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 004.056

До захисту допущено:
ВО завідувача кафедри
_____ Галина СОЗОННИК
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

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

зі спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Дослідження механізмів і стандартів кібербезпеки підключеного автомобіля як IoT»

Виконав (-ла):
студент (-ка) 2 курсу, групи ТС-21мп
Сидор Михайло Степанович _____

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

Рецензент:
Старший викладач СК №5 ІСЗЗІ
Мітін Сергій Вячеславович _____

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

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 «Телекомунікації та радіотехніка»

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

ЗАТВЕРДЖУЮ

ВО завідувача кафедри

_____ Галина СОЗОННИК

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Сидор Михайло Степанович

1. Тема дисертації «**Дослідження механізмів і стандартів кібербезпеки підключеного автомобіля як IoT**», науковий керівник дисертації д.т.н., професор Горицький Віктор Михайлович, затверджені наказом по університету від «31» 10 2023 р. № 5075-С

2. Термін подання студентом дисертації : 21.12.2023

3. Об’єкт дослідження: підключений автомобіль в системі IoT

4. Вихідні дані :

5. Перелік завдань, які потрібно розробити : Дослідити значення терміну «підключений автомобіль» ; функції підключеного автомобіля; технології які використовуються у підключеному автомобілі; кіберзагрози щодо підключеного автомобіля та методи боротьби з ними; методи сертифікації підключеного автомобіля

6. Орієнтовний перелік графічного (ілюстративного) матеріалу:

7. Дата видачі завдання : 21.10.2022

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
	Визначення підключеного автомобіля	01.09.2023-15.09.2023	
	Функції підключеного автомобіля	16.09.2023-30.09.2023	
	Проблеми та загрози підключених автомобілів	01.10.2023-16.10.2023	
	Механізми вирішення проблем кібербезпеки підключеного автомобіля	17.10.2023-31.10.2023	
	Роль 5G у підключеному автомобілі	01.11.2023-14.11.2023	
	Міжнародні та галузеві стандарти кібербезпеки підключеного автомобіля	15.11.2023-24.11.2023	
	Проблеми сертифікації кібербезпеки підключеного автомобіля	25.11.2023-30.11.2023	
	Робота над оформленням магістерської роботи	01.12.2023-04.12.2023	

Студент Михайло СИДОР

Науковий керівник Віктор ГОРИЦЬКИЙ

РЕФЕРАТ

Темою магістерської дисертації є дослідження механізмів і стандартів кібербезпеки підключеного автомобіля як IoT.

Робота містить 108 сторінок, зокрема 20 ілюстрацій, та 14 джерел інформації.

Тема магістерської дисертації є актуальною, так як через зростаючу кількість підключених автомобіль в інфраструктурі IoT потребує розробки стнадртів кібербезпеки для розробки механізмів їх стандартизації, для забезпечення безпеки користувача та його данних.

Мета дисертації полягає у дослідженні наявих та майбутніх загроз для підключеного автомобіля, та знаходження механізмів сертифікації кібербезпеки для автомобілів що взаємодіють з IoT.

Об’єктом дослідження є підключений автомобіль.

Предметом дослідження є наявні протоколи сертифікації підключеного автомобіля.

У дисертації було досліджено поняття «підключений автомобіль», що він з себе представляє, які технології використовує, його взаємодія з IoT, загрози які представляють з себе кібератаки на підключений автомобіль, методи захисту від них і механізми сертифікації підключеного автомобіля.

Ключові слова: інтернет речей, підключений автомобіль, автопілот, сертифікація, кіберзахист.

ABSTRACT

The topic of the master's thesis is the study of the mechanisms and standards of cyber security of the connected car as IoT.

The work contains 108 pages, including 20 illustrations, 14 sources of information.

The topic of the master's thesis is relevant, because in connection with the growth of the number of connected cars in the IoT infrastructure, it is necessary to develop cyber security standards to develop mechanisms for their standardization, to ensure the safety of the user and his data.

The purpose of the dissertation is to investigate current and future threats to the connected car, as well as search for cybersecurity certification mechanisms for IoT-enabled cars.

The object of research is a connected car.

The subject of the study is the existing certification protocols of the connected car.

The thesis examines the concept of "connected car", what it is, what technologies it uses, its interaction with IoT, threats posed by cyberattacks on a connected car, methods of protection against them and mechanisms of certification of a connected car

Keywords: Internet of Things, connected car, autopilot, certification, cyber protection.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП 9
1 ВИЗНАЧЕННЯ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ 10
1.1 Історія появи автомобіля 11
1.2 Зв'язок та обмін даними 13
1.3 Системи навігації 17
1.4 Автопілот 19
1.5 Системи безпеки 22
1.6 Віддалене керування та моніторинг 23
1.7 Оновлення програмного забезепечення 26
1.8 Екосистема для розваг та комфорту 26
1.9 Висновки до розділу 1 32
2 ФУНКЦІЇ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ 33
2.1 Категорії на які поділяються функції автомобіля 33
2.2 Висновки до розділу 2 36
3 АНАЛІЗ ІСНУЮЧИХ ЗАГРОЗ, СУТНІСТЬ ТА ПОНЯТТЯ КІБЕРБЕЗПЕКИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ 38
3.1 Сучасна ситуація в області кіберпідключеного автомобіля 38
3.1.2 Система ADAS 38
3.2 Види підключень 43
3.3 Висновки до розділу 3 53
4 ПРОБЛЕМИ ТА ЗАГРОЗИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ 55
4.1 Система DREAD 55
4.2 Оцінка загрози щодо бекенд-серверів, які обслуговують автомобілі під час руху 57
4.3 Загрози щодо каналів зв'язку автомобілів 57
4.4 Загрози для процедури оновлення прошивок під'єднаних автомобілів 59

4.5 Загрози, пов'язані з людським фактором 59
4.6 Висновки до розділу 4 61
5 МЕХАНІЗМИ ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ ПІДЛЮЧЕНОГО АВТОМОБІЛЯ 63
5.1 Шифрування трафіку 63
5.2 Безпека мережі 64
5.3 Оновлення програмного забезпечення 65
5.4 Ідентифікація та аутентифікація 67
5.5 Фізична безпека 68
5.6 Моніторинг та виявлення вторгнень 69
5.7 Безпека вбудованого програмного забезпечення 71
5.8 Висновки до розділу 5 72
6 РОЛЬ 5G У ПІДКЛЮЧЕНОМУ АВТОМОБІЛІ 74
6.1 Використання 5G у підключеному автомобілі 74
6.2 Висновки до розділу 6 75
7 МІЖНАРОДНІ ТА ГАЛУЗЕВІ СТАНДАРТИ КІБЕРБЕЗПЕКИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ 77
7.1 Впровадження CSMS 81
7.2 Диференціація від TISAX 84
7.3 Вимоги до автовиробників 87
7.4 Висновки до розділу 7 88
8 ПРОБЛЕМИ СЕРТИФІКАЦІЇ ПІДЛЮЧЕНОГО АВТОМОБІЛЯ 90
8.1 Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки 92
8.2 Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки 94
8.3 Схема сертифікації кібербезпеки підключеного автомобіля 102
8.4 Висновки до розділу 8 105
ВИСНОВКИ 106
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 107

