НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«На правах рукопису»
УДК 004.56

До захисту допущено:
В.о. завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою «Системи електронних комунікацій та Інтернету речей»

зі спеціальності 172 «Електронні комунікації та радіотехніка»

на тему: «Аналіз заходів кібербезпеки для інформаційно-комунікаційних систем підключених автомобілів»

Виконав:
студент VI курсу, групи ЦС-31
Тиришкін Олександр Андрійович _____

Науковий керівник:
Професор кафедри ЕКІР, д.т.н., професор
Горицький Віктор Михайлович _____

Рецензент:
Старший викладач Спеціальної кафедри № 5
Мітін Сергій В’ячеславович _____

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

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Електронні комунікації та радіотехніка»

Освітньо-професійна програма «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

_____ В’ячеслав НОСКОВ

«___»_____20__ р.

ЗАВДАННЯ

на магістерську дисертацію студенту

Тиришкіну Олександру Андрійовичу

1. Тема дисертації «Аналіз заходів кібербезпеки для інформаційно-комунікаційних систем підключених автомобілів», науковий керівник дисертації Горицький Віктор Михайлович, професор кафедри ЕКІР, затверджені наказом по університету від 22 травня 2023 р. № 1884-с.

2. Термін подання студентом дисертації 10 грудня 2024.

3. Об’єкт дослідження: системи інформаційно-комунікаційних технологій підключених автомобілів, мережі IoT, а також методи забезпечення їх кібербезпеки.

4. Вихідними даними для виконання роботи є інформаційні матеріали, що стосуються технологій забезпечення кібербезпеки для інформаційно-комунікаційних систем підключених автомобілів, а також міжнародні стандарти кібербезпеки, такі як ETSI EN 303 645 та ISO/SAE 21434. Додатково використовуються практичні методики тестування на проникнення в IoT мережі, зокрема у контексті автомобільних систем.

5. Перелік завдань, які потрібно розробити: провести аналіз стандартів безпеки ETSI EN 303 645 та ISO/SAE 21434. Особливу увагу слід приділити дослідженню архітектури CAN-шини та OBD-II, які є основними компонентами для інтеграції автомобілів в IoT-мережах. Також потрібно розробити практичні сценарії для проведення тестування на проникнення в підключений автомобіль, оцінити

ризики, які пов’язані з кіберзагрозами, та запропонувати ефективні заходи для покращення захищеності автомобільних інформаційно-комунікаційних систем.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація обсягом 9 слайдів.

7. Дата видачі завдання 1 грудня 2023.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз завдання, уточнення теми, формулювання мети, завдань, об’єкта та предмета дослідження	01.12.2023 – 25.12.2023	
2	Написання першого розділу, присвяченого актуальності кібербезпеки у світі	10.01.2024 – 05.02.2024	
3	Написання другого розділу, спрямованого на дослідження міжнародних стандартів кібербезпеки	20.02.2024 – 15.03.2024	
4	Аналіз вразливостей кібербезпеки в мережах IoT	01.05.2024 – 25.05.2024	
5	Оцінка ризиків і вдосконалення систем кібербезпеки автомобіля	10.07.2024 – 05.08.2024	
6	Узагальнення отриманих результатів і формування висновків	15.09.2024 – 10.10.2024	
7	Оформлення дипломної роботи	20.11.2024 – 15.12.2024	
8	Підготовка до захисту дипломної роботи	20.12.2024 – 30.12.2024	

Студент Олександр ТИРИШКІН

Науковий керівник Віктор ГОРИЦЬКИЙ

РЕФЕРАТ

Темою магістерської дисертації є аналіз заходів кібербезпеки для інформаційно-комунікаційних систем підключених автомобілів.

Робота складається з 70 сторінок, включає 21 ілюстрацію, 1 таблицю та 20 джерел інформації.

Актуальність теми пояснюється стрімким розвитком Інтернету речей (IoT), зокрема підключених автомобілів, які стають постійними об’єктами кібератак. Забезпечення безпеки таких мереж є критичним для запобігання витоку даних, зловживання функціональністю автомобілів та потенційної шкоди для користувачів.

Метою дисертації є аналіз ризиків, пов'язаних з вразливостями автомобільних IoT-мереж, розробка рекомендацій для підвищення їх кібербезпеки, а також оцінка ефективності протоколів захисту та методів тестування.

Об’єктом дослідження є підключені автомобілі.

Предметом дослідження є методи підвищення кібербезпеки таких мереж, включаючи практики тестування на проникнення, захисту CAN-шини та протоколів V2X.

У роботі була розроблена методика фізичного тестування шини CAN, яка дозволяє оцінити ризики несанкціонованого доступу та запропоновані рекомендації щодо впровадження вдосконалених заходів безпеки, таких як шифрування даних та сегментація мережі.

Результати дослідження можуть бути використані для впровадження практичних рішень з кібербезпеки в індустрії підключених автомобілів

КЛЮЧОВІ СЛОВА: IoT, кібербезпека автомобіля, машинне навчання, ISO, штучний інтелект, стандарти, датчики, система взаємодії, персональні дані, автономні транспортні засоби.

ABSTRACT

The topic of the master's thesis is the study of methods for improving the cybersecurity of connected car networks.

The work consists of 70 pages, includes 21 illustrations, 1 table and 20 sources of information.

The relevance of the topic is explained by the rapid development of the Internet of Things (IoT), in particular connected cars, which are becoming important targets of cyberattacks. Ensuring the security of such networks is critical to prevent data leakage, misuse of car functionality, and potential harm to users.

The purpose of the thesis is to analyze the risks associated with vulnerabilities of automotive IoT networks, develop recommendations for improving their cybersecurity, and evaluate the effectiveness of security protocols and testing methods.

The object of research is IoT networks of connected cars.

The subject of the study is methods for improving the cybersecurity of such networks, including penetration testing practices, CAN bus protection, and V2X protocols.

The paper develops a methodology for physical testing of the CAN bus, which allows assessing the risks of unauthorized access, and offers recommendations for implementing advanced security measures.

The results of the study can be used to implement practical cybersecurity solutions in the connected car industry.

KEYWORDS: IoT, car cybersecurity, machine learning, ISO, artificial intelligence, standards, sensors, interaction system, personal data, autonomous vehicles.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

APT - Advanced Persistent Threat – постійна розширена загроза

IoT – Internet of Things – Інтернет Речей

OWASP – Open Worldwide Application Security Project – відкритий проєкт з безпеки вебзастосунків

AI – Artificial Intelligence – штучний інтелект

MLLM – Multimodal Content Generation – мультимодальна генерація контенту

SSN – Social Security Number – номери соціального страхування

PIN – Personal Identification Number – персональні ідентифікаційні номери

ISO – International Organization for Standardization – міжнародна організація зі стандартизації

IEC – International Electrotechnical Commission – міжнародна електротехнічна комісія

FuSa – Functional Safety – функціональна безпека

ASIL – Automotive Safety Integrity Level – рівні цілісності автомобільної безпеки

HARA – Hazard Analysis and Risk Assessment – аналіз небезпек та оцінка ризиків

ECU – Electronic Control Unit – електронний блок управління.

PID – Parameter Identification – ідентифікація параметрів

IDS – Intrusion Detection Systems – системи виявлення вторгнень

FTP – File Transfer Protocol – протокол передачі даних

Transport Layer Security – Transport Layer Security – захист на транспортному рівні

LiDAR – Light Detection and Ranging – світловий радіолокатор

AES – Advanced Encryption Standard – симетричний алгоритм блочного шифрування

MFA – Multi-Factor Authentication – багатофакторна автентифікація

FOTA – Firmware Over-The-Air – оновлення вбудованого програмного забезпечення по повітрю

UDS – Unified Diagnostic Services – уніфіковані діагностичні сервіси

RDS – Radio Data System – система радіоданих

RSU – Roadside Unit – придорожні пристрої

PKI – Public Key Infrastructure – інфраструктура відкритих ключів

Trusted Platform Module (TPM) – модуль довіреної платформи

CAM – Cooperative Awareness Messages – повідомлення про співпрацю та обізнаність

DENM – Decentralized Environmental Notification Messages – повідомлення про навколишнє середовище

TCB – Trusted Computing Base – довірена обчислювальна база

ТЗ – транспортні засоби

АТЗ – автономні транспортні засоби

МН – машинне навчання

ЕБУ – електронний блок управління

ВСТУП

Питання кібербезпеки інформаційно-комунікаційних технологій стає більш актуальною в повсякденному житі. Зі збільшенням нових пристроїв та розвитку технологій прямо пропорційно збільшується і ризик кібератак. Саме Інтернет речей є новим революційним проривом, який створений для покращення повсякденного життя. Попри всю доступність та переваги, питання кібербезпеки є не лише технологічною потребою, але основним імперативом для забезпечення цілісності, конфіденційності та доступності до даних та послуг.

Побутова техніка, промислове обладнання та мережа інтелектуальних пристроїв поєднують у собі велику кількість сфер, таких як охорона здоров’я, транспортна інфраструктура, сільське господарство та промислове виробництво. У цих галузях кібербезпека відіграє більш важливу роль: системи та компоненти, які регулюють безпеку, повинні бути захищені від шкідливого впливу.

Сучасна автомобільна мережа та її внутрішні компоненти є критичними вузлами до атак, які загрожують та становлять загрозу як фізичній безпеці водія і пасажирів, так і конфіденційності їхніх даних. У минулому клонування електронних ключів було найпоширенішим способом незаконного доступу до автомобіля. Транспортні засоби все більше підключаються до таких технологій, як WI-FI та 3G, 4G і 5G, що дає хакерам безліч способів проникнути всередину. Понад чверть нинішніх атак використовують хмарні сервери або мобільні додатки автомобілів.

1 АКТУАЛЬНІСТЬ ТА ЗНАЧЕННЯ КІБЕРБЕЗПЕКИ У СВІТІ ВИСОКИХ ТЕХНОЛОГІЙ

Кібератаки — це не лише пряма загроза конфіденційним даним, а також можливий доступ до критично важливих вузлів таких, як космічні орбітальні системи, медична сфера. Вони можуть завдати репутаційні або юридичні проблеми, що може потягнути за собою інтелектуальну власність компанії, яка є головною частиною її успіху.

З появою нових технологій, від безпілотних автомобілів до систем домашньої безпеки з підтримкою Інтернету речей, загроза кіберзлочинності стає ще серйознішою. Тож не дивно, що міжнародна дослідницька та консалтингова компанія Gartner [1] прогнозує, що у 2024 році світові витрати на безпеку досягнуть 210 мільярдів доларів, а до 2028 року ринок досягне 314 мільярдів доларів.

Специфіка високотехнологічних компаній, наприклад, впровадження бізнес-рішень у хмарі, а також кількість конфіденційних даних, що генеруються, робить їх сприйнятливими до кібератак. Подальше шифрування в мережі є надійним та безпечним рішенням для їх передачі, цей комплекс допоможе запобігти різним типам загроз.

1.1 Еволюція кібератак: від перших інцидентів до сучасних загроз

За останні кілька десятиліть світ став свідком еволюції кібербезпеки. Пройшов вже той час, коли найбільшою проблемою були комп'ютерні віруси, бо збільшився рівень кіберзагроз із використанням фішингу, шкідливих програм, штучного інтелекту та машинного навчання наражають на постійну небезпеку приватних осіб, корпорації та уряди. Перші кроки кіберзлочинів розпочинаються з середини 20 століття. У 1962 році Аллен Шерр [2] аспірант МТІ зробив цифрове проникнення та вкрав паролі облікових засобів інших користувачів.

Першою публічною атакою можна вважати хробака Морріса в 1988 році. Сьогодні код віруса не має жодної загрози, бо сучасні комп'ютери мають сильний захист до вразливостей. Попри це, троян надихнув нове покоління хакерів, яке змусило багатьох людей ставитися до інформації з глибокою підозрою, якою вони діляться та зберігають.

Нові загрози через брак належного контролю: 1990-ті

Подальшим розвиток кібердіяльності стали 1990-ті роки. Зі швидким попитом на персональні комп'ютери та збільшенням поширення інтернету кількість кіберзагроз зросла з геометричною прогресією. Технології прогресували настільки швидко, що захисний механізм не встиг адаптуватися, що призвело до нових типів атак. Кінець XX століття схарактеризувався фішинговими атаками та методами соціальної інженерії, завдяки чому зловмисники отримували доступ до особистої інформації. Класичним прикладом є афера «Нігерійські листи» [3], назва набула свого значення через розсилку в Нігерії, ще до розповсюдження інтернету. Жертва отримувала лист щастя електронною поштою, де шахраї просили у отримувача листа допомоги у багатомільйонних грошових операціях, обіцяючи солідні відсотки із сум. Якщо одержувач погодиться брати участь, у нього поступово вимагались все більші суми грошей нібито на оформлення угод, сплату зборів, хабарі чиновникам.

Еволюція складних кіберзагроз: перше десятиліття 21 століття

20 січня 2008 року американська платіжна система Heartland Payment System [4] публічно оголосила про те, що зазнала катастрофічного порушення безпеки у своїй системі обробки платежів. На момент злочину компанія обробляла 100 мільйонів транзакцій з платіжними картками на місяць, що робить цю атаку найбільшим витоком даних, який будь-коли траплявся. Хакери змогли проникнути в систему компанії, скориставшись SQL-ін'єкцією, наявною на вебсторінка для входу в систему восьмирічної давнини, після чого вони витратили сім місяців на спроби отримати доступ до платіжної мережі, намагаючись уникнути виявлення кількома різними антивірусними системами, які використовує Heartland. Попри це, Visa вперше повідомила про «підозрілу

активність, пов'язану з певними обліковими записами власників карток» майже через рік, що змусило компанію звернутися до Міністерство юстиції США та найняти дві команди криміналістів для проведення розслідування. Було виявлено шкідливе програмне забезпечення, яке дозволило хакерам викрасти дані. Компанія уточнила, що в результаті витоку під загрозу не потрапили дані продавців, адреси або номери телефонів. Однак їх викрадення включало цифрову інформацію, записану на магнітній стрічці кредитних і дебетових карток. Маючи ці дані, злочинці можуть виготовляти підроблені картки, друкуючи ту саму викрадену інформацію виготовлену на подібних екземплярах

Ескалація кіберзагроз у 2020-х роках

У травні 2021 року компанія Colonial Pipeline [5] зазнала масштабної атаки зловмисників із вимогою викупу. Атака зашифрувала частину мережі компанії Colonial, яка транспортує 70% нафти для східного узбережжя США, заздалегідь припинила фізичні операції. Це призвело до дефіциту бензину та довгих черг на заправках на східному узбережжі. Ціна на пальне зросла до рекордного рівня. Для більшості американців це був перший досвід кібератаки, яка безпосередньо торкнулася їх. Подія зробила очевидним, що кібератаки на ланцюги постачання є проблемою національної безпеки. У 2021 році кількість атак на ланцюги постачання програмного забезпечення потроїлася порівняно з 2020 роком. Пандемія COVID-19 створила ще більше кібервикликів для логістичної мережі та транспортної галузі.

1.2 Сучасні методи захисту інформації

Інформаційна безпека охоплює інструменти та процеси, які організації використовують для захисту інформації. Сюди входять налаштування політик, які запобігають доступу сторонніх осіб до ділової або особистої інформації.

InfoSec - це галузь, що постійно розвивається та охоплює широкий спектр сфер, від безпеки мережі та інфраструктури до тестування й аудиту. Вона захищає конфіденційну інформацію від несанкціонованих дій, включаючи

перевірку, модифікацію, запис і будь-яке порушення або знищення. ЇЇ мета забезпечити конфіденційність критично важливих даних, таких як реквізити клієнтських рахунків, фінансової інформації або інтелектуальна власність.

Наслідки інцидентів безпеки включають крадіжку приватної інформації, фальсифікацію даних і видалення. Атаки можуть порушити робочі процеси та зашкодити репутації компанії, а також мати відчутну вартість. Своєю чергою організації повинні виділяти кошти на забезпечення заходів безпеки та гарантувати, що вони готові виявляти, реагувати та активно запобігати таким атакам, як фішинг, шкідливе програмне забезпечення та вірусам.

