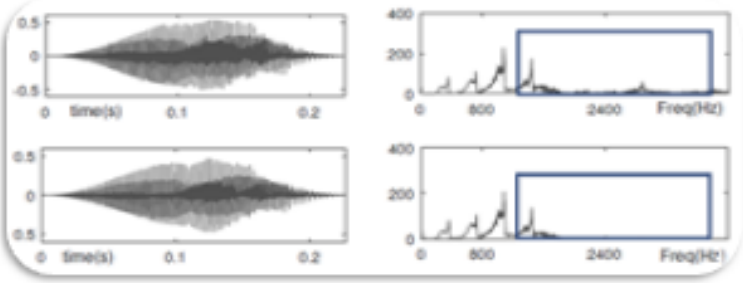


Конструкція зображена має кремнієву пластину та рухомий затвор, за допомогою яких усувається пряма видимість діафрагми мікрофона

13

Програмні методи захисту

Метод унікальних властивостей ультразвукових команд, відрізняє записані команди їх від справжніх. На рисунку показано демодульований сигнал кібератаки який відрізняється від вихідного сигналу і від записаного на високих частотах в діапазоні 800-2400 Гц.



Для підтвердження доцільності виявлення кібератаки, використовується метод опорних векторів в ролі класифікатора та витягуванням з аудіо функцій у частотній та часовій областіях. Для того, щоб класифікатор виявляв шкідливі голосові команди, необхідно використати декілька записаних аудіо зразків, інші зразки, можна використати, для тестування. Класифікатор може відрізнити відновлені аудіо записи від записаних з істинним плюсовим результатом і мінусовим показником на всі сто відсотків

14

Метод пошуку та виявлення ознак нелінійності сигналу. Він полягає у пошуку та виявленню ознак не лінійності сигналу, які передаються на мікрофон СГК. В цілому мікрофони та динаміки розроблені як лінійні системи, це означає, що вихідні сигнали є лінійними комбінаціями вхідних сигналів.

На практиці зазвичай компоненти в мікрофонах можуть бути лінійними тільки в чутних діапазонах частот, тобто більшими за 20 кГц. В ультразвукових смугах де частота менша як 25 кГц, вони показують нелінійність.

Програмні методи захисту від атаки світловими командами:

Програмний метод	Застосування
Додатковий рівень аутентифікації.	Метод полягає у використанні додаткового кроку аутентифікації перед виконанням критичних команд та зменшення спроб неправильного введення паролю, якщо система підтримує таку функцію.
Метод роботи злиття алгоритмів датчиків.	Виявлення атаки, використавши порівняння сигналів від кількох мікрофонів, ігноруючи голосові команди, які вводяться за допомогою одного спеціального пристрою

15

Метод вирішення задачі підвищення надійності голосового керування автомобіля

В результаті проведеного огляду першоджерел систем голосової аутентифікації різних автомобілів, був отриманий матеріал, аналіз якого дозволив зробити висновок, що для максимального забезпечення надійності системи голосового керування автомобіля, потрібно використовувати додаткову систему аутентифікації, яка дозволить лише водію, або довіреним особам використовувати весь функціонал транспортного засобу, виконувати керування системами та інше.

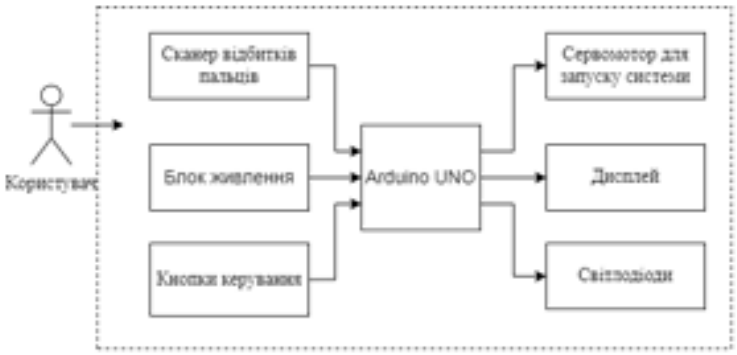
Для розв'язання проблеми з додатковою аутентифікацією створена автономна система безпеки, з можливістю аутентифікації користувача за допомогою відбитків пальців власника автомобіля, або довірених осіб.

Основними компонентами системи біометричної аутинтифікації водія будуть такі засоби: плата Arduino UNO, сканер відбитків пальців, LCD-дисплей, сервомотор для запуску системи автомобіля та додаткові апаратні пристрої для виконання різних функцій системи

16

Додаткова біометрична система аутентифікації користувача

Апаратно-програмна реалізація системи використовує в собі додатковий спосіб аутентифікації користувача, що базується на можливості запуску системи автомобіля, що своєю чергою дозволить використовувати його функціонал, та унеможливить використання, при неправильній біометричній аутентифікації за допомогою відбитку пальця. На рисунку зображено архітектуру біометричної системи аутентифікації.