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

IoT - Internet of Things

5G - п'яте покоління мобільних мереж

Автопілот - система що автоматично керується комп’ютером

ADAS - Advanced Driver Assistance System

DREAD - Damage, Reproducibility, Exploitability, Affected Users, Discoverability

V2X - Vehicle to X(thomething)

TISAX - Trusted Information Security Assessment Exchange

CEPT - Європейська конференція поштових та телекомунікаційних адміністрацій

CSMS - Charging Station Management System

ВСТУП

У сучасному світі, де технології активно інтегруються в різні сфери нашого життя, поняття "підключений автомобіль" стає все більш актуальним та значущим. Підключені автомобілі, що базуються на Інтернеті речей (IoT), пропонують широкий спектр інноваційних можливостей, від підвищення безпеки та комфорту водія до автоматизованих систем управління транспортним рухом. Однак разом із цими перевагами приходять нові виклики, зокрема, у сфері кібербезпеки.

Магістерська робота присвячена дослідженню механізмів і стандартів кібербезпеки підключених автомобілів як складової систем Інтернету речей. Зростання кількості підключених автотранспортних засобів вимагає глибокого розуміння викликів та потреб у забезпеченні кібербезпеки для забезпечення безпечності в епоху глобального цифрового зв'язку.

Основні аспекти, які вивчатимуться в роботі, охоплюють аналіз технічних засобів захисту, стандартів безпеки та принципів проектування, які застосовуються до підключених автомобілів. Також буде вивчено та проаналізовано основні вектори атак та загрози, що стикаються з підключеними автомобілями, і розглянуті методи захисту від них.

Мета даної магістерської роботи полягає в розкритті сучасного стану кібербезпеки в підключених автомобілях, визначенні ключових аспектів та вирішенні актуальних завдань у цій області. Враховуючи динаміку розвитку технологій, робота також ставить за мету визначити перспективи розвитку та найбільш перспективні напрямки у сфері кібербезпеки для підключених автомобілів.

1 ВИЗНАЧЕННЯ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

Для початку перед тим я розбирати тему курсової роботи, а саме системи оцінки відповідності, або ж сертифікація, кібербезпеки підключенгого автомобіля, потрібно зрозуміти, що саме представляє з себе підключений автомобіль.

Термін "підключений автомобіль" відноситься до транспортних засобів, які обладнані різноманітними технологіями для забезпечення зв'язку, обміну даними та автоматизації різних аспектів автомобільного виробництва та використання.

Підключені автомобілі можуть мати вбудовані системи, такі як GPS, Bluetooth, Wi-Fi, LTE або інші технології для обміну даними з іншими автомобілями, інфраструктурою доріг, а також зовнішніми сервісами і системами управління. Це дозволяє автомобілям взаємодіяти один з одним, отримувати оновлення програмного забезпечення від виробників, надсилати та отримувати дані про дорожні умови, здійснювати віддалене відстеження та керування через мобільні додатки тощо.

Підключені автомобілі можуть також використовувати технології автономного водіння та інші інновації для покращення безпеки та зручності для водіїв і пасажирів.

Також підключений автомобіль є автомобілем який може двосторонньо спілкуватися з іншими системами за межами самого автомобіля (LAN). Це дозволяє транспортному засобу спільно користуватися доступом до Інтернету, а отже і до даних, з іншими пристроями як всередині, так і зовні автомобіля. Що до програм, які мають безпосередньо найважливіше значення для безпеки транспортного засобу та людей які знаходяться в ньому, передбачається, що автомобілі також підключатимуться за допомогою виділеного зв'язку короткого радіусу дії (DSRC) радіостанції, що працюють в діапазоні 5,9 ГГц, що надається FCC, з дуже низьким рівнем латентності.

1.1 Історія появи автомобіля

Якщо поглибитись в історію, то можна дізнатися що перший підключений автомобіль з'явився ще у 1996 році. Це був автомобіль Cadillac DeVille, випущений компанією General Motors використовуючи підключені функції від своєї дочірньої компанії OnStar. Основною метою була безпека та надання екстреної допомоги транспортному засобу при аварії. Чим швидше прийде медична допомога, тим більше шансів вижити водіям та пасажирам. Дзвінок стільникового телефону буде переадресований на коллцентр куди агент надіслав допомогу. Спочатку OnStar працював лише з голосом, але коли стільникові системи додавали дані, система могла відправити GPS розташування до кол-центру. Після успіху OnStar багато автовиробників послідували за подібними програмами безпеки, які зазвичай мають безкоштовну пробну версію для нового автомобіля, а потім платну підписку після закінчення випробування.

У 2001 році введено дистанційну діагностику. У 2003 році були представлені звіти про стан транспортних засобів, покрокові вказівки та пристрій доступу до мережі. У 2007 році Continental представила телематику лише для даних. Влітку 2014 року Audi A3 був першим автовиробником, який запропонував доступ до точок доступу до Wi-Fi 4G LTE, а перше масове розгортання 4G LTE здійснила General Motors.[1]

Підключений автомобіль– наявність пристроїв в автомобілі, які з’єднують пристрої з іншими пристроями в автомобілі/транспорті та/або пристроями, мережами та службами за межами автомобіля, включаючи інші автомобілі, будинок, офіс або інфраструктуру. Доступ до Інтернету зазвичай підключений до локальної мережі. Багато експертів стверджують, що підключені автомобілі є частиною гігантського Інтернету речей.