Основними принципами інформаційної безпеки є конфіденційність, цілісність і доступність. Кожен елемент програмного забезпечення повинен бути розроблений для реалізації одного або декількох з цих принципів. Разом вони називаються «Тріада ЦРУ» [6]. До неї належать:

Конфіденційність

Заходи конфіденційності покликані запобігти несанкціонованому розголошенню інформації. Мета цього принципу полягає в тому, щоб зберігати особисту інформацію в таємниці та забезпечити її видимість і доступ до неї лише тим особам, які володіють нею або потребують її для виконання своїх організаційних функцій.

Ніхто не хоче мати справу з наслідками витоку даних, саме тому слід вживати серйозних заходів для забезпечення безпеки інформації, встановити засоби контролю безпеки для конфіденційних файлів і розробити чітку політику інформаційної безпеки щодо пристроїв. Конфіденційність охоплює цілий спектр засобів контролю доступу та заходів, які захищають вашу інформацію від несанкціонованого використання. Ідеальний спосіб зберегти конфіденційність даних і запобігти їхньому витоку - це впровадити запобіжні заходи.

Кожна інформація, якою володіє компанія, має цінність, особливо в сучасному світі. Фінансові дані, номери кредитних карток, комерційні таємниці або юридичні документи – все це вимагає належної конфіденційності. Іншими словами, доступ до конфіденційної інформації повинні мати лише ті люди, які

мають на це повноваження. Недотримання конфіденційності означає, що той, хто не повинен мати доступу, отримав його. Через навмисну поведінку або випадковим збігом обставин, порушення конфіденційності може призвести до серйозних проблем. Основні методи для збереження конфіденційності даних: шифрування, пароль, двофакторна автентифікація, біометрична верифікація.

Цілісність

У світі інформаційної безпеки цілісність означає точність і повноту даних. Засоби контролю безпеки, орієнтовані на цілісність, покликані запобігти зміні даних або їх неправомірному використанню несанкціонованою стороною. Цілісність передбачає підтримку узгодженості та вірогідності даних протягом усього їхнього життєвого циклу. Вони не повинні змінюватися під час передачі, і необхідно вжити запобіжних заходів, щоб унеможливити їх зміну неавторизованими особами.

Наприклад, у разі порушення їх цілісності хакер може захопити дані і змінити їх, перш ніж відправити адресату. Деякі засоби контролю безпеки, призначені для збереження автентичності інформації включають: шифрування, контроль доступу користувачів, контроль версій, процедури резервного копіювання та відновлення, програмне забезпечення для виявлення помилок.

Доступність

Доступність даних означає, що інформація доступна лише авторизованим користувачам. Це гарантія того, що до вашої системи та даних можуть отримати доступ автентифіковані користувачі, коли це буде потрібно. Подібно до конфіденційності та цілісності, доступність також має велике значення.

Ці методи зазвичай асоціюються з надійністю та часом безперебійної роботи системи, на які можуть впливати як нешкідливі проблеми, такі як збої в роботі обладнання, незаплановані простої програмного забезпечення та людські помилки, так і зловмисні проблеми або кібератаки та інсайдерські загрози. Якщо мережа несподівано виходить з ладу, користувачі не зможуть отримати доступ до важливих даних і додатків. Політики інформаційної безпеки та засоби контролю безпеки, розв'язувати проблеми доступності, створюючи різні

резервування інформації, щоб забезпечити безперервну працездатність і безперервність бізнесу.

Інформація рядового користувача є більш вразливою до загроз доступності даних, ніж інші два компоненти моделі CIA. Регулярне резервне копіювання за межами офісу може обмежити шкоду, засобам збереження та відтворення інформації, збоями в роботі сервера або стихійними лихами. Інформація має цінність лише тоді, коли до неї мають доступ потрібні люди в потрібний час.

Заходи інформаційної безпеки для зменшення загроз доступності даних включають: резервне копіювання за межами офісу, аварійне відновлення, резервування, обхід відмов, належний моніторинг, контроль навколишнього середовища, віртуалізація, кластеризація серверів, безперервність планування операцій.

1.3 Проблеми безпеки, пов'язані з розширенням застосування IoT

Безпека та конфіденційність інформації є одними з найважливіших питань для Інтернету речей в сучасному світі. Неправильне оновлення пристроїв, відсутність ефективних і надійних протоколів безпеки, необізнаність користувачів, відомий активний моніторинг пристроїв все це є найпоширенішими проблемами, з якими вони стикаються.

Інтернет речей - це концепція об'єднаних пристроїв усіх типів підключення дротового чи бездротового формату. Попит на IoT зростає в геометричній прогресії, бо ці гаджети мають велику сферу застосування, включаючи автомобільну галузь, освітній процес та розвиток різних бізнес-стратегій. Інтернет речей має за ідею надшвидкого зв’язку, де організації або комерційна установа можуть без особливих зусиль спілкуватися один з одним з будь-якої точки [7]. Кевін Ештон винайшов цей термін у 1999 році для просування концепції радіочастотної ідентифікації (RFID), яка охоплює датчики та виконавчі механізми. Однак оригінальна ідея була представлена ще в 1960-х роках. У той період вона називалася повсюдною обчислювальною технікою або

вбудованим інтернетом. Він представив цю концепцію для покращення діяльності ланцюгів постачання. Однак різноманітні функціональні можливості Інтернету речей допомогли йому набути великої популярності влітку 2010 року. Уряд Китаю надав IoT стратегічний пріоритет, запровадивши п'ятирічний план. Однак такий неконтрольований вибух збільшив виклики для приватності та безпеки.

IoT відрізняється від традиційних комп'ютерів і обчислювальних пристроїв, що робить його більш вразливим до викликів безпеки в різних аспектах :

Проблеми з оновленням: все програмне забезпечення потребує періодичних оновлень, щоб оновити функціонал або закрити диру в безпеці. Унікальні сценарії розгортання пристроїв Інтернету речей означають, що вони рідко отримують оновлення (нікому не спадає на думку перевіряти версію програмного забезпечення, наприклад підключені до інтернету лампочки або тостер). Це робить пристрої дуже вразливими до цілеспрямованих атак.

- Небезпечні паролі: пристрої Інтернету речей мають ряд проблем, пов'язаних з паролями. Виробники пристроїв зазвичай використовують слабкі паролі за замовчуванням, які користувачі не змінюють ні до, ні після їх розгортання. Крім того, виробники іноді включають в свої системи жорстко закодовані паролі, які користувачі не можуть змінити. Ці слабкі паролі наражають пристрої Інтернету речей на високий ризик. Зловмисники можуть просто увійти на ці пристрої за допомогою цих паролів, які легко вгадуються, або за допомогою простих атак грубої сили.
- Ненадійні місця розгортання: пристрої IoT часто призначені для розгортання в публічних і віддалених місцях, де зловмисник може отримати фізичний доступ до пристроїв. Завдяки цьому зловмисник може обійти наявні засоби захисту на пристроях.

Багато з цих пристроїв підтримують автоматично режим з'єднання та обмінюються інформацією з іншими пристроями в автономному режимі. Це вимагає розгляду доступних, методологій з безпекою IoT пристроїв.

1.4 Висновки до розділу 1

У цьому розділі було проаналізовано сучасну літературу, вебсайти та інші загальнодоступні матеріали, щоб ознайомитися з першими загрозами, їх еволюцією та подальшими методами захисту. Завдяки цьому був проведений аналіз слабких місць та способам протидії загрозам, з якими повинні боротися організації.

Сектор кібербезпеки переживає велику цифрову революцію, з використанням актуальних технологій адаптованого захисту. Однак з розвитком нових вразливостей збільшуються загрози конфіденційності користувачів та цілісності організацій. Для боротьби з кіберзлочинністю необхідна добре розроблена політика, а також визначення критичних ознак кібербезпеці, щоб можна було розробити комплексну політику захисту.

Кіберзахист необхідний для уникнення небезпек, спричинених кіберзагрозами, наприклад, порушенням конфіденційності, крадіжками даних, зловмисними актами вандалізму, інсайдерськими загрозами. Для забезпечення кібербезпеки Інтернету речей потрібно розробити багатогранну стратегію запобіганням хакерських атак. Це має охоплювати технічні, операційні та організаційні заходи, які включають автентифікацію для користувачів, шифрування та системи моніторингу безпеки. А також, швидке реагування на інцидент та формування культур безпеки в інтернет середовищі через навчання та дотримання безпечних практик і політик.

2 ДОСЛІДЖЕННЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ

У 2014 році була започаткована серія конференцій SSR, присвячена дослідженням стандартизації безпеки. За останні два десятиліття було розроблено широкий спектр стандартів, які охоплюють безліч аспектів кібербезпеки. Стандарт – це документ який визначають процедурою та настановою, для спрямування безпеки, надійності та узгодженості продукції, які опубліковані національними та міжнародними офіційними органами стандартизації, а також галузевими консорціумами [8].

ISO - це всесвітня федерація національних органів стандартизації. Робота з підготовки міжнародних стандартів зазвичай здійснюється через цей технічний комітет. Вона тісно співпрацює з Міжнародною електротехнічною комісією (IEC) з усіх питань електротехнічної стандартизації.

SAE International - це міжнародна асоціація, що об'єднує понад 128 000 інженерів та суміжних технічних експертів в аерокосмічній, автомобільній та комерційній галузях. Стандарти SAE використовуються для розвитку інженерії мобільності в усьому світі.

Сфера застосування стандартів кібербезпеки охоплює функції безпеки в додатках і криптографічних алгоритмах, які забезпечують контроль безпеки, процесів, процедур, керівних принципів і базових рівнів. Експерти з безпеки рекомендують впроваджувати стандарти кібербезпеки як фундаментально важливий елемент, що складається з набору найкращих практик для захисту організацій від загроз і ризиків кібербезпеки.

Основною метою стандартів кібербезпеки є запобігання або пом'якшення наслідків кібератак та зменшення ризику кіберзагроз. Впровадження стандартів дозволить заощадити час, зменшити витрати, збільшити прибутки, підвищити обізнаність користувачів, мінімізувати ризики та забезпечити безперервність бізнесу. Крім того, використання стандартів сприяє дотриманню організацією найкращих галузевих практик і процедур та надає можливість порівнювати систему безпеки на міжнародному рівні.

2.1 Огляд стандарту ESTI EN 303 645

ETSI EN 303 645 [9] - це перший стандарт кібербезпеки для споживчих пристроїв Інтернету речей, що застосовується в усьому світі випущений у червні 2020 року. Пройшов через коментарі та голосування в Національній організації зі стандартизації, що дозволило залучити ще більше зацікавлених сторін до його розробки та, зрештою, зміцнити отриманий стандарт. Він охоплює споживчі IoT-пристрої, підключені до мережевої інфраструктури та їх взаємодію з супутніми послугами, такими як смарт TV, камери відеоспостереження, динаміки, підключені пристрої домашньої автоматизації, дверні замки, детектори диму та багато інших.

Стандарт ETSI EN 303 645 всебічно охоплює життєво важливі аспекти безпеки споживчих пристроїв Інтернету речей, включаючи управління паролями, розкриття вразливостей, оновлення програмного забезпечення, безпечний зв'язок, зменшення поверхні атаки, захист даних і відмовостійкість системи, серед іншого. А також 33 вимоги до безпеки та 35 рекомендацій, які повинні бути реалізовані в споживчих пристроях IoT. Впроваджуючи ці рекомендації, виробники можуть гарантувати, що їхні пристрої відповідають необхідним стандартам безпеки та надають споживачам більш безпечну та надійну екосистему Інтернету речей.

Основні вимоги стандарту [10]:

Першим ключовим аспектом є підвищення кібербезпеки споживчих пристроїв IoT, а саме відмовитися від універсальних паролів за замовчуванням. Завдяки йому хакери можуть швидко отримати несанкціонований доступ до пристроїв, ставлячи під загрозу конфіденційність і безпеку користувачів. Кілька прикладів паролів за замовчуванням, які широко використовувалися в минулому:

- «admin» або «admin123»: це поширений пароль за замовчуванням для багатьох типів пристроїв, включаючи маршрутизатори, мережеві комутатори та вебінтерфейси;

- «password» або «123456»: ці паролі часто використовуються як паролі за замовчуванням для різних пристроїв та онлайн-акаунтів, попри те, що вони легко вгадуються і є слабкими;
- «guest» або «guest123»: деякі споживчі пристрої Інтернету речей, такі як бездротові точки доступу або розумні домашні пристрої, можуть мати паролі такого типу. Однак їх слід змінити з міркувань безпеки;
- «admin1234» або «admin_admin»: ці паролі також використовуються як облікові дані за замовчуванням для адміністративного доступу до пристроїв і систем;
- «1234» або «0000»: деякі прості пристрої, такі як цифрові замки, можуть мати такі паролі за замовчуванням, щоб запобігти несанкціонованому доступу.

Другим ключовим аспектом є впровадження засобів управління повідомленнями про вразливості. Своєчасне реагування на вразливості значно варіюється і залежить від конкретного інциденту, однак процес усунення вразливості завершується протягом 90 днів для програмного рішення, включаючи наявність патчів та повідомлення про проблему. Апаратне виправлення може зайняти значно більше часу, ніж програмне. Виробники повинні проявляти належну обережність щодо всіх програмних та апаратних компонентів, які використовуються в продукті, включаючи належну обережність для третіх сторін, які надають супутні послуги для підтримки функцій продукту. Програмні рішення часто містять програмні компоненти з відкритим кодом та сторонніх розробників. Створення та підтримка списку всіх програмних компонентів та їхніх під компоненти є необхідною умовою для моніторингу вразливостей продукту.

Основним аспектом є своєчасна розробка та розгортання оновлень безпеки. Належна практика полягає в тому, що все програмне забезпечення повинно бути новим і належним чином підтримуватися. Механізми оновлення можуть варіюватися від швидкості завантаження безпосередньо з віддаленого сервера, передачі з мобільного додатку до передачі через USB або інший

фізичний інтерфейс. Якщо зловмисник компрометує цей механізм, він може встановити на пристрій шкідливу версію програмного забезпечення. Оновлення безпеки можуть надаватися для пристроїв превентивно, як частина автоматичних оновлень, які можуть усунути вразливості безпеки до того, як вони будуть використані. Керування цим може бути складним, особливо якщо паралельно відбуваються пов'язані з цим оновлення служб або пристроїв. Тому чіткий план управління та розгортання є вигідним для виробника, так само як і прозорість для споживачів щодо поточного стану підтримки оновлень.

2.2 Безпека електронних систем автомобіля на основі ISO/SAE 21434

В останні роки еволюція дорожніх транспортних засобів настійно вимагала загальних правил для управління кібербезпекою в автомобільній промисловості. Постійне збільшення кількості електронних та програмних компонентів у транспортних засобах зумовлене безперервним розвитком, безпекою та захистом користувачів. Зокрема висхідна складність таких комунікацій потребує спільних стандартів і правил для різних учасників дорожньої інфраструктури.

ISO/SAE 21434 є стати стандартом кібербезпеки при розробці електронних систем в дорожніх транспортних засобах. Документ надає виробникам оригінального обладнання та їхнім постачальникам рекомендації щодо управління культурою, політикою та ризиками кібербезпеки на кожному етапі інжинірингового процесу. Стандарт не передбачає конкретних технічних рішень. Однак він являє собою загальну основу для управління ризиками кібербезпеки для декількох типів дорожніх транспортних засобів [11]. Автомобільний сектор знаходиться на шляху до повністю автономних транспортних засобів. Навіть якщо ці типи транспортних засобів не згадуються безпосередньо, стандарт можна вважати базовим для підвищення безпеки та захисту критично важливих кіберфізичних систем, таких як електронні компоненти автономних транспортних засобів. З іншого боку, автономні транспортні засоби можуть вимагати глибшого підходу до кібербезпеки, що має бути відображено в

стандарті. Документ ISO/SAE 21434 складається зі вступу, п'ятнадцяти розділів та восьми додатків. Перші два розділи визначають сферу застосування та нормативні посилання. Третій розділ містить низку визначень слів для створення загального глосарія автомобільної кібербезпеки, що було одним з основних очікуваних нововведень ISO/SAE 21434. Наступні розділи називаються «положеннями», де визначаються вимоги, рекомендації та робочі продукти. У п’ятому пункті важливим нововведенням є визначення та вимога до сильної культури кібербезпеки, де кібербезпека та безпека мають найвищий пріоритет, а також визначення в процедур обміну інформацією. В дев’ятому пункті визначаються цілі кібербезпеки, які є результатом аналізу загроз та оцінки ризиків, пов'язаних з об'єктом. Зокрема, цей пункт визначає декілька документів, що базуються на ідентифікації активу, оцінці впливу, аналізі шляхів атаки та визначення величини ризику.