17

Апаратні та програмні складові системи

Апаратна складова автомобільної системи біометричної аутентифікації, складається, з сукупності апаратних пристроїв, що своєю чергою здійснюють зчитування відбитку пальця користувача і виконують функції керування даних. Структура апаратної системи біометричної аутентифікації охоплює в собі наступні пристрої:

- модуль сканера відбитків пальців;
- кнопки керування системою;
- LED-індикатори;
- сервомотор для запуску системи;
- LCD-дисплей;
- Додаткові апаратні засоби;
- системна плата Arduino UNO

Програмна складова автомобільної системи біометричної аутентифікації містить в собі програмне забезпечення для:

- бази даних, яка використовується для зберігання та накопичення зображень відбитків пальців користувача, та інших довірених осіб і містить інформацію про них;

- забезпечення для аналізу та класифікації розпізнавання збережених даних системи біометричної аутентифікації;

За допомогою програмного забезпечення пристрій зчитує відбиток пальця користувача або іншої довіреної особи.

18

Результати дослідження та тестування

В дослідженні брали участь сім користувачів, ідея полягала в тестуванні функції перевірки відбитків пальців системи, тобто самого режиму роботи. Кожний користувач робив більше тридцяти спроб перевірити свій відбиток пальця, який був збережений системою раніше.

Користувач	Кількість спроб	Підтверджено	Невдала спроба	Відсоток підтверджених спроб
1	35	33	2	93.3 %
2	35	34	1	96.6 %
3	35	33	2	93.3 %
4	35	32	3	90 %
5	35	34	1	96.6 %
6	35	31	4	87.7 %
7	35	33	2	93.3 %

аутентифікації користувачів були вдалими

19

Проведення експерименту відбувається, шляхом виявлення відбитків пальців для системи, спрямованих на пошук значення відсотку успіху інших відбитків пальців, які не були введені в базу даних сканера. Експеримент виконується шляхом встановлення відбитка пальця користувача, а потім продовження встановлення відбитка пальця другого користувача. Для визначення відсоткових значень будуть перевірені зміни семи правих відбитків пальців користувачів, які були використані за допомогою зразка сканування іншої особи, що не була зареєстрована у сканері датчика відбитку пальця.

Відбиток пальця	Позитивний (справжній)	Негативний (справжній)	Хибно-позитивний	Помилково-негативний	Автомобільна система
1	1	0	0	0	виключена
2	1	0	0	0	виключена
3	1	0	0	1	виключена
4	1	0	0	0	виключена
5	1	0	0	0	виключена
6	1	0	0	0	виключена
7	1	0	0	0	виключена
8	1	0	0	0	виключена
9	1	0	0	0	виключена
10	1	0	0	0	виключена

20

Висновки

У першому розділі розглянуто основні поняття та концепції спеціалізованих комп'ютерних систем автомобіля. Також здійснено комплексний огляд системи голосового керування автомобілем та способи взаємодії даної системи з користувачем. Проведено аналіз засобів для забезпечення та підвищення надійності, в результаті якого можна сформулювати комплекс методів підвищення надійності голосового керування автомобілем. В перше поставлено та вирішено питання принципу роботи спеціалізованих автомобільних систем «Android Auto» та «Apple CarPlay».

У другому розділі проведено аналіз в результаті якого були сформовані концепції зарубіжних аналогів спеціалізованих комп'ютерних систем голосового керування автомобілем «Android Auto» та «Apple CarPlay». Проведено дослідження основних недоліків та вразливостей голосових помічників для даних систем, в результаті якого сформульовано загрози для системи голосової аутентифікації автомобіля.

Запропоновано модель виявлення загроз та забезпечення надійності голосових помічників «Siri» та «Google Assistant», що дозволяє удосконалити засоби які потрібно використовувати для підвищення надійності спеціалізованих комп'ютерних систем автомобіля. Проведена порівняльна оцінка моделі виявлення сучасних способів кібератак, яка показала можливості проведення атак ультразвуковими та світловими командами на систему голосового керування автомобілем.

Висновки

У третьому розділі проведено дослідження оцінки впливу та запропоновано нову класифікацію існуючих методів та засобів для забезпечення надійності спеціалізованих комп'ютерних систем голосового керування автомобілем «Android Auto» та «Apple CarPlay» на основі захисту системи голосової аутентифікації систем від кібератак ультразвуковими та світловими командами.

Проведено аналіз методу виявлення кібератаки за допомогою ультразвукових команд «DolphinAttack», визначено можливі наслідки та створена схема модулів, розроблений метод підвищення безпеки, що дозволяє на підготовчому етапі проведення кібератаки попередити та унеможливити її виконання.

В результаті дослідження запропоновано апаратні та програмні методи забезпечення надійності спеціалізованих комп'ютерних систем «Android Auto» та «Apple CarPlay» від кібератак на основі проведення ультразвуковими та світловими командами. Запропоновано метод, що дозволяє вирішити задачу забезпечення надійності голосового керування, використовуючи метод додаткової біометричної аутентифікації користувача.