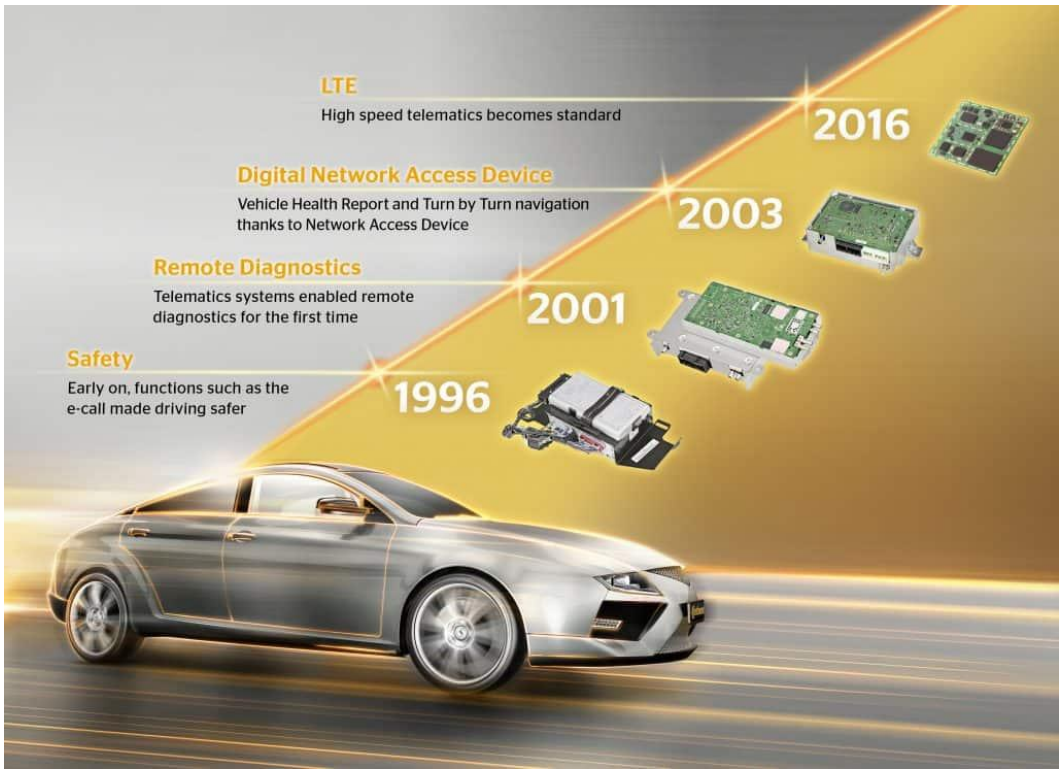


Рисунок 1.1 - Розвиток систем OneStar [1]

Рисунок.1.2 - BMW Connected NA

Інтернет-з’єднання можуть надавати з’єднання, які попереджають про трафік, зіткнення та інші попередження про безпеку. Служби консьєржа від додатків або автовиробників сповіщають водія про час виїхати, щоб прибути вчасно за допомогою календаря і надсилають текстові повідомлення друзям або діловим партнерам, щоб попередити їх про час прибуття. Наприклад, BMW Connected NA.

1.2 Зв'язок та обмін даними

Підключені автомобілі впроваджують різноманітні технології для поліпшення досвіду водіння, забезпечення безпеки та оптимізації управління транспортними потоками. Ось деякі основні аспекти підключених автомобілів:

1. Зв'язок та обмін даними: Автомобілі можуть бути підключені до мережі через вбудовані модулі LTE, 5G або інші технології, що дозволяють обмінюватися даними між автомобілями, інфраструктурою доріг і хмаровими сервісами. Це може включати інформацію про трафік, погоду, безпеку та інші корисні дані.

Єдиних стандартів для подібного способу обміну даними, відомого як V2X (Vehicle-to-Everything) або система обміну даними між автомобілями та іншими учасниками дорожнього руху, ще не прийнято. Натомість, у перспективі підтримка зв’язку між транспортними засобами регулюватиметься різними стандартами – кожна країна та автовиробник впроваджуватимуть свої власні. «Якщо говорити про систему V2X, то тут Bosch використовує багатоканальний/багаторівневий підхід. Ми розробили універсальний блок зв'язку, який може працювати з усіма типами передачі даних», – каже Дірк Хоайзель, член правління компанії Robert Bosch GmbH. Суть у тому, що Bosch об'єднує блок підключення і телематичний пристрій, які індивідуально здатні працювати лише з однією технологією передачі, таким чином створюючи єдиний центральний блок зв'язку. Автомобілі зможуть використовувати доступну в містах мережу Wi-Fi, або користуватися мобільним

інтернетом, якщо перша відсутня. Управляти цими різноманітними комунікаційними параметрами нескладно завдяки програмним рішенням від резидента Кремнієвої долини – компанії Veniam. Їхня технологія стежить за станом мережі і може автоматично перемикатися з однієї на іншу в конкретних ситуаціях. Таким чином, програмне забезпечення гарантує безперервне підключення до мережі: автомобілі, наприклад, зможуть, попереджати один одного про можливі небезпеки і запобігати їм, у той час як водій буде слухати свою улюблену музику.

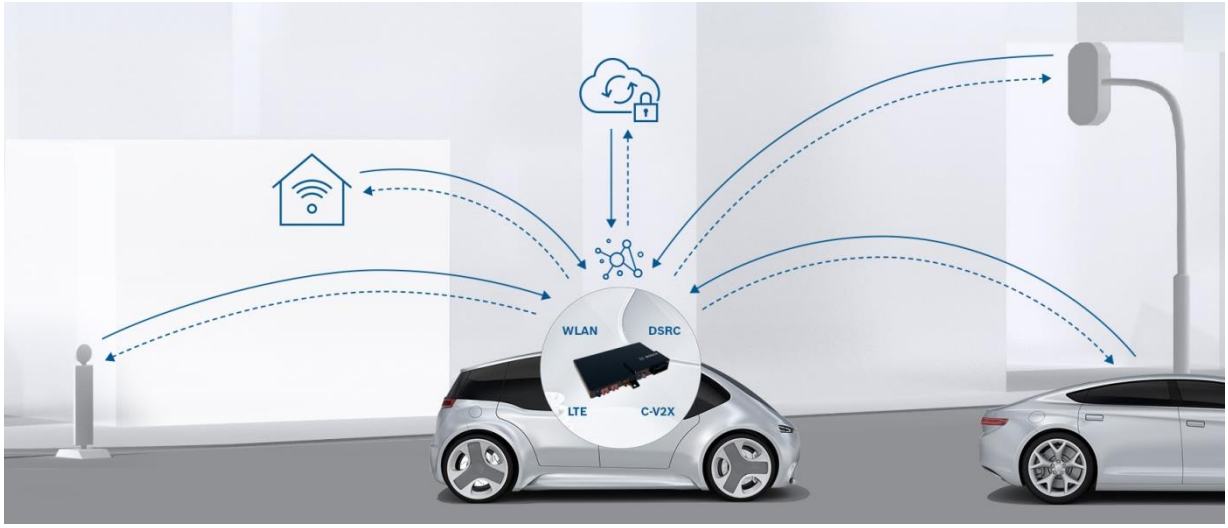


Рисунок 1.3 - Приклад роботи V2X

Bosch розробляє блок управління для всіх типів передачі даних. Очікується, що до 2025 року кількість підключених до однієї мережі транспортних засобів на дорогах Європи, США та Китаю перевищить 470 мільйонів (джерело: PwC). Спочатку більшість автомобілів будуть підключатися безпосередньо до хмари; але, завдяки V2X, в майбутньому все більше автомобілів зможуть безпосередньо контактувати один з одним, а також з об’єктами дорожньої інфраструктури: світлофорами, дорожньо-будівельними майданчиками, пішохідними переходами, будівлями тощо. Потім вони зможуть попереджати одне одного про потенційні небезпеки на дорогах, наприклад, про затори, аварії або ожеледь. Виходячи з отриманих даних транспортні засоби будуть регулювати швидкість руху, що забезпечить більш плавний трафік, особливо в містах. Однак зараз єдиних стандартів

регулювання V2X зв'язку не існує. У той час як Китай використовує технологію мобільного V2X-зв’язку (C-V2X), що базується на мобільних системах зв’язку, Європа і США планують впровадити стандарти передачі даних на основі Wi-Fi (DSRC – бездротової мережі малого радіусу дії та технології інтелектуальних транспортних систем ITS-G5) спільно з C-V2X. Така плутанина і використання різних стандартів зв'язку може призвести до проблем взаємодії між транспортними засобами. На цей випадок у Bosch також є рішення – універсальний блок підключення до мережі. Обладнані ним транспортні засоби зможуть перебувати в загальній мережі незалежно від країни використання. «Завдяки тому, що ми об'єднали дві технології в одну, все більше водіїв по всьому світу зможуть користуватися V2X і кермувати автомобілем безпечно та зручно», – каже Дірк Хоайзель.