2.3 Взаємодія міжнародних стандартів в автомобільній кібербезпеці

Найсильніший зв'язок існує між ISO/SAE 21434 та ISO 26262. На перший погляд, можна помітити багато спільного в тому, як обидва стандарти пояснюють свої сфери застосування. Існує декілька типів фаз: управління, концепції, розробки продукту та після розробки. Оскільки ISO 21434 дотримується того ж підходу, що й ISO 26262, ця схожість є очікуваною. Однак, при більш уважному розгляді можна виявити кілька нових фаз, які є унікальними для кібербезпеки.

ISO 26262 - міжнародний стандарт функціональної безпеки, розглядає потенційні небезпеки, спричинені несправностями в електронних та електричних системах транспортних засобів. Стандарт розглядає потенційні небезпеки, спричинені несправностями в електронних та електричних системах транспортних засобів. Функції FuSa є невід'ємною частиною кожного етапу розробки автомобільного продукту, від специфікації до проєктування, впровадження, інтеграції, верифікації, валідації та випуску у виробництво [12].

Щоб зменшити численні ризики, які інноваційні технології вносять в сучасні транспортні засоби, ISO 26262 надає набір детальних настанов і вимог до їх функціональної безпеки, в тому числі та до функціональної безпеки:

Життєвий цикл автомобільної безпеки, який охоплює управління, розробку, виробництво, обслуговування та виведення з експлуатації. Крім того, стандарт підтримує адаптацію необхідних заходів на цих етапах життєвого циклу.

Аспекти функціональної безпеки всього процесу розробки, включаючи такі види діяльності, як специфікація вимог, проєктування, впровадження, інтеграція, верифікація та конфігурація.

Рівні цілісності автомобільної безпеки: підхід до визначення класів ризиків, специфічний для автомобільної галузі, що базується на ризиках.

ASILs використовуються для визначення необхідних вимог до безпеки елементів для досягнення прийнятного залишкового ризику.

Вимоги до валідації та заходів підтвердження гарантують, що достатній і прийнятний рівень безпеки досягається.

Новими доповненнями в ISO 21434 є:

- управління кібербезпекою, залежне від проєкту: оскільки вимоги та застосування кібербезпеки можуть відрізнятися в різних автомобільних рішеннях, до стандарту було додано частину шість.
- безперервна діяльність з кібербезпеки**:** загрози кібербезпеці постійно розвиваються, що робить її безперервною діяльністю. Необхідно аналізувати нові загрози та оновлювати автомобільне програмне забезпечення, щоб протистояти їм. У цьому відношенні кібербезпека різко відрізняється від стандарту функціональної безпеки, у якому небезпеки і пов'язані з ними ризики аналізуються на початковому етапі, а механізми захисту впроваджуються на місці.
- метод оцінки ризиків**:** стандарт ISO 21434 чітко визначає методи оцінки ризиків, які включають такі процеси, як ідентифікація активів, аналіз шляхів атаки тощо. ISO 26262 визначає HARA як основний спосіб

ідентифікації загроз і пов'язаних з ними ризиків, і він значною мірою охоплює фазу концепції.

2.4 Висновки до розділу 2

Сучасні підключені до інтернету транспортні засоби мають бути не лише надійними та високотехнологічними, але й безпечними. У багатьох аспектах кібербезпека безпосередньо відповідає за фізичну безпеку автомобіля, пасажирів і учасників дорожнього руху. У свою чергу зростає важливість функціональності кібербезпеки для надійного захисту від майбутніх загроз.

Розглядаючи стандарти, що фокусується на кібербезпеці автомобільних систем такі, як ISO/SAE 21434 та ETSI EN 303 645, що встановлюють вимоги для IoT-пристроїв. Їх схожість і взаємодоповнюваність відкривають нові можливості для вдосконалення сучасних транспортних систем. Хоча стандарти кібербезпеки для автомобільної промисловості все ще є досить новими, очевидно, що розробка нових інструментів і технологій, які реалізують обидва стандарти, стане важливим кроком на шляху їх інтеграції.

Майбутня галузь автомобільної промисловості отримує більшу залежність від співпраці виробників, постачальників, регуляторів і незалежних експертів. Ця взаємодія необхідна для подальшого розвитку безпеки у складнішому цифровому середовищі. Крім того, впровадження цих стандартів у великомасштабне виробництво створює єдиний підхід до управління ризиками та закладає новий фундамент для подальшого розвитку технологічної безпеки всією автомобільної інфраструктури. Незалежно від нових викликів, які можуть з'явитися в майбутньому, співпраця різних зацікавлених сторін відкриває перспективу реалізації комплексної концепції безпеки, яка забезпечуватиме одночасно функціональність, надійність і захист сучасних автомобілів.

3 АНАЛІЗ ВРАЗЛИВОСТЕЙ В МЕРЕЖАХ IOT

Проєкт OWASP в Інтернеті речей бере свій початок з 2014 року. Його основна мета – це допомога виробникам, розробникам та підприємствам в забезпечені покращеного захисту для IoT пристроїв. Проєкт продовжує свою роботу і сьогодні який представляє десять головних вразливостей, яких слід уникати при розгортанні інтелектуальних систем. Замість того, щоб складати окремі списки ризиків та вразливостей команда проєкту створила єдиний уніфікований список. Він охоплює в собі речі, яких треба уникати при роботі з безпекою IoT.

Вразливості OWASP IoT [13]:

1. Слабкі або легко вгадуванні паролі

Пристрої Інтернету речей зазвичай мають вебінтерфейси, які використовуються для конфігурації та управління, а також для виконання автентичних завдань на пристрої, таких як мережеві служби. Якщо ці інтерфейси не налаштовані належним чином, зловмисники можуть отримати доступ до конфіденційної інформації та спричинити несанкціоновані зміни в конфігурації пристрою.

Оцінки тестування безпеки IoT довели, що більшість протестованих пристроїв IoT містять паролі, які легко вгадуються. Вони є вбудованими, що слугує серйозною проблемою, коли розробники розміщують жорстко закодовані облікові дані в компонентах пристроїв IoT, наприклад, у прошивці.

У свою чергу виробники повинні впровадити відповідні механізми автентифікації та управління паролями, щоб переконатися, що паролі надійні і їх нелегко вгадати. Крім того, слід заохочувати користувачів змінювати паролі за замовчуванням на пристроях і робити їх більш надійнішими від підбору під час виконання налаштувань пристрою.

2. Незахищені мережеві служби

Вразливості в протоколах або конфігураціях безпеки, такі як незашифровані протоколи зв'язку, відсутність належних конфігурацій мережевої

безпеки та використання застарілого або вразливого програмного забезпечення, відносяться до незахищених мережевих сервісів. Зловмисники можуть використовувати ці вразливості для доступу до конфіденційних даних, здійснення атак на інші системи або отримання несанкціонованих дозволів на пристрій.

Безпечні мережеві протоколи, такі як Transport Layer Security та регулярне оновлення мережевих служб можуть зменшити цю проблему. Проведення періодичних оцінок вразливості мережі допомагає виявити критичні недоліки безпеки в мережах IoT.

3. Незахищені інтерфейси екосистеми

Вразливість виникає через незахищеність інтерфейсів між різними компонентами, що існують в екосистемі IoT. Різні пристрої можуть мати погано захищені вебінтерфейси, API або мобільні інтерфейси із зовнішніми системами, такими як традиційні IT-системи, хмарні сервіси та інші пристрої IoT. Зловмисники можуть використовувати їх для отримання доступу до конфіденційних даних, здійснення атак на інші системи або керування пристроєм та його функціями.

Рішенням цього є послідовне виправлення API, впровадження суворого контролю доступу для обмеження доступу до чутливих інтерфейсів, розгортання захищених каналів зв'язку між різними компонентами екосистеми IoT та впровадження шифрування.

4. Відсутність безпечного механізму оновлення

Пристрої Інтернету речей є безпечними, економічно ефективними, малопотужними та простими у використанні, це призводить до того, що в багатьох ситуаціях питанням безпеки не приділяється належної уваги. Відсутність механізму оновлення може зробити пристрої чутливими до певних експлойтів або вразливостей.

Зловмисники можуть скористатися застарілим програмним забезпеченням або прошивкою, щоб поставити під загрозу загальну безпеку пристрою. Вразливість платіжних систем Інтернету речей може призвести до серйозних

наслідків, які включають фінансові втрати, несанкціонований доступ до конфіденційних даних та порушення роботи критично важливих систем.

Впровадження таких функцій, як цифровий підпис, механізми відкату та перевірка прошивки на пристроях, допомагає виробникам ефективно усунути вразливості.

5. Використання незахищених або застарілих компонентів

Основною проблемою, яка виникає в пристроях Інтернету речей, є використання в них застарілих або незахищених компонентів. Багато пристроїв IoT інтегровані зі сторонніми компонентами, що може призвести до вразливостей. Виробники, які використовують відкритий вихідний код для створення пристроїв Інтернету речей, створюють складний ланцюжок постачання, який важко відстежити. Ці компоненти можуть успадкувати вразливості, відомі зловмисникам і створити ландшафт загроз, який може призвести до компрометації пристрою.

Рішенням цього є регулярне оновлення програмного забезпечення, яке виправляє вразливості різних компонентів (прошивки або фреймворки) в пристроях Інтернету речей. Потрібно також відстежувати та отримувати сповіщення про вразливості безпеки в компонентах, які використовуються в системах IoT.

6. Відсутність належного захисту конфіденційності

Різні пристрої Інтернету речей отримують і зберігають конфіденційну особисту інформацію, але при цьому вони не забезпечують належного захисту приватності. Це може бути збір даних без згоди користувача або належного контролю безпеки та обмін даними з третіми сторонами не маючи відповідних дозволів.

Ефективними рішеннями є впровадження принципів конфіденційності, використання шифрування для захисту конфіденційних даних під час зберігання та передачі, а також отримання згоди користувача на збір та використання даних.

7. Незахищена передача даних

Передача даних у вигляді простого тексту без шифрування є серйозною проблемою для пристроїв Інтернету речей. Пристрої збирають як конфіденційні дані, так і інформацію про користувачів. Зловмисники можуть маніпулювати ними під час передачі або використовувати вразливі місця.

Наприклад, у деяких випадках, коли пристрій використовує протокол передачі файлів, зловмисник може отримати доступ до трафіку і модифікувати його. До цієї вразливості може призвести незахищений протокол HTTP, який маршрутизує кожне з'єднання з Інтернетом.

Безпечні протоколи, такі як HTTPS для передачі файлів, шифрування конфіденційних даних, розгортання надійних засобів контролю доступу до даних і регулярний аудит практики зберігання даних допомагають захистити передачу і зберігання даних в пристроях Інтернету речей.

8. Відсутність управління пристроями

Неспроможність ефективно керувати пристроями Інтернету речей може скомпрометувати всю мережу. Відсутність плідного управління пристроями призводить до того, що зловмисники можуть маніпулювати або керувати пристроями IoT. Відсутність управління може призвести до несанкціонованого доступу, маніпуляцій з пристроями або підміни прошивки.

Наприклад, прострочені SSL-сертифікати на пристроях можуть призвести до того, що зв'язок з Інтернетом буде здійснюватися за протоколом HTTP. Сертифікати SSL не оновлюються, оскільки пристрій не може надати оновлення, що робить його вразливим.

Рішенням цього є впровадження надійних механізмів автентифікації, таких як унікальні облікові дані пристрою та впровадження контролю доступу, щоб обмежити функції керування пристроєм відповідними фахівцями, може усунути цей ризик.

9. Небезпечні налаштування за замовчування

Налаштування за замовчуванням зазвичай є незахищеними, що робить пристрої Інтернету речей вразливими до ризиків високого рівня безпеки. До них

відносяться конфігурації за замовчуванням, які використовувалися спочатку, але були залишені без змін. Це можуть бути стандартні імена користувачів, паролі, відкриті порти, незашифровані комунікації тощо. Часто налаштування за замовчуванням можуть містити вразливі місця в системі безпеки, наприклад, відкриті сервіси, які працюють з правами суперкористувача.

Зміна стандартних імен користувачів, конфігурацій та паролів під час початкового налаштування пристрою, а також вимкнення небажаних служб і портів для мінімізації поверхні атаки може допомогти зменшити вразливість.

10. Відсутність фізичного захисту

Відсутність фізичного захисту може бути перешкодою для забезпечення фізичної безпеки. Це робить вбудовані пристрої вразливими до різних апаратних атак або фальсифікації прошивки, що дає хакерам несанкціонований доступ, наприклад, для входу в систему з правами Root. Надалі це може призвести до вилучення інформації та бути корисною для віддалених атак або контролю над пристроєм Інтернету речей.

Для захисту пристроїв можна вжити певних заходів, наприклад, вимкнути або ізолювати пристрої, налагодити порти, використовувати їх для перевірки прошивки, впровадити механізми виявлення несанкціонованого доступу та не зберігати конфіденційні дані.

3.1 Аналіз вразливостей IoT інфраструктури підключеного автомобіля

Тестування на проникнення Інтернету речей виходить за рамки окремих пристроїв і охоплює цілі екосистеми. Від розумних будинків і промислових об'єктів до підключених автомобілів, де кожен взаємопов'язаний вузол становить потенційний ризик. Проведення ретельного тестування на проникнення IoT забезпечує загальну стійкість цих систем. Вектори атак в інтелектуальних пристроях включають апаратне забезпечення, прошивку, мережу, бездротовий зв'язок, мобільні та вебдодатки, а також хмарні інтерфейси API.

По суті, тестування на проникнення передбачає імітацію атаки на системи IoT, подібно до навчань з безпеки. Основна мета полягає у виявленні вразливостей та слабких місць, якими можуть скористатися хакери, завдяки чому зможе спростити організаціям й приватним особам вживати дії на упередження для подальшого усунення недоліків.

Віддалене хакерство є глибокою та багатогранною перешкодою для сучасних розумних автомобілей. Першою причиною є те, що через їхню значну залежність від бездротового зв'язку задля виконання таких важливих функцій, як навігація, керування та обмін даними. Також, нові транспортні засоби мають великий спектр різноманітних каналів зв'язку. Одним з таких є V2X, стільникові мережі та Wi-Fi, що дозволяю взаємодіяти з іншими транспортними засобами, інфраструктурою і хмарними сервісами. У кожного з них є ряд потенційних вразливостей, якими кіберзловмисники можуть скористатися для отримання несанкціонованого доступу до критично важливих систем транспортного засобу [14].

Надалі використовуючи слабкі місця в програмній архітектурі або комунікаційних протоколах транспортного засобу, зловмисники можуть отримати доступ мережу. Що своєю чергою призведе до виконання шкідливих дій, таких як отримання контролю над системами керування, прискорення і гальмування автомобіля, зміна його запланованого маршруту або відключення важливих функцій безпеки. Проблеми такого масштабу можуть потягнути за собою катастрофічні наслідки, що у свою чергу ставить під загрозу життя пасажирів й інших учасників дорожнього руху та потенційно може призвести до масштабних дорожньо-транспортних пригод.