У четвертому розділі досліджено проблему недосконалості голосової аутентифікації користувача, та для вирішення даної проблеми було розроблено та реалізовано апаратно-програмний продукт додаткової біометричної автомобільної системи аутентифікації користувача. Виконано комплексну оцінку ефективності використаних моделей та методів для вирішення поставленої задачі.

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1011103344

Дата перевірки:
09.05.2022 07:51:08 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.05.2022 07:53:13 EEST

ID користувача:
100005591

Назва документа: Башук_Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи г...

Кількість сторінок: 93 Кількість слів: 15827 Кількість символів: 127162 Розмір файлу: 4.12 MB ID файлу: 1011002831

1.09%
Схожість

Найбільша схожість: 0.56% з джерелом з Бібліотеки (ID файлу: 1010929453)

0.36% Джерела з Інтернету	6	Сторінка 95
0.73% Джерела з Бібліотеки	51	Сторінка 95

0.35% Цитат

Цитати	12	Сторінка 96

Не знайдено жодних посилань

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	23

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

ID: 103328 Название: Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем Добавлено в БД: 2022-05-09 Авторы: Башук В.Ю. Руководители: Гнатчук Є.Г. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	112434	847	488 (0%)	9 (1%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Башук Віталій Юрійович

Тема: Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомобілем

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___-____ Кількість сторінок записки __117_____

1. Короткий зміст роботи та прийнятих рішень: Розроблений метод підвищення безпеки системи голосового керування автомобілем, що дозволяє на підготовчому етапі проведення кібератаки попередити та унеможливити її виконання за рахунок блокування ультразвукових коливань пристрою, що проводить записування вхідного сигналу. Запропоновано метод, що дозволяє вирішити задачу забезпечення надійності голосового керування автомобілем, використовуючи засоби додаткової біометричної аутентифікації користувача.

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

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі розглянуто основні поняття та концепції спеціалізованих комп'ютерних систем автомобіля. В перше поставлено та вирішено питання принципу роботи спеціалізованих автомобільних систем «Android Auto» та «Apple CarPlay».

У другому розділі проведено дослідження основних недоліків та вразливостей голосових помічників для спеціалізованих автомобільних систем, в результаті якого сформульовано загрози для системи голосової аутентифікації автомобіля.

У третьому розділі проведено дослідження оцінки впливу та запропоновано нову класифікацію існуючих методів та засобів для забезпечення надійності спеціалізованих комп'ютерних систем голосового керування автомобілем «Android Auto» та «Apple

CarPlay» на основі захисту системи голосової аутентифікації систем від кібератак ультразвуковими та світловими командами.

Також розроблений метод підвищення безпеки, що дозволяє на підготовчому етапі проведення кібератаки попередити та унеможливити її виконання.

У четвертому розділі досліджено проблему недосконалості голосової аутентифікації користувача, та для вирішення даної проблеми було розроблено та реалізовано апаратно-програмний продукт додаткової біометричної автомобільної системи аутентифікації користувача. Виконано комплексну оцінку ефективності використаних моделей та методів для вирішення поставленої задачі.

Проведено експериментальне дослідження системи, в результаті якого було встановлено, що система виконує всі задані функції.

4. Позитивні сторони роботи: У роботі за результатами виконаних теоретичних та практичних досліджень розроблено додаткову біометричну систему аутентифікації користувача для підвищення надійності голосового керування автомобілем, та захисту від сучасних методів кібератак.

5. Негативні сторони роботи: -

6. Оцінка графічного оформлення та пояснювальної записки роботи: -

7. Відгук про роботу в цілому: Робота виконана на достатньо високому науковому рівні.

8. Інші зауваження: -

9. Оцінка дипломної роботи: Розглянувши представлену кваліфікаційну роботу вважаю, що робота заслуговує оцінки відмінно 5.00 (А).

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Бедратюк Леонід Петрович, доктор фізико-математичних наук, професор, завідувач кафедри інженерії ПЗ ХНУ

"10" 05. 2022 р. (підпис)

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Башук Віталій Юрійович
ПІБ здобувача вищої освіти

ФПКТС, 2 курсу, групи КІ2м-20-1

ЗАЯВА

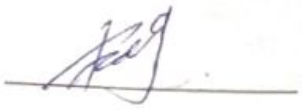
З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та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

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

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

11. 05. 2022.

дата



підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Методи та засоби забезпечення надійності спеціалізованої комп'ютерної системи голосового керування автомоіблем

Автор: Башук Віталій Юрійович

Спеціальність: 123 – Компютерна інженерія та програмування

Освітня програма: освітньо-наукова

Науковий керівник: Гнатчук Єлизавета Геннадіївна, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

1) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
2) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 1.09% і адресується до 56 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Є. Г. Гнатчук

Гарант ОП _____ О. С. Савенко

Завідувач кафедри КІСП _____ Т. О. Говорущенко