Рисунок 1.4 - Модуль зв’язку від BOSCH

Програмне забезпечення Veniam забезпечить надійне підключення

Програмне забезпечення від Veniam підсилює якість з'єднання модуля зв'язку від Bosch. Крім того, програмне забезпечення відстежує витрати і швидкість передачі даних для кожного варіанту підключення. Наприклад,

якщо потрібно терміново сповістити водія про те, що перед ним із провулку виїжджає автомобіль, кожна мілісекунда має значення. Така критична інформація повинна передаватися автомобілеві в режимі реального часу за допомогою високонадійних технологій, завжди готових до використання, навіть якщо затрати на передачу таких даних більші. У той же час, оновлення програмного забезпечення з хмари чи оновлення карти навігаційної системи в такій ситуації можуть бути призупинені, допоки не стане доступною мережа Wi-Fi. Однак точки доступу до Wi-Fi в громадських місцях або будинках працюють не завжди. Програмне забезпечення Veniam враховує плюси і мінуси кожного з типів зв'язку і завжди встановлює оптимальне з’єднання. «Унікальна комбінація інтелектуального програмного забезпечення Veniam і мережевого блоку Bosch значно розширює можливості обробки даних автомобіля, прокладаючи шлях для розвитку хмарних сервісів і безпечного пересування», – каже Жоао Баррос, засновник і головний виконавчий директор Veniam. За спільно розроблене рішення Bosch і Veniam були номіновані на премію в категорії «Штучний інтелект автомобілів і технології безпілотного водіння» на найбільшій у світі виставці електроніки CES 2019 у Лас-Вегасі.

Тести Bosch V2X-зв’язку в Європі, США і Китаї

У найбільшому європейському тестуванні в цій галузі («Безпечне водіння із застосуванням інтелектуальних технологій – перевірено в Німеччині» або simTD) зв'язок V2X довів свою придатність для використання як в лабораторних симуляціях, так і у повсякденних умовах. Bosch зіграв значну роль в цьому проекті. З лютого 2017 року Bosch, Vodafone та Huawei проводять випробування V2X з першими тестовими модулями 5G – і є першими, хто проводить такі тести в Європі. Автострада A9 в Баварії на північ від Мюнхена – локація для тестів систем попередження при зміні смуги на автостраді, а також при раптовому гальмуванні автомобіля, що рухається попереду. V2X також зможе покращити системи допомоги водієві, наприклад, адаптивний круїз-контроль (ACC). Влітку 2018

року в Детройті (США) Bosch тестувала, як транспортні засоби контактують з інфраструктурою дорожнього руху, камерами та датчиками. У тесті була продемонстрована технологія DSRC на основі Wi-Fi, де на обладнані системою транспортні засоби приходили повідомлення про сигнали дорожнього руху та пішоходів, що перетинають вулицю. ESCRYPT, дочірня компанія в Bosch Group, забезпечила технології інформаційної безпеки для цих демонстрацій V2X. У Китаї Bosch тестує спеціальний зв'язок з використанням Wi-Fi та мобільного інтернету. Тести стосуються оповіщення систем при обгоні та інших складних маневрах.

Системи навігації та автопілоту: Підключені автомобілі можуть використовувати вбудовані системи навігації з реальним часом, щоб надавати водіям актуальну інформацію про маршрут, дорожні умови та можливі альтернативні шляхи. Деякі автомобілі також мають функції автопілоту, які дозволяють автоматизовано керувати автомобілем в ряді ситуацій.

1.3 Системи навігації

Системи навігації:[10]

Апаратна частина

Усередині корпусу міститься три головних складових: плата, дисплей і акумулятор. Більше 10 років всі навігаційні пристрої сенсорні, тому від клавіатури швидко відмовилися.

Дисплей

Працює дисплей навігатора як і всі сенсори електронних гаджетів: підключення до шлейфу, через який проходять всі дані. Єдина особливість цього дисплея в антиблікове покриття, а це головна вимога до автомобільного пристрою, що вигідно відрізняє його від мобільника.

Плата

Тут впаяні всі елементи, необхідні для роботи гаджета. Являє собою міні-комп'ютер з мікросхемою, оперативною пам'яттю і процесором.

GPS-антена

Являє собою класичну антену, налаштовану на прийом супутникових хвиль в певній частоті. По виду установки може знімною і упаяний, але на якість прийому сигналу це не впливає.

Процесор (чіпсет)

Призначений для обробки прийнятого антеною сигналу. Існує безліч поколінь чіпсетів, які відрізняються якістю і швидкістю обробки інформації, а сучасні, крім супутника, приймають перевідбиті сигнали

Пам'ять

У автомобільного GSP три пам'яті: оперативна, внутрішня і BIOS. Оперативна пам'ять забезпечує швидку роботу навігатора, завантаження даних і оновлення розташування в режимі реального часу. Внутрішня пам'ять необхідна для завантаження карти, додаткових додатків і призначених для користувача даних. Пам'ять BIOS призначена для зберігання завантаження програми навігації.

Додаткові елементи

Крім іншого навігатори можуть оснащуватися Bluetooth для синхронізації з іншими гаджетами, GPRS-модуль і радіоприймач для отримання даних про трафік.

ПО

Програмне забезпечення підлаштовано спеціально під потреби навігатора. Особливістю ПО є те, що вона також підвантажує бібліотеки, необхідні для роботи всіх програм.

Навігаційна програма

Такі навігатори, як Garmin, Tomtom застосовують свої навігаційні карти, що забезпечує хорошу її роботу. Інші навігатори використовують сторонні карти, такі як Navitel, IGO і інші.

Рисунок 1.5 - Приклад навігаційної системи

Функції автомобільної навігаційної системи

Навігатор виконує таку роботу як:

прокладання маршруту з точки "А" в точку "Б";

-пошук необхідної адреси;

-аналіз потенційного маршруту, пошук короткого шляху;

-завчасне визначення дорожніх перешкод (ремонт дороги, ДТП тощо);

-Попередження про постах Державтоінспекції;

-статистика пройденого шляху;

-визначення швидкості руху машини.