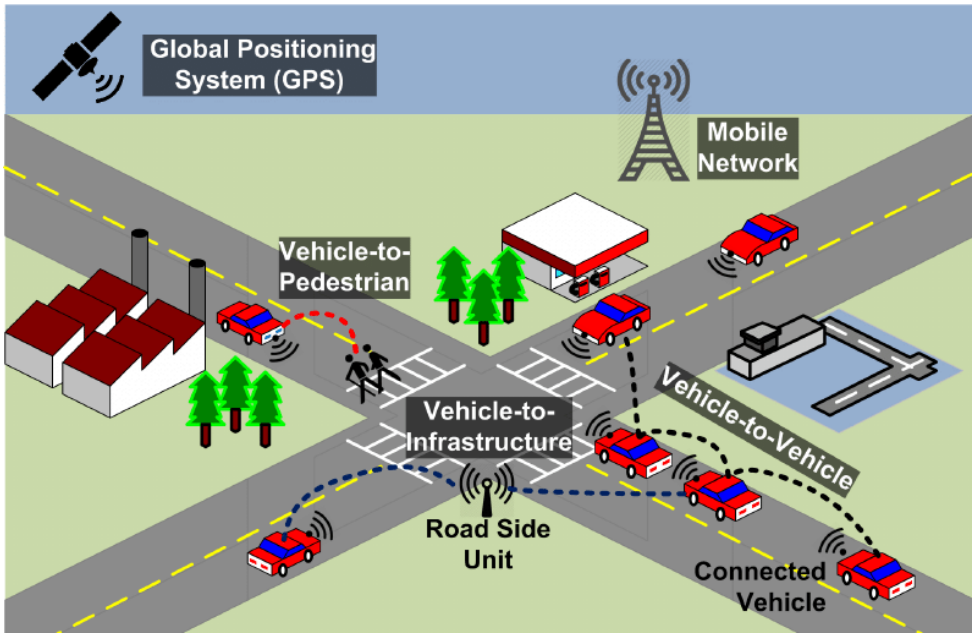

Рисунок 3.1 - Приклад роботи зв'язку V2X в автономних транспортних засобах

З автоматизацією та спрощенням водіння сучасні автономні транспортні засоби покладаються на складний набір датчиків, якими є: радари, камери Lidar та ультразвукові датчики. У комплексі це додаткове управління слугує для точного сприйняття та інтерпретації навколишнього середовища, отримання критичної інформації. Однак ця залежність призводить до майбутніх маніпуляцій з транспортним засобом. Підробка цих датчиків несе за собою неправдиві дані в сенсорній системі, у той час, як глушіння порушує нормальне функціонування датчиків, що передбачає за собою перевантаження зайвим шумом або сигнальними перешкодами. Використовуючи ці дії хакери здатні створювати фіктивні сценарії, це може призвести до того, що системи керування транспортним засобом будуть неправильно інтерпретувати навколишнє середовище. Прикладом може бути, створення хибних перешкод на шляху транспортного засобу. Все це прямо пропорційно призведе до раптового гальмування, а приховування реальних перешкод, до зіткнення транспортного засобу. У підсумку водій отримає нестабільну поведінку й відсутність прямого керування авто, це створить значні ризики для безпеки пасажирів та інших учасників дорожнього руху.

3.2 Перспективи розвитку захисту для IoT пристроїв

Безпека пристроїв IoT з кожним днем все більше змінюється через ринкові тенденції та розвиток нових загроз і вразливостей. Постійний моніторинг останніх розробок у виявленні вразливостей, методах атак і стратегіях пом’якшення є фундаментальним аспектом ефективного тестування на проникнення. Ось чому було розроблено багато складних рішень кібербезпеки для захисту критично важливих систем і даних. Завдяки цим передовим технологіям безпеки загрози можна не тільки виявити, але й пом’якшити за допомогою різноманітних інструментів, таких як системи виявлення вторгнень, шифрування, бездротові оновлення та надійні протоколи автентифікації [15]. Нище приведено ключові аспекти:

Системи виявлення вторгнень

Загальним сегментом у питанні кібербезпеки автономних транспортних засобів є система виявлення вторгнень. Вона постійно відстежує мережевий трафік і діяльність пристрою на предмет ознак зловмисної поведінки. Завдяки чому використовується максимально швидке виявлення та реагування на потенційні загрози в режимі реального часу, тим самим захищаючи критичні системи та дані транспортного засобу. Система IDS може бути налаштована на виявлення широкого спектра кіберзагроз. А саме, спробу несанкціонованого доступу, незвичайні моделі трафіку даних і аномалії, які своєю чергою свідчать про наявність шкідливого програмного забезпечення.

Сучасні IDS системи використовують складні алгоритми машинного навчання та аналітику виявлення загроз для покращення своїх можливостей виявлення. Завдяки чому використовуються модель навчання на історичних даних для розпізнавання векторів атак і має покращений рівень адаптації до майбутніх загроз. Модель штучного навчання з більшою точністю та швидкістю ідентифікує загрози, а також аналізує великі масиви даних мережевого трафіку і системних журналів. Завдяки цим діям покращується точність та ефективність виявлення загроз.

Шифрування

Шифрування є важливою основою кібербезпеки в сучасних автономних транспортних засобах та відіграє ключову роль у захисті великих обсягів даних. Основним аспектом є перетворення інформації у закодовану форму, яку можна розшифрувати лише за допомогою певного алгоритму. Завдяки цьому конфіденційність інформації може передаватись і зберігатися без перешкод. Сучасні методи шифрування, такі як AES і RSA, можуть більш надійно захистити зв'язок між інструментами, інфраструктурою та хмарними службами.

Симетричні блочні алгоритми шифрування широко використовуються в галузі ефективної та надійної безпеки інформації. Це робить його ідеальним для високошвидкісного шифрування великих обсягів даних. RSA — це асиметричний алгоритм шифрування, який зазвичай використовується для безпечного обміну ключами та даними між сторонами без спільного використання приватних ключів.

Регулярні оновлення

Динамічний характер загроз кібербезпеці вимагає регулярних оновлень програмного забезпечення та прошивки для автономних транспортних засобів (ТЗ). Бортові оновлення (OTA) є важливим інструментом у цьому процесі, що дозволяє виробникам віддалено розгортати виправлення безпеки, помилок та вдосконалення на автомобілях без водіїв, які не мають фізичного доступу до автомобіля. Ця можливість необхідна для швидкого усунення нещодавно виявлених вразливостей та забезпечення захисту систем транспортних засобів від нових загроз. Оновлення по повітрю (OTA) необхідні для підтримки безпеки та функціональності вашої AV-системи. Безпечний механізм оновлення забезпечує цілісність наданого програмного забезпечення без зовнішнього втручання. Типовим прикладом є Ota від Tesla, яка успішно встановлює критичні виправлення безпеки на автомобілі у відповідь на виявлені вразливості. Стійкість антивірусної системи до шкідливих програм підвищується в результаті регулярних оновлень.

Протоколи автентифікації

Нові протоколи автентифікації є критично важливими заходами в питанні кібербезпеки. Вони забезпечують авторизацію до пристроїв, щоб користувачі та системи могли отримати доступ для взаємодії з мережею керування автономного транспортного засобу. Завдяки цим протоколам здійснюється легітимність суб'єктів, які намагаються встановити зв'язок з автомобілем. У результаті робота інструменту і конфіденційність даних захищені від несанкціонованого доступу. Багатофакторна автентифікація підвищує безпеку, вимагаючи декількох форм перевірки, перш ніж транспортний засіб зможе дозволити доступ до системи. Цифрові сертифікати є ще одним важливим компонентом надійного протоколу доступу. Вони використовує механізм відкритих ключів (PKI) для автентифікації пристрою та користувача. Коли різні гаджети або користувачі намагається приєднатися до мережі транспортного засобу, цифровий сертифікат використовує метод шифрування для автентифікації.

3.3 Висновки до розділу 3

Тестування на проникнення в системах IoT вимагає більшої уваги, ніж перевірка окремих пристроїв. Воно охоплює цілі екосистеми, де під загрозою можуть опинитися кожен вузол і взаємозв'язок у складному ланцюзі. Від розумних будинків і заводських роботів до підключених автомобілів – уся інфраструктура IoT може стати вразливою. Виконання ретельного тестування на проникнення сприяє зміцненню загальної стійкості систем IoT, дозволяючи своєчасно виявляти й усувати ризики, які зловмисники можуть використати для зламу або саботажу.

Інфраструктура IoT в свою чергу передбачає з’єднання на різних рівнях: на апаратному, мережевому, а також бездротовому. Модель такого роду атак при тестуванні допомагає знайти ті набори, які хакери зможуть використати для доступу до конфіденційної інформації. Основною задачею на тестування є

визначення об'єктів нападу і розробка схеми захисту, яка буде захищати організації та користувачів від більшості атак навіть до їх вчинення.

Автономні та підключені до інтернету транспортні засоби потребують надійного бездротового з’єднання для контролю, навігації, передачі даних все це підпадає під вплив безпосередньо кіберзагрозам. Для взаємодії з іншими автомобілями, інфраструктурою та хмарними сервісами вони використовують канали V2X, стільникові мережі, Wi-Fi, кожен з яких несе в собі потенційні вразливості для комунікаційних протоколів чи програмній архітектурі. Все це може дозволити зловмисникам отримати контроль над критично важливими системами. Вони здійснюють такі дії: маніпулювання системами гальмування і прискорення, зміна маршруту, вимкнення безпекових функцій. Подібні атаки несуть загрозу для водіїв, пасажирів та інших учасників дорожнього руху, створюючи ризики масштабних дорожньо-транспортних пригод.

Автономні транспортні засоби використовують широкий набір сенсорів, включаючи LiDAR, радари, камери та ультразвукові датчики, для забезпечення точного розпізнавання навколишнього середовища. Однак вони також є слабким місцем. Через них транспортні засоби стають вразливими до атак, прикладом є підробка даних або глушіння. Ця методика полягає в тому, щоб ввести сенсори в оману, надаючи їм неправдиві дані, а глушіння – у створенні шуму, який порушує функціонування сенсорів. Таким чином, зловмисники можуть створювати фальшиві перешкоди або, навпаки, приховувати справжні, що веде до хибного інтерпретування середовища автомобілем. Наприклад, фальшиві об'єкти можуть змусити автомобіль раптово зупинитися, а реальні – залишитися непоміченими, що може призвести до зіткнень. Ці сценарії порушують стабільність роботи автономних транспортних засобів, що створює небезпеку для пасажирів і людей навколо.

4 ОЦІНКА РИЗИКІВ ТА ВДОСКОНАЛЕННЯ СИСТЕМ КІБЕРБЕЗПЕКИ АВТОМОБІЛЯ

Підключений автомобіль вже став реальністю. Це тема охоплює не лише споживачів і виробників, але й дослідників безпеки та IT-експертів. У гіршому випадку хакерів-злочинців. Протягом багатьох років експерти з безпеки спостерігали той факт, що настільний ПК більше не єдина ціль цифрових атак. Значна частина шкідливого програмного забезпечення зараз адаптована для ураження мобільних пристроїв. Було б необачно вважати, що такий розвиток подій залишить без уваги підключений до мережі автомобіль.

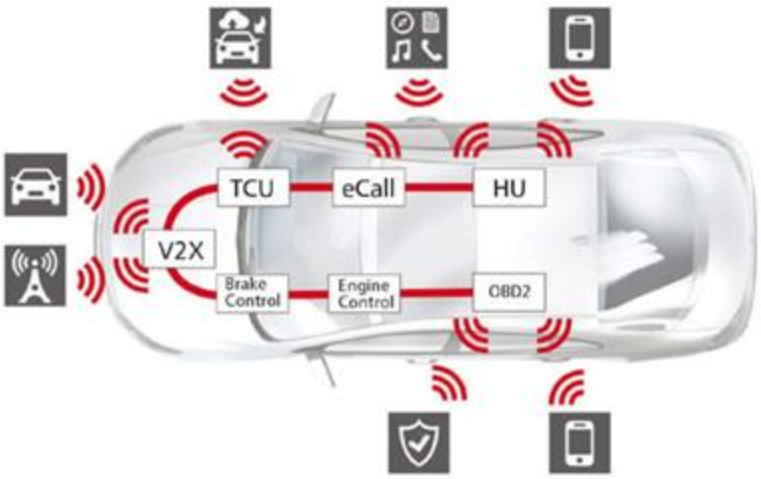

Рисунок. 4.1 - Основні системи зв'язку автомобіля

До сьогодні атаки злочинних хакерів на транспортні засоби та їхні системи були дуже рідкісними винятками. Ключова важливість безпеки для підключених автомобілів стала очевидною для автовиробників. Коли транспортний заісб стає персональним мобільним пристроєм, що використовується його власником для зв'язку, а також персоналізується за допомогою додатків, це надає потенційним зловмисникам безліч можливостей для маніпуляцій.

Відмова від усіх повітряних інтерфейсів - концепція, яку давно підтримує частина автомобільної індустрії - не відповідає інтересам клієнтів. Потреба в з'єднанні для обміну даними також очевидна з інноваційними послугами V2V

або V2I, які будуть розроблятися, у тому числі в їхньому зв'язку з автономним водінням. Отже, у майбутньому неможливо повністю відмовитися від Bluetooth, WLAN або стільникового зв'язку в транспортному засобі [16].

З іншого боку, класичний підхід, де використовується зворотній дзвінок та виправлення помилок також не забезпечить своєчасного успіху в захисті транспортних засобів від цифрових зловмисників. Крім того, кампанії з відкликання викликають величезні витрати і завдають шкоди репутації автовиробника. Перегони з автомобільними хакерами в такий спосіб виграти неможливо. Адже пройдуть місяці, перш ніж всі автомобілі, що опинилися під загрозою, отримають виправлення. Такий часовий проміжок для відвернення небезпеки є неприйнятним, адже маніпульований транспортний засіб може становити величезну небезпеку як для водія, так і для його оточення. Крім того, у багатьох випадках за цей час можна виявити нові вразливості в програмному забезпеченні автомобіля, що робить патч вже застарілим на момент його встановлення.

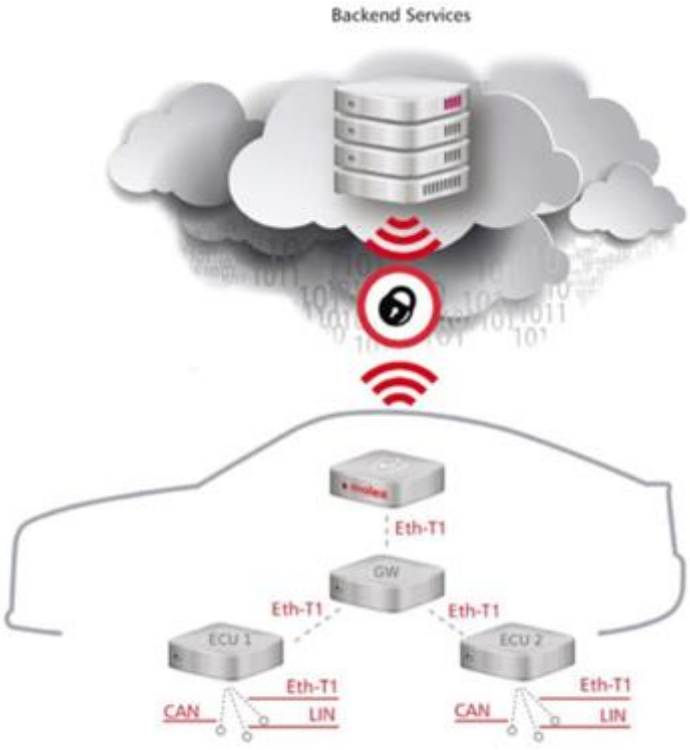

Рисунок. 4.2 - Архітектура шлюзового методу в оновленні програмного забезпечення автомобіля

Постачальники додатків та операційних систем для смартфонів постійно постачають на термінальні пристрої найновіші версії своїх продуктів. Іноді мова йде про невеликі виправлення для усунення слабких місць, а в інших випадках на ринок випускаються нові версії, що включають нові функції. Такі оновлення програмного забезпечення та мікропрограм доставляються «по повітрю», тобто за допомогою дистанційного методу. Як тільки ці оновлення передаються на пристрій, вони завантажуються і встановлюються автоматично.

Прошивка по повітрю - це відповідь на виклики, пов'язані зі швидким оснащенням безлічі пристроїв останніми оновленнями. Процедура оновлення забезпечує можливість швидкого і безперервного усунення слабких місць за допомогою відповідних патчів, одночасно інтегруючи нові функції і модернізуючи криптографічні методи для захисту.