1.4 Автопілот

Автопілот:[11]

Більшість автомобільних концернів сьогодні ведуть роботу по створенню автономного транспорту. Автомобілі, автобуси, безпілотні таксі, колісні дрони для служби доставки – сьогодні все частіше можна почути про

подібні речі. І це вже не фантастика. Однак транспортні засоби зі справжнім автопілотом усе ще мають характер дослідницьких прототипів.

Що ж таке автопілот? Просте визначення звучить наступним чином: «Автопілот - пристрій або програмно-апаратний комплекс, що керує транспортним засобом за певною, заданою йому траєкторією». З одного боку усе зрозуміло, але в більш допитливих виникають певні питання.

Насправді, водії вже давно користуються частково автономними транспортними засобами. Деякі функції, якими оснащуються сучасні машини, не вимагають втручання людини. Круїз-контроль – це вже доволі висока система автоматизації, а загалом до самостійних систем можна віднести навіть функцію вмикання світла при відчиненні дверей автомобіля.

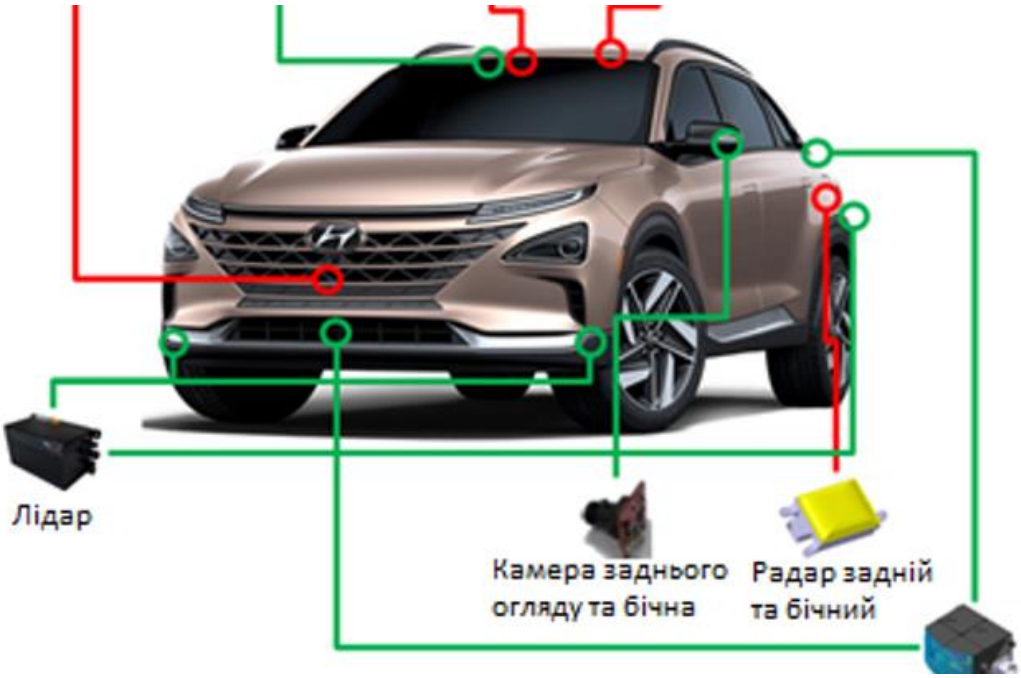


Рисунок 1.6 - Приклад систем зовнішнього моніторингу

Деякі з систем зовнішнього моніторингу та комунікації, що задіяні в роботі автопілоту.

Таким чином, визначення «автопілот» довгий час залишалося досить загальним. Не так давно, десь у той час, коли на дороги виїхала перша Tesla Model S, стала очевидною потреба у кількох важливих речах: створенні

інфраструктури та законодавчої бази для подібної техніки, а також кваліфікації подібного транспорту з системами автономного управління.

Однією з організацій, що запропонувала більш точне визначення автопілота та класифікацію таких систем стала Національна адміністрація безпеки дорожнього руху США (NHTSA). Оскільки дослідники організації мали перед собою живі приклади таких великих компаній, як Google і Tesla, можна стверджувати, що на сьогоднішній день класифікація NHTSA є найповнішою та найсучаснішою.

Рисунок 1.7 - Взаємодія автомобіля з інфраструктурою міста

Інфраструктура – важлива умова масового впровадження автономного транспорту.

Також класифікацію автопілотів приписують Товариству Автомобільних Інженерів (SAE), тому у різних джерелах, найчастіше, можна зустріти саме ці дві абревіатури. Так чи інакше, більшість автовиробників використовують саме цю класифікацію для позначення рівня автономності своєї продукції.

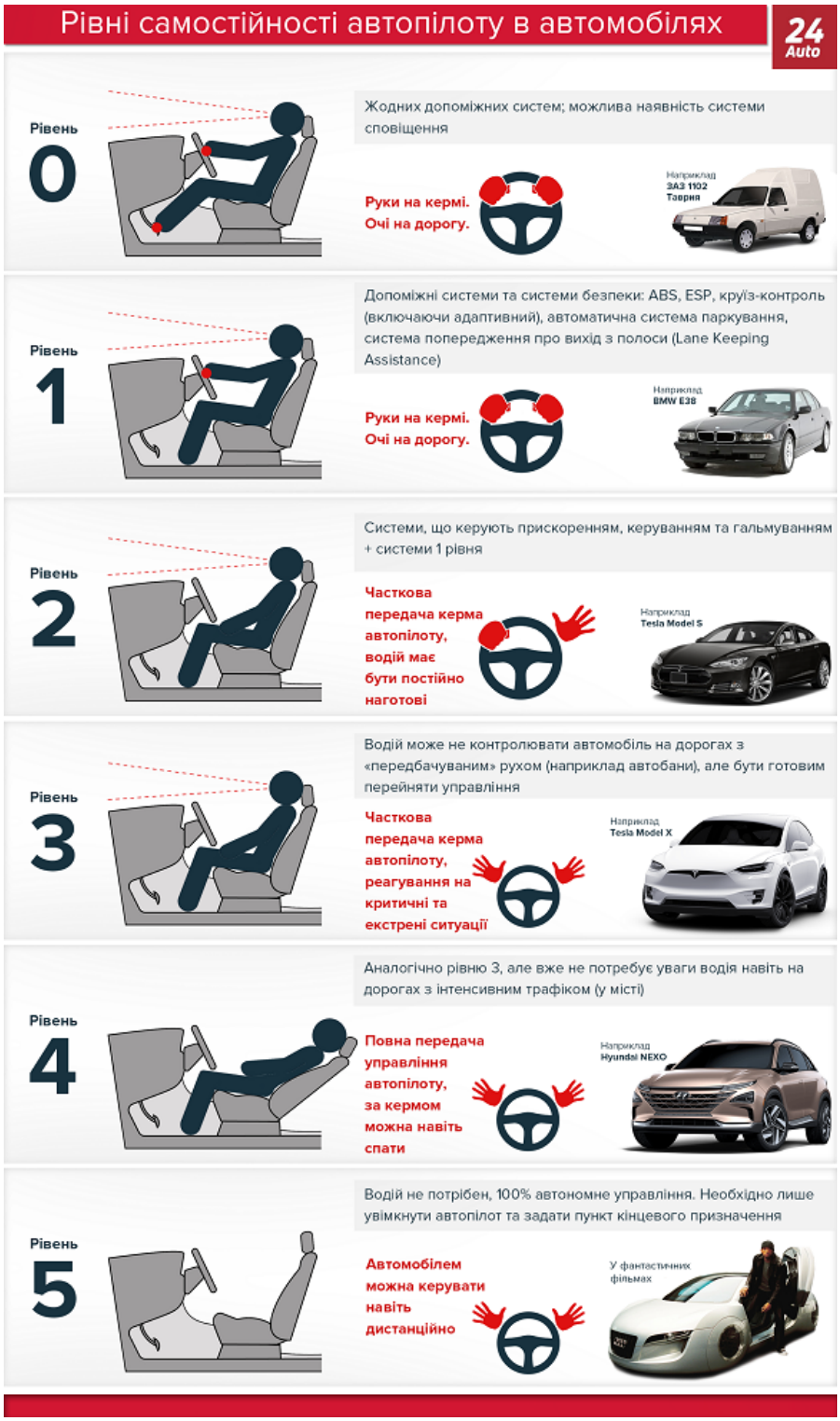


Рисунок 1.8 - Рівні самостійності автопілота на автомобілях

1.5 Системи безпеки

Системи безпеки: Підключені автомобілі можуть використовувати різні сенсори та камери для виявлення небезпек на дорозі та уникнення аварій.

Деякі системи можуть автоматично реагувати на небезпеку, виконуючи автоматичне гальмування або уникнення зіткнень.

1.6 Віддалене керування та моніторинг

Віддалене керування та моніторинг: Власники підключених автомобілів можуть використовувати мобільні додатки для віддаленого керування різними функціями автомобіля, такими як запуск двигуна, блокування або розблокування дверей, а також відстеження місцезнаходження автомобіля.

У наш час дуже широко використовується комп'ютерна діагностика, як основний спосіб визначення несправностей автомобіля. Комп'ютерна діагностика автомобіля - це процес, при якому відбувається читання кодів несправностей на основних вузлах, стирання цих кодів і подальша їх корекція. Для цього застосовуються дилерські сканери та інші прилади. До них відносяться тестери, мультифункціональні стенди, портативні рідери. Сучасне діагностується обладнання та програмне забезпечення дозволяють зчитувати і засікати найменші зміни в роботі систем управління двигуном, трансмісією, панелі приладів і інших систем. Сама процедура дуже проста, водій помічає несправність свого транспортного засобу і приїжджає на стацій технічного обслуговування, автомобіль сканують і ставлять діагноз. Це звичайно ж все добре, але на це йде багато часу, а якщо врахувати очікування вільного поста, час витрачений на діагностику з виїздом, потім і очікування запчастин для ремонту. Все це час, а багато компаній, організацій в цей період зазнають збитків, через простій транспорту. Над вирішенням цієї проблеми, працюють вже не один рік, світові лідери з виробництва автомобілів, Scania, Chevrolet. Вони розробляють і запускають свої системи дистанційної діагностики. Система дистанційної діагностики Scania (Scania Remote Diagnostics) може бути встановлена на вантажівках, що поставляються після вересня 2012 року, оскільки вони обладнані пристроями

Scania Communicator. Сервіс дозволяє майстерням виконувати діагностику на відстані, даючи можливість заздалегідь отримати уявлення отранспортном засобі. Компанія Chevrolet представляє технологію Proactive Alerts, яка буде оцінювати стан автомобіля і повідомляти про можливі в найближчому майбутньому несправності. Система запускається разом з пуском двигуна і перевіряє роботу стартера, паливного насоса і акумулятора. Отримані в ході аналізу показники порівнюються з еталонними значеннями для даної моделі автомобіля і середніми показниками інших автомобілів даної моделі через бази даних OnStar. Так що ж таке віддалена комп'ютерна діагностика автомобіля. Будьяке пристрій з GPRS передавачем, відправляє показники датчиків на сервер. На сервері проводиться обробка інформації і при виході даних вище або нижче заданого діапазону фіксується несправність, дата, час і супутні показники. Надсилається повідомлення власникові і майстру виконує обслуговування і ремонт даного автомобіля. Спеціаліст переглядає дані і умови виникнення відхилень. Приймається рішення про терміновість прийняття заходів. До приїзду автомобіля вже буде відомий діагноз і замовлені запчастини. Великі автокомпанії використовують цей спосіб з офіційними приладами, визначеними регламентами, правилами, а як же бути власникам вживаних автомобілів, і клієнтам не офіційних станцій технічного обслуговування. Останнім часом дуже популярними стали універсальні діагностичні гаджети-адаптери OBD-II, побудовані на базі мікроконтролера ELM327. [12]

Розглянемо для прикладу варіант використання ELM-327 з можливістю передачі даних через Bluetooth. Цей прилад може здійснити дистанційну діагностику. Адаптер передає інформацію через Bluetooth з'єднання на смартфон, на базі операційної системи Android. Можливість сполучення тестера і смартфона відбувається з встановленням програми Torque, рис.1.10.

Рисунок 1.9 - Вид гаджетів-адаптерів OBD-II з різними способами підключення до зовнішнього пристрою

Використовуючи мобільний інтернет, передаємо значення на віддалений сервер ПК. Так само є варіант выкористання ELM-327 на базі програмного забезпечення Windows, Windows Mobile, iOS.

Рисунок 1.10 - програма Torque Android

За таким принципом для дистанційної діагностики автомобіля можна використовувати тестери Launch. За допомогою таких адаптерів OBD-II можна виконувати наступні операції:

- читати діагностичні коди несправностей (DTC – Diagnostic Trouble Codes), як стандартні, так і спеціальні (коди виробника), а також відображати їх значення;
- проводити очищення DTC і вимикати MIL (світловий напис «CheckEngine» на панелі приладів);
- відображати інформацію контрольних пристроїв, що підключаються: частота обертання колінчатого вала і навантаження двигуна; температура оливи і охолоджуючої рідини, стан системи подачі палива; швидкість руху ТЗ; короткострокова і довгострокова витрата пального; абсолютний тиск, температура і масова витрата повітря, склад горючої суміші; кут випередження запалювання тощо.

Особливості робочих процесів систем моніторингу технічного стану. Фахівці АТ в сервісних підприємствах ІТС зчитують і інтерпретують коди, проводячи діагностування стану РС.

1.7 Оновлення програмного забезепечення

Оновлення програмного забезпечення: Підключені автомобілі можуть отримувати оновлення програмного забезпечення від виробників через інтернет. Це дозволяє вдосконалювати функціональність, покращувати безпеку та додавати нові можливості під час експлуатації автомобіля.