Щоб забезпечити можливість оновлення великої кількості блоків управління за допомогою FOTA, використовується метод шлюзу. Між серверною частиною і блоками управління, які підлягають оновленню, він оснащений мобільним радіоінтерфейсом, бере на себе роль посередника. Він отримує всі програмні пакети через радіоінтерфейс і розподіляє їх на пристрої призначення за допомогою систем шини CAN або більш продуктивних каналів зв'язку, таких як Ethernet. Крім того, електронний блок управління шлюзу виконує основну функцію контролю і координації всього процесу оновлення. У разі виникнення помилки може знадобитися запуск механізмів відкату.

4.1 Огляд архітектури діагностичної системи автомобіля

Продуктивність і складність електронних функцій постійно зростає завдяки автономному водінню, бездротовому управлінню та розвагам. За поточними оцінками, 90% інновацій в автомобільному секторі відбуваються в автомобільній електроніці та програмному забезпеченні. Прямим наслідком цієї тенденції є те, що ці електронні функції необхідно аналізувати, діагностувати, а потім підтримувати і вдосконалювати в польових умовах. Для майбутніх

технологій, таких як автономне водіння, абсолютно необхідно, з одного боку, контролювати алгоритми в польових умовах, а з іншого - вбудовувати отримані дані в автомобілі без необхідності відвозити машину в майстерню. Якщо оновлення програмного забезпечення одночасно зачіпають кілька серій автомобілів, то польові заходи, що проводяться авторизованими майстернями, коштують дорого і займають багато часу.

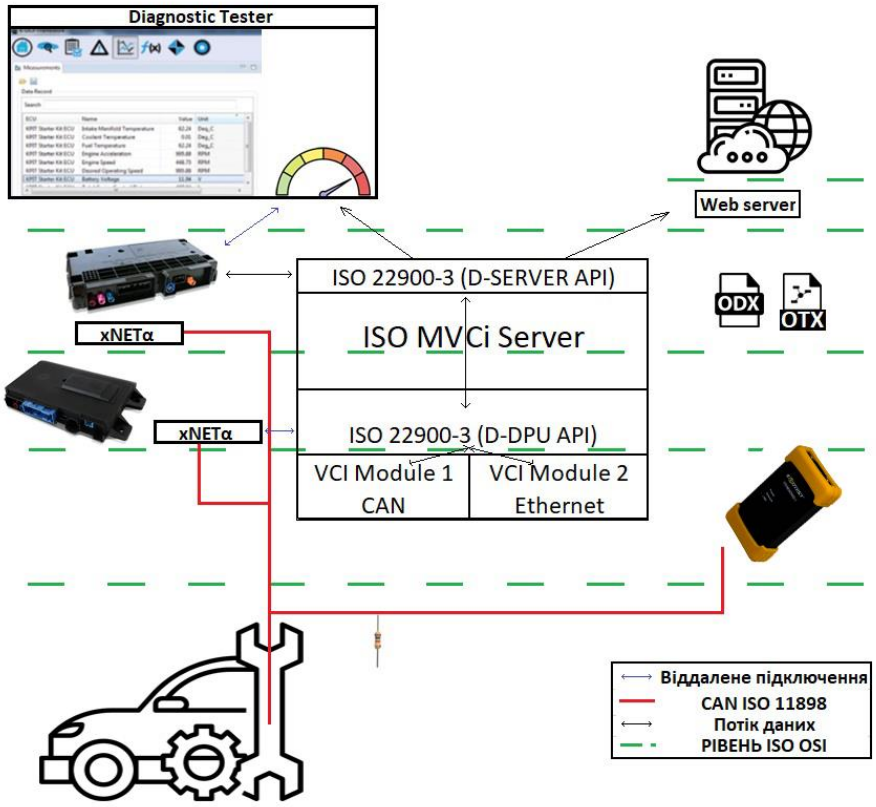

Рисунок 4.3 - Стандартизована архітектура системи діагностики з віддаленими інтерфейсами

Діагностичний протокол OBD-II широко використовується для збору інформації про стан автомобіля, зокрема про рівень викидів, для їх подальшого аналізу та моніторингу. Основною метою цього протоколу є забезпечення відповідності транспортного засобу екологічним стандартам і вимогам [17]. Відповідно до стандарту SAE J1979, кожен PID (ідентифікатор параметра) у системі OBD-II відповідає за запитування конкретних даних про певні параметри транспортного засобу. Наприклад, PID може приймати значення таких

параметрів, як швидкість двигуна, швидкість автомобіля, температура охолоджувальної рідини.

Слід зазначити, що не всі параметри автомобіля охоплюються стандартними кодами PID OBD-II. Виробники мають право додавати або змінювати ці коди за допомогою іншого діагностичного протоколу, наприклад UDS. Це дасть змогу налаштувати систему набагато гнучкішим способом для збору тих конкретних даних, які можуть знадобитися в діагностиці чи регулюванні конкретного автомобіля. Під час підключення діагностичного інструменту до порту OBD-II, електронний блок управління негайно обробляє та відповідає на запити, які надходять. Типовий формат кадру OBD-II показано на рисунку 4.4, який чітко визначає структуру обміну даними: поле ідентифікації вказує, чи є повідомлення запитом, чи відповіддю, а поле номера байта вказує на кількість даних, необхідних для повідомлення. Це стандартизує процес передачі даних і спрощує діагностику автомобіля.

Протокол OBD-II складається з десяти режимів, кожен зі своїм призначенням. Деякі режими використовуються для читання та видалення зареєстрованих кодів несправностей, тоді як інші надають дані в реальному часі, такі як поточна швидкість автомобіля, оберти двигуна або температура. Наприклад, третє поле кадру OBD-II визначає режим роботи протоколу з відповідним PID, зазначеним у четвертому полі. Існують такі PID, які вимагають використання певних формул, щоб отримані значення можна було перетворити на зрозумілий для людини вигляд. Одночасно поля даних (A, B, C, D) містять шістнадцяткові байти, які потім обробляються та перетворюються на логічні значення відповідно до мінімальних і максимальних граничних.

Рисунок 4.4 - Загальна структура OBD-II

Однією з можливих вразливостей, пов’язаних з використанням OBD-II, є здатність параметрів системи керування людиною, що може призвести до негативних наслідків. Наприклад, зловмисник може ввести невірне значення

температури охолоджувальної рідини двигуна, повідомляючи про її підвищення, навіть якщо все працює нормально. Це спричинить непотрібну роботу вентилятора охолодження радіатора, створюючи навантаження на систему охолодження та впливаючи на роботу двигуна.

Інша дія – це пошук на приладовій панелі низьких обертів двигуна. Це може дезорієнтувати водія, змушуючи його їхати швидше, ніж потрібно. У цьому випадку підвищується ризик виникнення надзвичайної ситуації, яка може загрожувати життю як самого водія, так і його пасажирів чи інших учасників дорожнього руху. Таким чином, безпека протоколу OBD-II має бути постійним пріоритетом, а також предметом удосконалення, щоб звести до мінімуму можливості зовнішнього втручання.

4.1.1 Структура OBD-II

Порт OBD-II, представлений Американським товариством автомобільних інженерів (SAE) у 1996 році, є важливим елементом сучасних автомобільних діагностичних систем. Цей стандарт був розроблений, як для регулювання викидів небезпечних речовин в атмосферу відповідно до вимог Агентства з охорони навколишнього середовища (EPA). Він вимагає, щоб всі автомобілі мали 16-контактний роз'єм, щоб діагностичні дані могли бути отримані з електронного блоку управління (ЕБУ) автомобіля.

Завдяки уніфікації діагностичної системи порт OBD-II забезпечує доступ до діагностичних кодів несправностей і ідентифікаторів параметрів, що дозволяє вимірювати такі параметри, як швидкість або витрата палива, у режимі реального часу. DTC слугують для виявлення несправностей у різних підсистемах автомобіля, а PID використовуються для моніторингу робочих параметрів транспортного засобу. Ці функції реалізуються через зчитувачі OBD-II, які запитують дані від ECU, використовуючи п’ять основних протоколів сигналізації: SAE J1850, ISO 15765, ISO 1941-2 та ISO 14230-4. Інформація з ECU

надходить у вигляді шістнадцяти кодів, які інтерпретуються відповідно до стандарту SAE J1979.

Таблиця 4.1 - Інтерфейс Роз'єму OBD-II

Номер контакту	Опис	Номер контакту	Опис
1	Непідключений	9	Непідключений
2	J1850 B+	10	J1850 B-
3	Непідключений	11	Непідключений
4	Шасі (заземлення)	12	Непідключений
5	Сигнальне заземлення	13	Непідключений
6	CAN-H	14	CAN-L
7	ISO K Line	15	ISO L
8	Непідключений	16	Акумулятор

Порт OBD-II має 16 контактів (рис. 4.5), однак у типовій конфігурації використовується лише дев'ять з них. Ця особливість робить стандарт гнучким для інтеграції з іншими системами автомобіля. Наприклад, автовиробники, як General Motors або Chrysler, застосовують додаткові шини даних, такі як GM LAN або Chrysler CCD, для підвищення ефективності діагностики. Ці шини використовуються для оновлення програмного забезпечення, налаштування систем і проведення розширеної діагностики. Однак виробники транспортних засобів часто обмежують доступ до специфікацій своїх систем, вимагаючи значних фінансових внесків для отримання даних про архітектуру ECU. Попри це, незалежні розробники створили пристрої, які розширюють функціональність порту OBD-II. Сучасні гаджети, оснащені Wi-Fi, Bluetooth або стільниковим зв’язком, відкривають нові можливості, зокрема страхування, що базується на пробігу, управління автопарком і відстеження використання автомобіля.

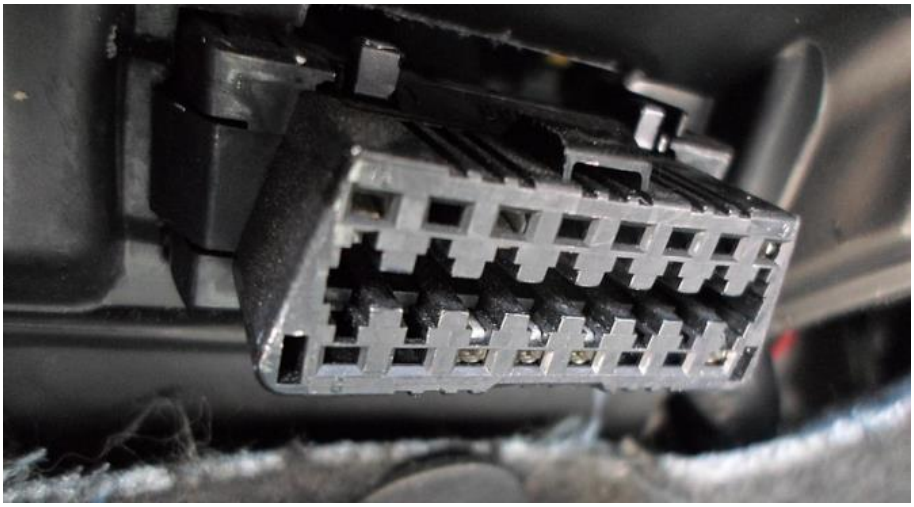

Рисунок 4.5 - Роз'єм OBD-II

З появою мобільних технологій зчитувачі OBD-II стали важливим інструментом для управління автопарком. Це охоплює всі аспекти життєвого циклу транспортного засобу – від закупівлі до виходу з експлуатації, що дозволяє зменшити ризики, покращити якість обслуговування та підвищити ефективність з найменшими витратами. Інформація з порту OBD-II дозволяє контролювати такі параметри, як швидкість, пройдена відстань, витрата палива, що допомагає зменшити викиди CO2 і підвищити безпеку на дорозі.

Дослідження в цій галузі показали ефективність інтеграції OBD-II з GPS і Wi-Fi для створення систем реального часу. Наприклад, автомобіль оснащується OBD-II сканером для зчитування значень даних, що передаються з датчиків, а потім передаються на віддалений сервер для аналізу. Такі системи активно використовуються в управлінні автопарком: вони фіксують витрату палива, оцінюють поведінку водія, відстежують місцезнаходження транспортного засобу та паспортні дані.

Хоча порт OBD-II є потужним діагностичним інструментом, він також створює нові виклики для безпеки. Потенційну загрозу можуть становити порти доступу до сторонніх пристроїв, сприяє несанкціонованому втручанню в роботу автомобіля. Це підкреслює важливість розробки додаткових інструментів захисту та шифрування даних. В цілому його впровадження є важливим кроком у стандартизації діагностики транспортних засобів, допомагаючи поліпшити

умови навколишнього середовища і підвищити ефективність управління автомобільними системами. Інтеграція з сучасними технологіями відкриває широкі перспективи для інновацій, спрямованих на підвищення комфорту, безпеки та екологічності транспортної інфраструктури.

4.1.2 Архітектура шини CAN

Усередині автомобіля порт OBD-II з'єднаний з однією або декількома комунікаційними шинами. CAN - це протокол шини, який підтримується завжди. Сам по собі він є високошвидкісним, який транслює весь мережевий трафік на всі вузли даної шини. У сучасних автомобілях шина CAN підключена до порту OBD-II та часто може приймати й передавати весь трафік на зовнішню сторону інтерфейсу.

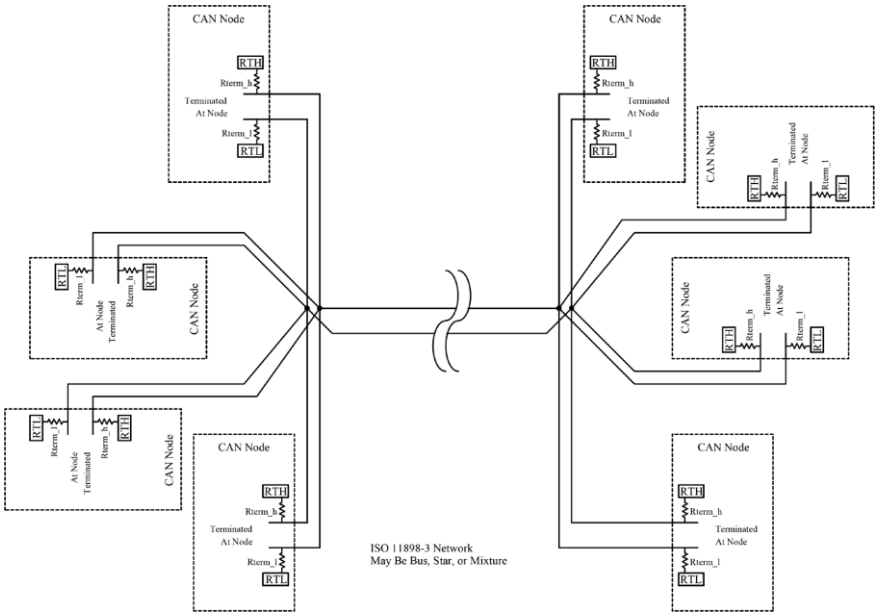

Рисунок 4.6 - Електронний блок управління підключені до CAN-шини

Однак CAN використовується в автомобілі не тільки для передачі діагностичних кодів несправностей. Сучасні транспорті засоби мають сотні датчиків і блоків управління, які контролюють все: від керування автомобілем (рульове управління, гальмування, прискорення) до периферійних функцій,

таких як замки дверей або інформаційно-розважальні системи. Вся інформація, якою обмінюються ці компоненти, передається через шину CAN або аналогічну (часто власну) шину і зазвичай доступна через порт OBD-II.

На відміну від мереж з комутацією пакетів на основі TCP, які присутні в IT-інфраструктурі більшості організацій, протокол CAN надсилає всі дані до всіх вузлів на певній шині. Кожен CAN-кадр містить адресу призначення. Однак, він не містить адреси джерела, тому вузол автентифікації не має можливості дізнатися, чи є джерело легітимним.

Протокол CAN страждає від декількох проблем з безпекою, які не вирішені в більшості сучасних автомобілів. Існують дві причини цих проблем. Перша полягає в тому, що більшість мереж та блоків управління були розроблені, коли доступ до шини вимагав фізичного доступу до автомобіля. Таким чином, безпека не була першочерговим завданням. Друга причина полягає в тому, що швидкість і синхронізація вважаються більш важливими для безпеки і продуктивності транспортного засобу, ніж безпека даних. Небажано, наприклад, чекати зайву мілісекунду на перевірку відправника байта даних, коли ця мілісекунда необхідна для спрацьовування подушки безпеки.