1.8 Екосистема для розваг та комфорту

Екосистема для розваг та комфорту: В підключених автомобілях можуть бути вбудовані розважальні системи, додатки, аудіо- та відеофункції, які дозволяють пасажирам комфортно проводити час під час поїздки.

Інформаційно-розважальна система транспортного засобу – це поєднання апаратного та програмного забезпечення, яке надає інформацію і розваги водію та пасажирам автомобіля. Втілюється це через аудіо/відео (A /

V) інтерфейси та елементи керування, наприклад, сенсорні екрани, панелі кнопок і голосові команди тощо. Розширені інформаційно-розважальні системи дозволяють підключити Bluetooth та Wi-Fi, потокове передавання живих медіа та розумну технологію мобільної інтеграції. Компоненти та функціональність залежать від специфікації.

Згідно з Consumer Reports, приблизно 82% автомобілів, проданих у 2019 році, були обладнані панеллю керування із сенсорним екраном, у порівнянні з 53% – у 2014 році. Удосконалення смартфона та зростання хмарних технологій стало поштовхом до розвитку ринку інформаційних розваг у автомобілях. І тепер відповідно до дослідження Allied Market Research у 2018 році, ця галузь оцінюється у понад $11,14 мільярда.

У виробництві автомобілів відбулася зміна парадигми – від механічної винахідливості до якості програмного забезпечення, виконання та інтеграції. За останні кілька років різко зріс попит на системи, які пропонують комфорт та розваги в автомобілі – музика за запитом, розумна навігація та опції гучного зв’язку. І не випадково цей зсув співпадає зі стрімким попитом смартфона та всіх сервісів, до яких ми звикли отримувати доступ одним натисканням на екран.

Усвідомлюючи потенціал збільшення прибутку від автомобільних технологій, багато великих гравців автомобільної промисловості зараз інтегрують системи розваг у свої машини. Це своєю чергою розвиває ринок для всіх автовиробників.

Загалом, підключені автомобілі спрямовані на створення безпечніших, зручніших та більш ефективних транспортних засобів за допомогою інтеграції передових технологій.[13]

Автомобілі стають все більш поширеним програмним забезпеченням. Дійсно всередині звичайного автомобіля є понад мільйон рядків коду. Але поява інформаційно-розважальних систем у транспортних засобах відбулася у той час, коли багато автомобілів ще використовували застарілу програмну

технологію. Отже, незважаючи на попит, є три важливі елементи, які виробники автомобілів повинні врахувати:=

Постійно оновлюйте програмне забезпечення

Інформаційно-розважальні системи для транспортних засобів зазвичай розробляються як частина довгострокового проекту, який триває кілька років. Специфіка таких проектів полягає у тому, що їх, як правило, розробляють десятки інженерів впродовж певного періоду часу. В умовах безупинних технологічних змін цей час грає не на користь виробників, які можуть втратити можливість проектувати. Крім того, технології часто базуються на класичному розумінні традиційної вбудованої інженерії (у виробництві електроніки), що фактично суперечить значенню цифрового «тренду». Гнучкість до змін – єдиний спосіб залишатися актуальними на ринку.

Це довела індустрія мобільних телефонів, яка протягом багатьох років відчувала жорстку конкуренцію між Android, iOS, Symbian (припинено, незважаючи на використання найпотужнішого програмного забезпечення C/C ++) та Windows Phone (також припинено). Найбільш гнучкі конкуренти змогли випередити тих, хто залишився на бажаних платформах, адже вони відреагували на зміни ринку.

Щоб бути на крок попереду, виробники зараз використовують такі стратегії:

- Розробка додатків, орієнтована на конкретні інформаційно-розважальні системи
- Автовиробники хочуть диференціюватися від конкурентів. Багато виробників розробляють власне програмне забезпечення для своїх унікальних інформаційно-розважальних систем автомобілів, щоб збільшити свої розробки принаймні на 50% до 2025 року.

Деякі німецькі виробники вже створили спеціалізовані підрозділи інженерії програмного забезпечення для автомобілів у своїх компаніях. Ці

команди відповідають за розробку програмного забезпечення для автомобілів, цифрових екосистем та функцій продажу, орієнтованих на клієнтів.

Удосконалювати доступні програми за допомогою інтеграції існуючих платформ.

Здебільшого виробники віддають перевагу опції використання існуючих екосистем Google або Apple, а не розробці програмного забезпечення з нуля. Це означає, що їхні інформаційно-розважальні системи транспортних засобів сумісні з більшістю смартфонів і підтримують автоматизовані функції з навігації, здійснення телефонних дзвінків, програвання музики та виконання інших завдань.

Деякі монопольні німецькі та скандинавські виробники автомобілів обрали цей шлях, оголосивши про перехід до Android Automotive Google. Але цей крок вважають дещо суперечливим, оскільки такий перехід вимагає постійної розробки та обслуговування декількох програмних додатків.

Використовувати незалежну крос-платформу або відкрите програмне забезпечення:

Виробники можуть використовувати незалежні крос-платформи та/або відкрите програмне забезпечення як основу для своїх інформаційно-розважальних систем автомобіля. Операційна система на це не впливає. Розглянемо Qt, спадкоємну систему Symbian. Qt є C/C++ зворотно сумісною і може бути легко адаптована “класичними” вбудованими командами розробників. Це крос-платформа, яка може працювати на Android. В основному вона підтримує інтерфейс на основі OpenGL, що має вирішальне значення у світі розваг. Крім того, стек C/C++ забезпечує високу продуктивність та досвід користування у реальному часі, які є критичними для безпеки в автомобілі. Альтернативний варіант, який варто розглянути, – Xamarin. Він має більшість переваг Qt, окрім мови програмування. Це вимагає переходу на C#, що може означати уточнення кваліфікації вашої існуючої інженерно-розважальної команди.

Незалежно від стратегії, якій ви віддаєте перевагу, впровадження вдосконаленого програмного забезпечення дозволить досягти максимальної продуктивності автомобіля та допоможе вам зберегти конкурентоспроможні переваги. Зараз споживачі шукають універсальний пристрій для мобільності, який повторює досвід смартфона. Це зобов'язання виробників авто – забезпечувати інновації та оновлення програмного забезпечення.

Для подолання викликів автомобільної діджиталізації багато автомобільних компаній набирають зовнішніх постачальників послуг, щоб полегшити перехідний період.

Вимоги адресного підключення

Інформаційно-розважальні системи транспортних засобів – це місце перетину автовиробників, замовників та онлайн-сервісів. Ці послуги вимагають підключення між зовнішніми пристроями такими, як: мобільні та Інтернет, медіа-трансляції, навігації та миттєвого обміну інформацією.

Вже зовсім скоро власники автомобілів зможуть домовитись про зустріч з друзями, знайти місце, де поїсти та забронювати стіл в Інтернеті, використовуючи інформаційно-розважальну систему свого автомобіля як центр управління з одним великим дисплеєм, у якому розміщений інтегрований екран і кластер інструментів. Невдовзі це стане стандартною функцією усіх автомобілів.