Транспортний засіб із вразливими місцями в системі безпеки створює значне занепокоєння, оскільки досвідчений зловмисник може активно використовувати ці вразливості для власної вигоди. На відміну від традиційних підходів до захисту, які передбачають, що система або її компоненти мають функціонувати в певних межах і реагувати на зовнішні стимули передбачуваним чином, хакери прагнуть порушити логіку та контрольні механізми системи. Їхні дії спрямовані на маніпуляцію елементами системи для досягнення власних цілей, що робить загрозу складнішою та непередбачуваною.

У сучасній архітектурі автомобільних шин така ситуація створює серйозні проблеми з безпекою. Зокрема, пристрої OBD-II, призначені для використання на вторинному ринку, можуть стати слабкою ланкою. Вони здатні приймати довільний CAN-трафік ззовні через свій бездротовий радіоінтерфейс і передавати його без будь-якої перевірки або фільтрації на внутрішню CAN-шину

автомобіля через порт OBD-II. Саме ця вразливість стала ключовим об’єктом уваги в ході початкового дослідження, оскільки демонструє, як легко можна обійти захисні механізми при наявності належного обладнання та навичок.

4.1.3 Роль DTC кодів у діагностиці автомобіля

DTC розшифровується як "Діагностичні коди несправностей", які були створені Товариством автомобільних інженерів. Коди генеруються системою бортової діагностики автомобіля. Кожен символ у п'яти значних кодів DTC означає певну проблему.

Існує два основних стандарти: OBD-II, який використовується в легких і середніх транспортних засобах. Всі вони мають бути відповідними до цього стандарту. Другим є J1939, який використовується у важких транспортних засобах, таких як міські автобуси, сміттєвози та цементовози [18].

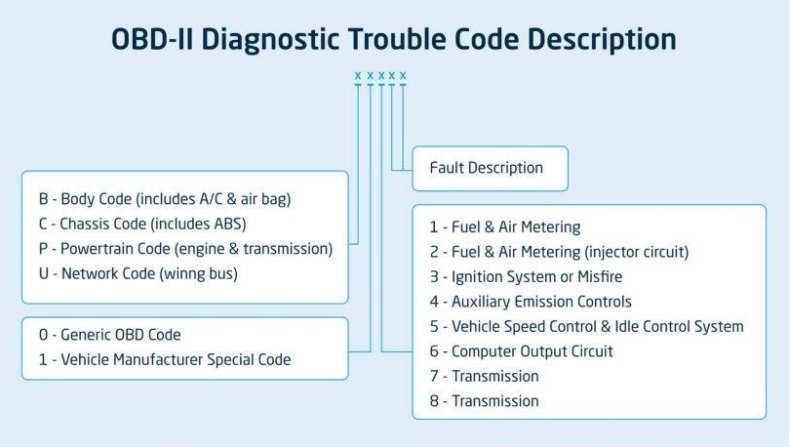

Рисунок 4.7 - Структура розшифрування кодів несправностей OBD-II

Існує 4 типи коду, перший "B": вказує на проблему з відправкою, який включає двигун, трансмісію, силову установку та паливну систему. Код "C" вказує на проблему з ходовою частиною. Це стосується механічних систем поза кабіною, таких як рульового управління, підвіски та гальмування. Код "P" описує проблему з кузовом і стосується деталей, розташованих в салоні. U-код вказує на

проблему з бортовим комп'ютером і функцією інтеграції автомобіля, керованого OBD.

Другий символ DTC - є цифра, "0" або "1": "0" означає стандартний міжнародний код SAE. Він також відомий як загальний код, тобто він застосовується до всіх автомобілів, які відповідають міжнародному стандарту OBD-II. "1" – код, який є специфічним для марки або моделі автомобіля. Він відомий як розширений код, що не підпадає під стандарт SAE.

Третім символом DTC є вісім цифр:

0: Вимірювання палива і повітря та допоміжні засоби контролю викидів;

1: Система впорскування палива та дозування повітря;

2: Дозування палива та повітря;

3: Система запалювання або пропуски запалювання;

4: Допоміжний інструмент управління розрядкою;

5: Управління швидкістю транспортного засобу, система управління холостим ходом та допоміжний вхід;

6: Комп'ютерна вихідна схема ;

7-8: Передача;

Четвертим та п’ятим символами DTC – є два значні числа від 0 до 99, які називаються "індексом конкретної помилки". Визначає точну несправність автомобіля.

Приклад застосування кодів несправностей на основі помилки авто: за допомогою OBD-сканера відображається код DTC P0420 під час підключення до діагностичного порту автомобіля. В цьому випадку буква "P" вказує на проблему з трансмісією або паливною системою автомобіля. Число "0" означає, що це стосується всіх транспортних засобів, сумісних з OBD-II. Число "20" вказує на проблему з каталітичним нейтралізатором автомобіля.

Завдяки проведеному аналізу з кодом P0420 виникла проблема із каталітичним нейтралізатором. Рівень кисню в ньому нижче бажаного порогу, тому в повітря просочується більше забруднювальних речовин – це є проблемою, яку слід вирішити якнайшвидше. Коди OBD-II в основному використовується

для автомобілів малої та середньої вантажності, для важких автомобілів потрібно зчитувати коди J1939.

4.2 Підходи до аналізу безпеки та захисту автомобільних мереж

Сильна мотивація для безпеки в транспортних засобах виникає через зростання складності електронної інфраструктури та доступності комунікаційних інтерфейсів для користувачів на борту транспортних засобів. Це означає, що споживчі пристрої можуть бути з'єднані з бортовими мережами. Стандартні апаратні засоби, такі як Ethernet та Wi-Fi, інтегровані в сучасні транспортні засоби на ряду з USB та Bluetooth. Через те, що ці інтерфейси стандартизовані і доступні кожному, у тому числі хакерам, атаки на транспортні засоби стають все більш вірогідними. На рисунку 4.8 показано частину сучасних бортових мереж в автомобілях та мотоциклах.

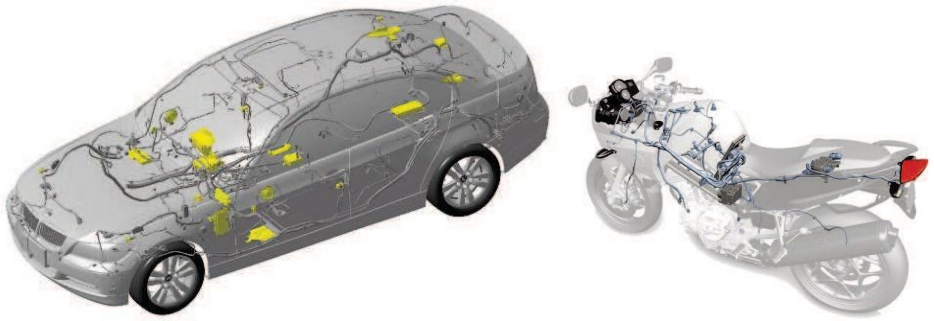

Рисунок 4.8 - Бортові мережі автомобіля та мотоцикла

Зі збільшенням фінансових стимулів зростає і ризик успішних атак.

Вже сьогодні кіберзлочинці активно експлуатують вразливості в системах безключового доступу та мультимедійних системах автомобілів, що створює серйозні ризики для водіїв і виробників. Існують також маніпуляції з бортовою мережею для подолання правових обмежень. Прикладом цього є введення фальшивих сигналів швидкості для того, щоб маніпулювати мультимедійною системою під час руху.

Для досягнення цих цілей дослідники IT-безпеки розробляють рішення, що спираються на різні підходи, які відповідають різним вимогам безпеки та обмеженням спеціального прикладного середовища. Потреба в безпеці класичних комп'ютерних систем еволюціонувала від відкритих мереж і систем із закритими групами користувачів (наприклад, дослідницька мережа ARPAnet) до відкритої групи користувачів із прикладною автентифікацією та іншими рішеннями безпеки.

У сфері безпеки додатків існує кілька відомих підходів до запобігання, виявлення та стримування атак:

- Оптимізовані для безпеки методи програмування;
- Тестування програмного забезпечення;
- Цифрові підписи та інфраструктура відкритих ключів;
- Механізми контролю доступу;
- Політики для вводу/виводу та доступу до файлів;
- Пакетні фільтри;
- Динамічний аналіз інформаційних потоків;
- Підтримка апаратної безпеки;
- Безпечне зберігання ключового матеріалу та виконання алгоритмів.

Більшість згаданих вище рішень не застосовуються самі по собі. За умови правильного застосування в об’єднанні декількох аспектах безпеки вони забезпечують покращений рівень захисту.

4.2.1 Моделі атак на автомобільні мережі

У перших поколіннях багаторівневого зв'язку транспортні засоби використовували інформацію надану RSU. Завдяки чому вони знали про інші транспортні засоби поблизу, маючи змогу завчасно та адекватно попередити водія про небезпеку. Хоча для класичних функцій автомобіля, таких як цифровий одометр і фізичний контроль доступу, зазвичай застосовуються власні рішення безпеки. Між-транспортний зв'язок у свою чергу повинен спиратися на чітко

визначені стандарти, які повинні визнавати і дотримуватися всі виробники та постачальники. Завдяки цьому відкривається нове вікно можливостей для атак, які можуть бути використані навіть віддалено і призвести до серйозних наслідків. Без додаткових заходів безпеки зростає ризик нових загрози, де зловмисники можуть використовувати програми безпеки у своїх цілях, таким чином ставлячи під загрозу безпеку водіїв.

Сучасна вбудована мережева архітектура, яка використовується для обміну даними між датчиками вторгнень і блок ЕБУ з часом розширюється. Не всі промислові виробники ще усвідомили необхідність захисту CAN-шини, оскільки це не залежить від місця користувача або зовнішньої частини автомобіля. Однак експерименти показали, наскільки серйозними можуть бути наслідки таких атаки.

У 2007 році було доведено, що система передачі трафіку TMC може функціонувати через RDS з мінімальними зусиллями. Це продемонструвало, як FM-радіо може бути використане для передачі інформації про трафік, що інтегрується у навігаційні пристрої, надаючи користувачам можливість уникати заторів завдяки інформації про дорожні події у реальному часу та їх маршрутизацію. Ця атака була заснована на зворотній інженерії, де було виявлено відсутність криптографічного захисту. Загалом можна виділити два типи атак: посягання на цілісність транспортного засобу та з метою порушення приватності водія шляхом збору [19].

З впровадженням Wi-Fi у сучасних автомобілях зростає ризик злому автомобільного інтерфейсу. Це обумовлено тим, що бездротові з'єднання відкривають нові вектори атак, які можуть використовуватися зловмисниками задля доступу до внутрішніх систем авто. Для здійснення такого типу атак не завжди потрібні глибокі технічні знання, відсутність належного шифрування, слабкі паролі або вразливості в програмному забезпеченні можуть дозволити зловмисникам перехоплювати трафік, впливати на роботу автомобільних систем або навіть отримувати контроль над деякими функціями, такими як відкриття

дверей або запуск двигуна. У наступному списку показано, які служби та інтерфейси вразливі до атак:

- мобільні пристрої (інтеграція споживчих пристроїв для інформаційно-розважальних цілей);
- діагностика та перепрограмування (доступ до майстерні та обслуговування);
- віддалені послуги (внутрішня частина OEM, доступна через мережеве підключення транспортного засобу);
- додатки та віджети.

Спільним у всіх цих областях є те, що все це має високий рівень взаємодії з бортовою мережею автомобіля. Діагностика та перепрограмування вимагають глибокого доступу до функцій автомобіля, тоді як інформаційно-розважальні пристрої, на перший погляд, можуть здатися тривіальними, але сучасні автомобільні мережеві архітектури ігнорують цей факт.

Польові експлуатаційні випробування спрямовані на оцінку доцільності та ефективності між-транспортного зв'язку (Car2X) у реальних ситуаціях. У рамках таких випробувань певна кількість транспортних засобів, зазвичай від десяти до двохсот одиниць, оснащується бортовими системами зв’язку та використовується на визначеній території, яка обладнана стаціонарними комунікаційними точками RSU. У всіх чинних FOT застосовується криптографічний захист бездротового зв’язку. Наприклад, у проєкті simTD використовується інфраструктура відкритих ключів для забезпечення довгострокової та короткострокової ідентифікації. Вони створюються і керуються через PKI, розроблену консорціумом проєкту, а концепція короткострокових ідентифікаторів використовує підхід прямої анонімної атестації, схожий з Trusted Platform Module. Через обмеженість обчислювальної потужності бортових систем часто спрощуються криптографічні протоколи. Наприклад, у simTD замість еліптичної криптографії, передбаченої для стандартизації та короткострокових сертифікатів використовується RSA-512. Ці проєкти координуються в межах ініціативи Drive C2X, яка проводить

випробування сумісності технологій із метою стандартизації в ETSI. Попри те, що комунікаційні рішення Car2X ще не стали стандартом у сучасних транспортних засобах, їх розробка триває завдяки численним дослідницьким проєктам і польовим випробуванням. Хоча основна увага приділяється бортовому зв’язку, він також важливий для встановлення довіри в системах Car2X. Наразі розглядається підхід на основі сертифікатів із різними рівнями довіри, який гарантує безпеку та конфіденційність зв’язку між-транспортними засобами, а також між автомобілями та інфраструктурою.

У системах Car2X існує два типи повідомлень, які називаються CAM і DENM. Повідомлення маячків називаються повідомленнями про спільне інформування Cooperative Awareness Messages. Ці маячки періодично транслюються і повідомляють про місцезнаходження, швидкість і прискорення автомобіля. Повідомлення CAM-маяків використовуються для уникнення зіткнень та розраховує прогноз траєкторії для навколишнього транспортного засобу , щоб водій міг бути попереджений у разі виникнення потенційного сценарію зіткнення.

Інший тип повідомлень - це так звані розподілені повідомлення про навколишнє середовище (DENM). Вони повідомляють локальну інформацію, таку як попередження про небезпеку, що генерується раптовим маневром гальмування або якщо вже зафіксовано аварію. Ці повідомлення також використовуються для передачі інформації про стан доріг та інфраструктури, а також інформації про стан придорожніх об'єктів, таких як світлофори. У той час як повідомлення CAM завжди споживаються на приймачі, повідомлення DENM можуть передаватися далі іншим транспортним засобам, наприклад, для поширення попереджень транспортним засобам, що знаходяться попереду за напрямком руху, або автомобілям, які рухаються у зустрічному напрямку.

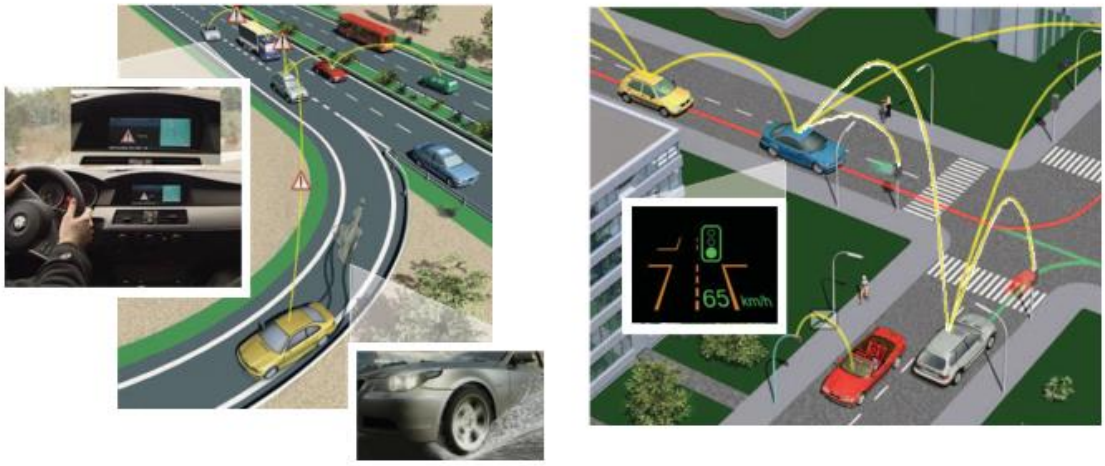

Рисунок 4.9 - Приклади комунікації Car2X

Важливим фактором бездротового зв'язку є належний захист вмісту з використанням ECC, завдяки коротшій довжині ключа та підписів. Певною особливістю Car2X є те, що для підписання даних, які надсилаються, використовуються сертифікати псевдонімів. Це означає, що ідентифікація транспортного засобу не може бути легко розкрита, завдяки чому зберігається конфіденційність водіїв. Кожен транспортний засіб має довгостроковий сертифікат ідентичності. Він використовується для автентифікації у внутрішній ІПК, щоб отримати нові дані, які потім використовуються на дорозі.

4.2.2 Практичне тестування на проникнення в CAN-шину

Цей тип тестування є важливим етапом дослідження вразливостей автомобільних систем. Сучасні транспортні засоби все більше покладаються на електронні блоки управління та мережі передачі даних для забезпечення роботи ключових функцій автомобіля. Однак попри їхню функціональність, з’являються можливості для несанкціонованого доступу до внутрішніх систем транспортного засобу.

Для тестування було застосовано спеціалізоване обладнання, яке дало змогу аналізувати інформацію, яка передається через шину автомобіля та модифікувати її для дослідження можливих вразливостей. Першим етапом

проведення тестування було підключення до CAN-шини автомобіля через порт OBD-II із використанням адаптера ELM327, оснащеного Bluetooth-модулем ZS-040.

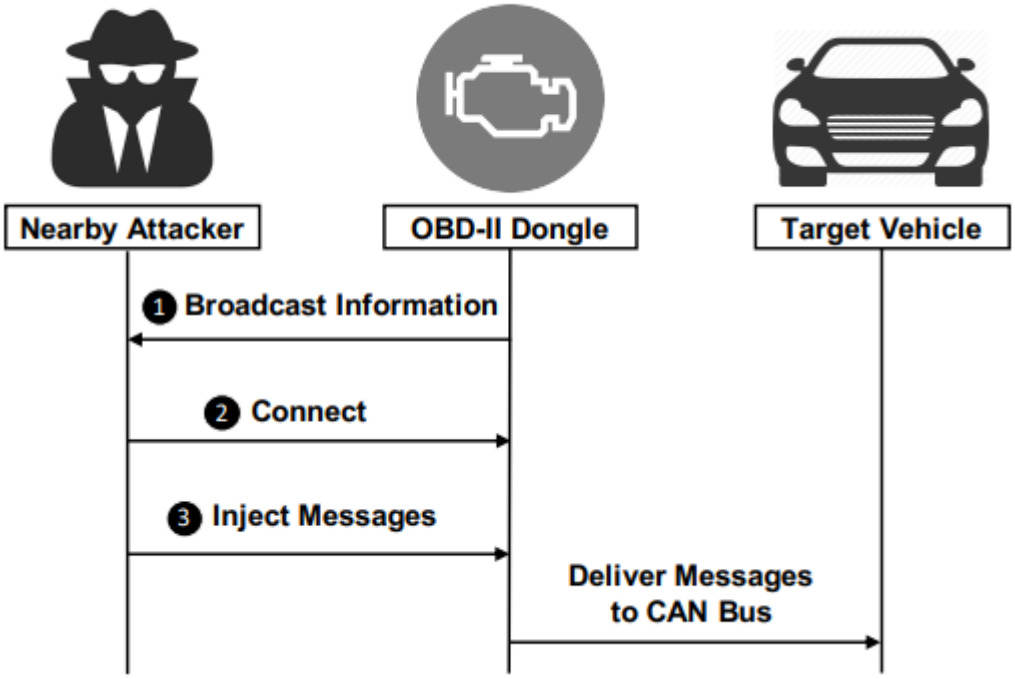

Рисунок – 4.10 - Модель атаки на автомобіль

Майже всі автомобілі, що виробляються сьогодні, зобов'язані за законом мати інтерфейс для підключення діагностичного обладнання. Передача даних через цей модуль відбувається за кількома стандартами. ELM327 призначений для роботи в якості моста між цими портами бортової діагностики (OBD) і стандартним послідовним інтерфейсом.

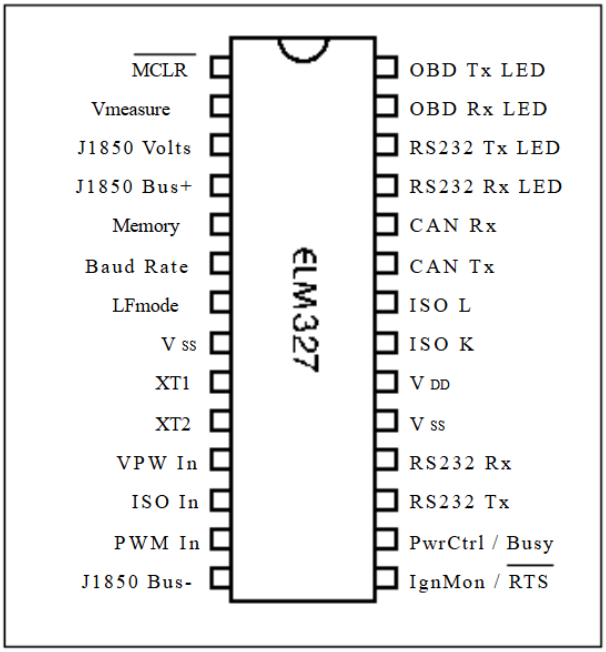

Рисунок 4.11 - Схема з'єднань мікросхеми ELM327

Крім можливості автоматичного виявлення та інтерпретації дев'яти протоколів OBD, ELM327 також забезпечує підтримку високошвидкісного зв'язку, сплячого режиму з низьким енергоспоживанням. Він повністю налаштовується, за потребою будь-яких змін для користувача.

Цей адаптер дозволив передавати дані на програмне забезпечення, встановлене на смартфоні або комп’ютері, що забезпечило можливість взаємодії з електронними системами автомобіля. На рисунку 4.12 представлено індикацію помилки "Check Engine" на панелі приладів автомобіля, яка активується системою у випадку виявлення збоїв у роботі двигуна або його підсистем. Цей індикатор підтверджував, що система успішно сприймає команди, передані через CAN-шину.

Рисунок 4.12 - Поимлка "Check Engine"

Після підключення до контролера двигуна вдалося встановити стійкий зв’язок із електронним блоком управління (ЕБУ). Програмний інтерфейс модуля (рис. 4.13) дозволив зчитувати типи з’єднання між адаптером та CAN-шиною, а також отримувати доступ до параметрів налізу та тестування. На рисунку 4.14 показано стан підключення модуля до CAN-шини.

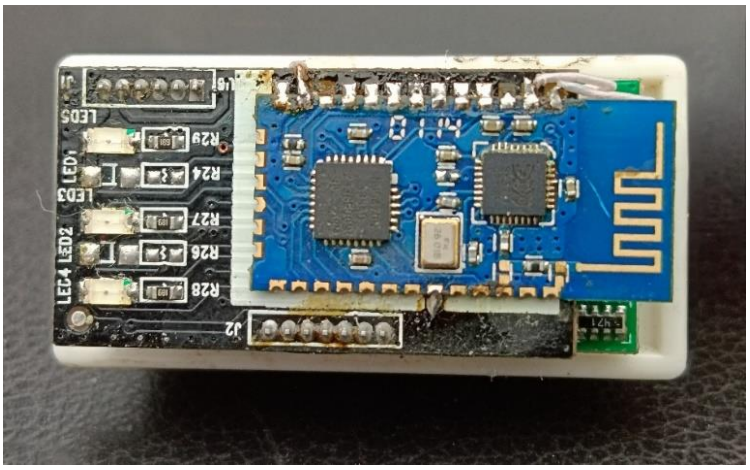

Рисунок 4.13 - Модуль ELM327 із Bluetooth модулем

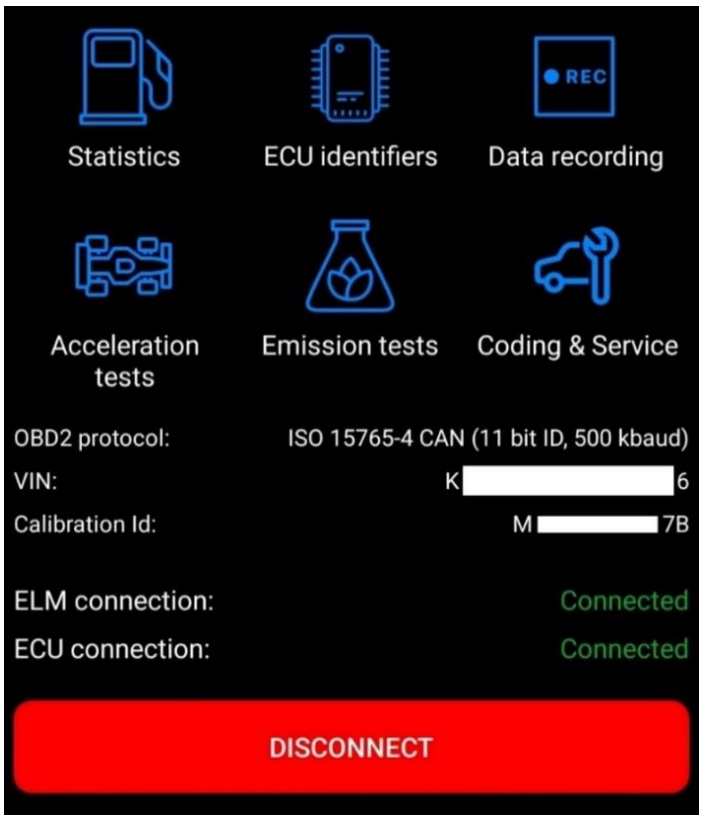

Рисунок 4.14 - Стан підключення модуля до CAN-шини

Функціонал програмного забезпечення продемонстрував можливість зчитування даних, переданих через спідометр автомобіля. У режимі реального часу передавалася інформація про швидкість руху та інші параметри. На рис. 4.15 наведено приклад інтерфейсу програми.

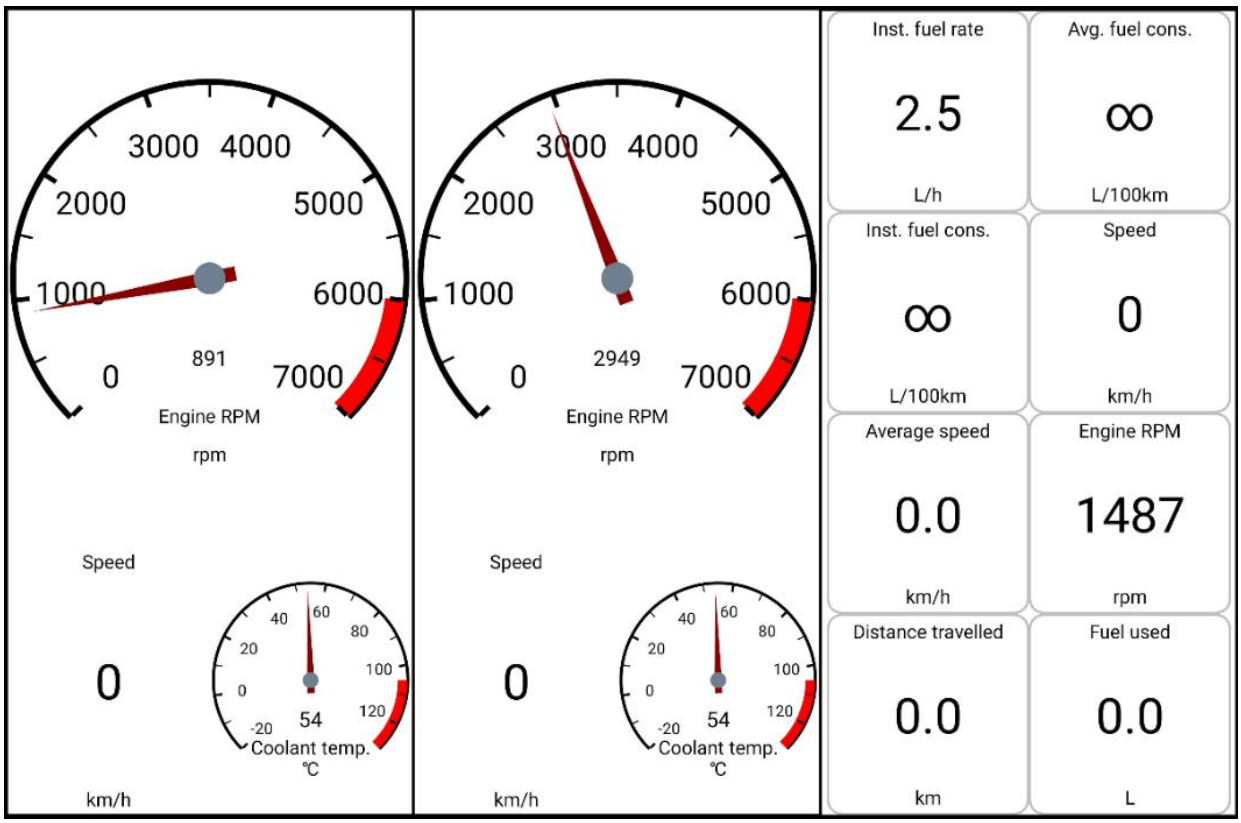

Рисунок 4.15 - Інтерфейс показників в реальному часі

Особливу увагу було приділено меню "Coding Service" (рис. 4.16), яке дозволяло змінювати параметри автомобіля. Зокрема, вдалося виконати зміну скидання адаптації блоку управління двигуном та налаштувати інші параметри. Це продемонструвало потенційну можливість несанкціонованого втручання у функції автомобіля, що потребує посилення безпеки.

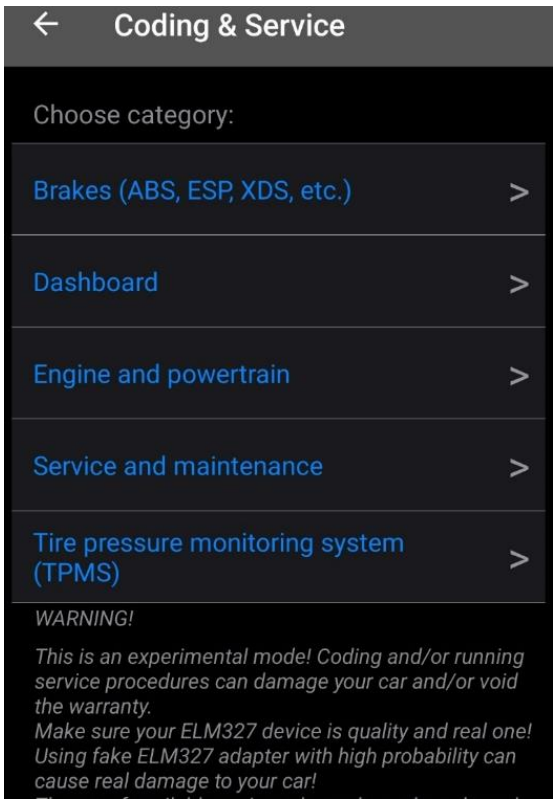

Рисунок 4.16 - Меню "Coding Service" у програмному забезпеченні

У розділі "Engine and Powertrain" здійснювалося зчитування даних про двигун і трансмісію, а також виконувалися операції, пов’язані з обслуговуванням паливної системи. Це дозволяло оцінити технічний стан приводу та його окремих компонентів.

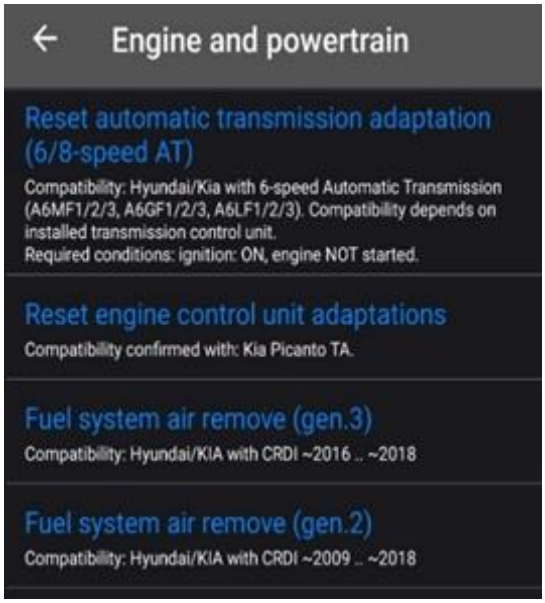

Рисунок 4.17 - Меню "Engine and Powertrain"

Завдяки меню "Diagnostic Trouble Codes" було зчитано діагностичні коди несправностей (DTC), які з’явилися в процесі експлуатації автомобіля. За допомогою цієї функції було проведено тест системи, що дозволив визначити наявні помилки, після чого спроба їх видалення.

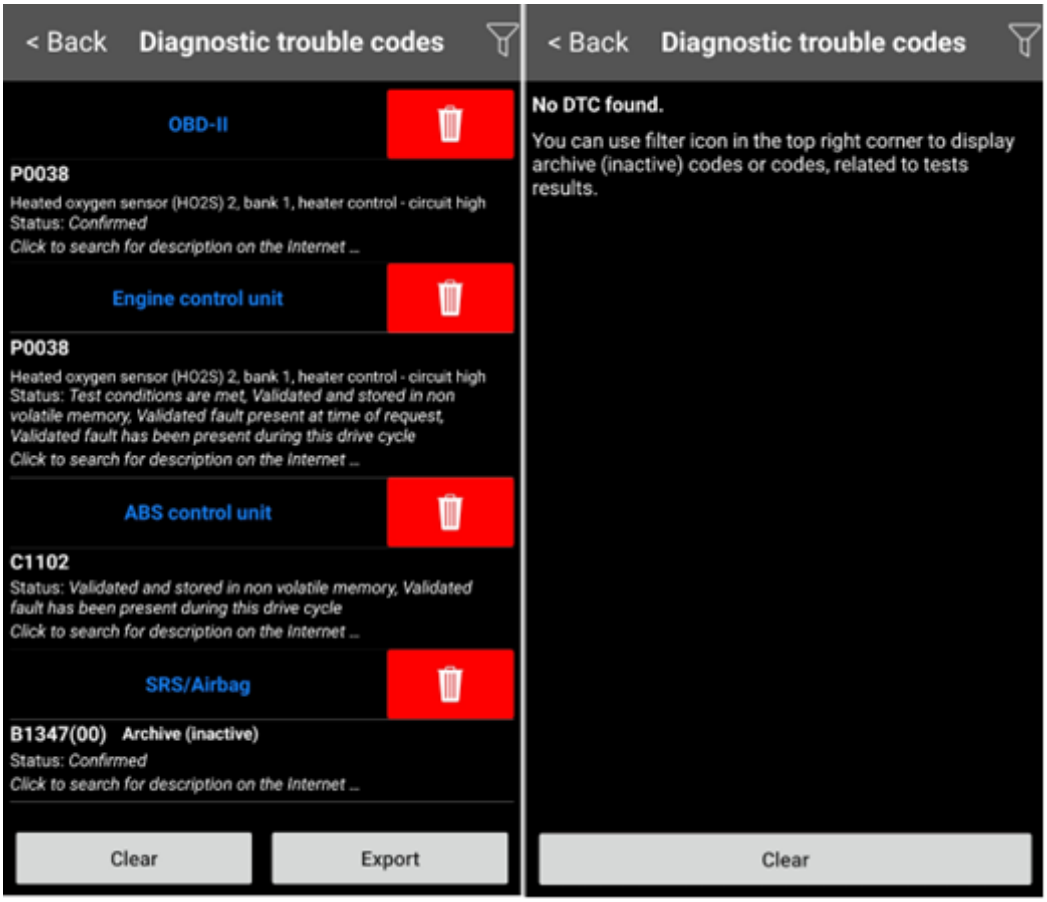

Рисунок 4.18 - Меню "Diagnostic Trouble Codes"

На етапі видалення помилок система видала попередження про можливі наслідки цього процесу, такі як втрата діагностичної інформації, важливої для технічного обслуговування. Після підтвердження видалення інструмент перейшов у стан "без помилок". На рис. 4.19 показаний результат очищення коду несправності. На рисунку 4.20 продемонстровано вже змінені параметри приборної панелі.

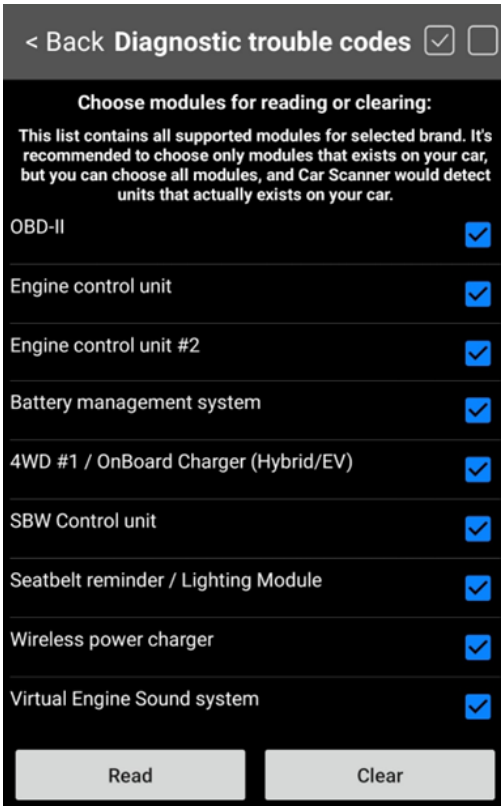

Рисунок 4.19 - Стан автомобіля після видалення помилок у програмному забезпеченні

Рисунок 4.20 - Модифікована панель приладів

Фактичні тести підтвердили вразливість в системі CAN-шини, що виявило можливість несанкціонованого доступу до керування транспортним засобом. У

ньому підкреслюється необхідність впровадження сучасного кіберзахисту для захисту автомобілів від потенційних кібератак.

4.3 Рекомендації щодо підвищення безпеки автомобільних мереж

Вразливість інформаційно-розважальних систем транспортних засобів, що використовують інтернет, є відкритим полем для поглиблених досліджень та оглядів. Безпека V2X-комунікацій не була детально досліджена, завдяки чому розв'язання цієї проблеми є найбільш пріоритетною. Оскільки ця технологія знаходиться в зародковому стані, було б доцільніше, щоб дослідники зосередилися на стратегіях тестування безпеки систем зв'язку транспортних засобів. Тому розробка стандартів авторизації промислової безпеки буде корисною в цьому відношенні.

Безпека і захист - це всебічний процес, який має бути досконально реалізованим, тому розробники систем повинні бути в курсі останніх досягнень в області атак на автомобіль. По-перше, ілюзорна атака або обман за допомогою помилкового сигналу світлофора є відкритим полем для вивчення, щоб забезпечити безперебійне функціонування загального трафіку авто. У свою чергу це дозволить не сповільнювати і головне не обмежувати загальну ефективність руху, особливо на перехрестях і багатосмугових дорогах.

Машинозчитувані дорожні знаки з електронними підписами значно покращили загальну безпеку в контексті дорожнього руху. По-друге, сенсорні детектори несанкціонованого доступу потребують поглибленого вивчення та аналізу. Тобто функціональність та чутливість всіх сенсорів повинні бути перевірені та повідомлені миттєво перед запуском. Розробка пристроїв захисту від несанкціонованого втручання має бути такою, щоб фізичний доступ до пристрою не спричиняв часткового або повного доступу до мережі. Крім того, оцінка безпеки під час заряджання є ще однією сферою для подальших досліджень, враховуючи аспекти захисту електромережі, захисту зарядних станцій та безпеки зв'язку.

4.4 Висновки до розділу 4

Оцінка ризиків і вдосконалення систем кібербезпеки транспортних засобів є складним процесом, який охоплює багато аспектів. Все це має бути врахованим технічними спеціалістами для організаційних комплексів. Оскільки підключені автомобілі перетворюються на глобальні інформаційні мережі, виникають нові виклики безпеці, які вимагають співпраці між автовиробниками, дослідниками безпеки, IT-фахівцями та регуляторами.

Вразливість автомобільних систем, зокрема через інтерфейс OBD-II і шину CAN, підкреслює, що, незважаючи на технологічну складність сучасних транспортних засобів, існує кілька шляхів для несанкціонованого доступу до внутрішніх систем автомобіля. Це вказує на те, що для виявлення та усунення вразливостей необхідно регулярно тестувати та вдосконалювати діагностичні системи. Технічний підхід до безпеки транспортних засобів повинен не тільки забезпечувати захист від відомих загроз, а й адаптуватися до нових ризиків, особливо за рахунок постійного розвитку технологій підключення до інтернету та інших мереж.

Вивчення ризиків, пов'язаних з пристроями на вторинному ринку, зосереджено на необхідності введення суворих стандартів контролю якості та безпеки для таких пристроїв, як адаптери OBD-II та інші додаткові пристрої, підключені до автомобільних систем. У свою чергу недбалий контроль над цими пристроями такого рівня, у кілька разів підвищує вразливість критичних аспектів автомобіля до кібератак, саме ці критерії можуть стати відправною точкою для зловмисників. Оскільки на ринку з’являється все більше таких пристроїв, виробники та розробники в першу чергу повинні впроваджувати більш просунуті заходи безпеки, для зменшення ризиків злому.

Найновіші технології безпеки, які використовують автовиробники, мають включати захищенні обчислювальні бази даних та мережі і використовувати ізоляцію програм у віртуальних середовищах. Все це зменшує можливості для успішного злому критично важливих сегментів автомобіля. Ще одним, не менш

важливим кроком є постійне оновлення та вдосконалення систем захисту до доступу до даних, ці компоненти гарантують їх цілісність та конфіденційність.

Основним критичним аспектом є фізичний доступ до автомобіля та його частин. Різні гаджети і частини транспортного засобу вимагають додаткового ступеня захисту. Пам'ять і схеми, які захищають від несанкціонованого доступу до основних складових, які можуть бути стерті, якщо пристрій втручається за допомогою світлочутливих запобіжників. Важливість безпеки транспортних засобів зростатиме з інтеграцією систем V2V/V2I. Атаки на такого типу пристрої можуть порушити роботу транспортних засобів, але також призвести до катастрофічних наслідків на рівні транспортної інфраструктури, оскільки вимагають від виробників максимальної уваги до можливих загроз. Розвиток та інтеграція новітніх технологій у сфері автомобільного транспорту залежить від досягнення високого рівня безпеки.

ВИСНОВКИ

Важливим аспектом розвитку сучасного світу є кібербезпека у сфері IoT пристроїв. З впровадженням цих всеосяжних технологій для покращення рівня життя та комфорту людини, прямо пропорційно зростає ризик атак на ці пристрої. Зокрема, основними проблемами є дистанційного злому, викрадання даних і DoS-атак, що призводить до відмови в обслуговуванні. Тому потреба у розробці стратегій боротьби з цими загрозами стає дедалі гострішою. Хоча поточні підходи включають системи виявлення вторгнень IDS, шифрування, регулярні оновлення програмного забезпечення та надійні протоколи автентифікації, однією з головних проблем є відсутність стандартизації в галузі, обмежені ресурси та складність реалізації механізмів безпеки в багатокомпонентних системах. Вирішення цих інцидентів залежить від зацікавлених сторін. Процес повинен включати виробників, експертів у справах кібербезпеки, законодавців та інших фахівців. А також побудови єдиного Центру обміну та Аналізу інформації. Де він буде ініціювати загальну модель для обміну інформацією про відомі загрози та кращі практики між учасниками ринку.

Майбутнє автономних транспортних засобів залежить від інноваційних технологій, які забезпечують адаптивність систем та стійкість до нових викликів. Штучний інтелект та машинне навчання входить у ключову складову частину цієї еволюції. Зазвичай це веде до створення інформаційних систем, які можуть не лише виявляти кіберзагрози в режимі реального часу, але і передбачити можливі сценарії цих атак зі зміною динамікою. Наприклад, за допомогою ШІ потрібно в рази менше часу для аналізу великих обсягів даних від датчиків автомобіля та інфраструктури, щоб виявити будь-які аномалії. З іншого боку, використання блокчейн-технологій також слугує додатковим захистом несанкціонованих змін.

Законодавчі та політичні зміни мають вирішальне значення для створення безпечного робочого середовища. Ефективна правова база повинна включати стандарти безпеки, які враховують технологічний прогрес і мінливий контекст

кіберзагроз. Наприклад, прийняття міжнародних стандартів, таких як ISO/SAE 21434, надає автомобільній промисловості єдиний підхід до безпеки, що дозволяє уникнути потреби в різних підходах різних виробників. Крім того, спільні дослідницькі ініціативи академічних та державних установ, приватних компаній сприяють розробці передових рішень, які можна швидко впровадити в реальних умовах. Прогресивна політика має також зосереджуватися на захисті прав споживачів, створюючи механізми, які гарантують конфіденційність і безпеку їхніх даних. Поєднання технологічних інновацій, галузевої співпраці та ефективного регулювання створить умови для впровадження безпечних автономних транспортних засобів, забезпечуючи майбутню довіру суспільства для нових технологій.

СПИСОК ВИКОРСИТАНИХ ДЖЕРЕЛ

1. Information Security and Risk Management, Worldwide, 2022-2028 [Електронний ресурс]:[Веб-сайт]. – Електронні дані. – Режим доступу: https://www.gartner.com/en/documents/5315863

2. Unveiling Cyber History 1962: Allan Scherr, The First Computer Troll [Електронний ресурс]:[Веб-сайт]. – Електронні дані. – Режим доступу: https://www.chaintech.network/blog/unveiling-cyber-history-1962-allan-scherr-the-first-computer-troll/

3. Advance-fee scam [Електронний ресурс]:[Веб-сайт]. – Електронні дані. – Режим доступу: https://en.wikipedia.org/wiki/Advance-fee_scam

4. The Heartland Breach: A Cautionary Tale for E-Commerce [Електронний ресурс]:[Веб-сайт]. – Електронні дані. – Режим доступу: https://blog.comodo.com/e-commerce/the-heartland-breach-a-cautionary-tale-for-e-commerce/

5. The Attack on Colonial Pipeline [Електронний ресурс]:[Веб-сайт]. – Електронні дані. – Режим доступу: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

6. What is the CIA Triad [Електронний ресурс]:[Веб-сайт]. – Електронні дані. – Режим доступу: https://www.coursera.org/articles/cia-triad

7. What is IoT Technology and Its Applications? [Електронний ресурс]:[Веб-сайт]. – Електронні дані. – Режим доступу: https://blp.ieee.org/what-is-iot-technology-and-its-applications/

8. Standards organization [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://en.wikipedia.org/wiki/Standards_organization

9. All you need to know about ETSI EN 303 645[Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://www.zariot.com/overview-etsi-en-303645/

10. ETSI. Cyber Security for Consumer Internet of Things: Baseline Requirements / ETSI EN 303 645 V2.1.1 [Електронний ресурс] / – Режим доступу до ресурсу: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

11. ISO/SAE. Road vehicles — Cybersecurity engineering /ISO/SAE 21434 — 2021-08 [Електронний ресурс] / – Режим доступу до ресурсу: https://www.iso.org/ru/standard/70918.html

12. ISO 26262 [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://en.wikipedia.org/wiki/ISO_26262

13. OWASP IoT Security Testing Guide [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://owasp.org/www-project-iot-security-testing-guide/

14. Knight, A. Hacking Connected Cars: Tactics, Techniques, and Procedures — 2020

15. Liyanage, M., Braeken, A., Kumar, P., Ylianttila, M. IoT Security — 2020

16. Beckmann, C., & Rukzio, E. Automotive User Interfaces: Creating Interactive Experiences in the Car — 2016

17. Unlocking On-Board diagnostics: A Guide to OBD 2 Protocol [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://www.embien.com/automotive-insights/on-board-diagnostics-a-comprehensive-guide-to-obd-2-protocol

18. Pelletier, P. Automotive Diagnostic Systems: Understanding OBD-I & OBD-II Revised — 2017

19. Injecting RDS-TMC Traffic Information Signals [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://docslib.org/doc/11106835/injecting-rds-tmc-traffic-information-signals

20. Oka, D. K., Nadahalli, S., Yost, J., Bojanki, R. P., & Weimerskirch, A. Building Secure Automotive IoT Applications: Developing robust IoT solutions for next-gen automotive software — 2021