Спалах Covid-19 пришвидшив розвиток автономного автомобіля, і виробники адаптувались до перспективи довгострокового соціального дистанціювання. Лише кілька місяців тому споживачі не відмовлялися від візитів СТО, щоб перевірити авто на оновлення. А тепер бренди повинні обдумати запуск віддалених оновлень програмного забезпечення для навігації та розваг.

Зважаючи на це, виробники автомобілів можуть гарантувати безперебійне підключення, хоча ізольовано домогтися цього неможливо. Автовиробникам все частіше доведеться працювати з зовнішніми

постачальниками послуг, щоб створити програмне забезпечення для різних рівнів доступу.

Гарантія безпеки

Коли автомобілі зараз більше нагадують комп'ютери на колесах, ніж традиційні транспортні засоби, існує більша загроза порушення безпеки. Інформаційно-розважальні системи транспортних засобів особливо піддаються спробам злому, якщо вони базуються на застарілому програмному забезпеченні, тому так важливо, щоб воно залишалося актуальним.

Оскільки інформаційно-розважальні системи тепер розробляються як комплексний центр управління драйверами, конфіденційна інформація, включаючи історію викликів, контакти, текстові та електронні повідомлення, можуть зберігатися на інформаційно-розважальному блоці. І оскільки ця інформація не розроблена відповідно до сучасних принципів безпеки програмного забезпечення, вона піддається атакам сторонніх виробників.

Дослідники безпеки продемонстрували, що вони можуть підключатися до систем керування автомобіля через інтерфейс інформаційно-розважальних програм, отримуючи доступ до трансмісій, інформаційно-розважальних та кліматичних функцій. Автомобільні компанії об'єдналися для вирішення проблем цих вразливих місць, але такі інциденти вже спричинили ризики і рознервували людей. Таким чином, кібербезпека автомобілів стала основним компонентом виробництва автомобілів.

Зрештою, як і захист від зовнішніх загроз, технології в автомобілі повинні гарантувати безпечну взаємодію водія під час руху. Отже, інтерфейс інформаційно-розважальної системи автомобіля повинен бути простим у використанні та не відволікати увагу. Стандарт ISO 26262 функціональної безпеки регулює системи розваг, щоб мінімізувати відволікання водіїв і, таким чином, зосереджувати увагу водіїв на дорозі. Згідно з дослідженнями What Car?, вдосконалена система голосового управління є найменш відволікаючим способом виконання завдань на ходу. Однак найкращі

рішення для автомобільних інформаційних розваг пропонують цілу низку можливостей інтерактивності, щоб водій міг обрати найзручніший залежно від ситуації.

1.9 Висновки до розділу 1

Підключений автомобіль є визначальним поняттям в сучасній автомобільній промисловості, що відображає глибокі трансформації та інновації в області автомобільних технологій. Термін "підключений автомобіль" визначає транспортний засіб, який взаємодіє з Інтернетом та іншими пристроями, створюючи екосистему, що революціонізує спосіб, яким ми сприймаємо автомобіль та взаємодіємо з ним.

Підключені автомобілі впроваджують ряд інновацій, що охоплюють безпеку, комфорт, ефективність та автоматизацію. За допомогою вбудованих сенсорів, мережевих з'єднань та інтелектуальних систем управління, вони здатні збирати та обробляти величезний обсяг даних для поліпшення досвіду водіння та оптимізації функціонування автомобіля.

Однак із зростанням підключених функцій з'являються і нові виклики, зокрема у сфері кібербезпеки. Забезпечення безпеки підключених автомобілів стає критичною задачею, оскільки вони стають об'єктом потенційних кібератак та зловживань. Розуміння і ефективне вирішення цих викликів визначає успішне впровадження підключених автомобілів та забезпечення їхньої безпеки в середовищі Інтернету речей.

Загалом, підключені автомобілі не тільки змінюють спосіб, яким ми сприймаємо автомобіль, але й визначають новий етап в еволюції транспортних засобів, де технології та інновації взаємодіють для створення безпечних, зручних та динамічних систем мобільності.

2 ФУНКЦІЇ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

2.1 Категорії на які поділяються функції автомобіля

Функції підключеного автомобіля поділяються на кілька категорій:

1.безпека

2.навігація

3.інформаційно-розважальна система

4.діагностика/ефективність

5.оплата.

Безпека

Допомога на дорозі – найпопулярніша і найвідоміша послуга

On Star, в якій агенти допомагають водіям у випадках аварій або інших небезпек, звертаючись до органів влади та рятувальників залежно від потреби. Дослідження довели, що служби екстрених викликів запобігають травмам , а системи уникнення зіткнень зменшують кількість аварійних випадків.

Попереджений про дорожній рух, безпеку та зіткнення – коли автомобіль під’єднано до навігації, міської інфраструктури або карт громад, таких як Waze, HERE або TomTom, водій може отримувати сповіщення про зіткнення, затори, вибоїни, сміття на дорозі тощо. Автомобіль також може зв’язуватися різними способами з іншими пристроями, такими як транспортний засіб – транспортний засіб (V2V), транспортний засіб – інфраструктура (V2I), транспортний засіб – пішохід/телефон (V2P) або транспортний засіб – усе (V2X) для отримання складної інформації наприклад, включення або зміна вогнів, коли в той же час немає інших автомобілів.

Навігація

навігація через додаток для смартфона/iPhone або через вбудовану систему навігації GPS.

сповіщення про від'їзд і текстові сповіщення – під'єднавшись до додатків за межами автомобіля, водій може отримувати сповіщення про найкращий час для виїзду, тоді як автомобіль або програми повідомляють друзів чи колег про час прибуття автомобіля.

трафік в режимі реального часу – керівництво з використанням трафіку в реальному часі та ситуацій.

погода в режимі реального часу – сповіщення про погану погоду, коли вона змінюється.

платежі в русі – можливість оплатити речі, не виходячи з транспортного засобу.

Інформаційно-розважальний

музика/аудіо, подкасти, Інтернет-радіо через різні пристрої, такі як смартфон або планшет з підтримкою Інтернету. Є програми, які відтворюють музику відповідно до вашого настрою.

смартфон/iOS/Android та власні програми чи програми.

голосові команди та елементи керування «вільні руки » – часто головний пристрій реагує на голосові команди, наприклад «Відтвори мою пісню». а більш складні варіанти можуть бути в стилі Siri, наприклад «Перейти до найближчої заправки.

Bluetooth – це бездротове з'єднання зазвичай дозволяє водієві використовувати Bluetooth для мобільного телефону або смартфона для створення та отримання телефонів. Часто біля водія розташований мікрофон, щоб водій міг говорити, а голос абонента відтворюється через динаміки автомобіля. Bluetooth також можна використовувати для потокової передачі музики з під'єднаного Bluetooth пристрою, наприклад iPod, iPhone, смартфона або планшета чи iPad з підтримкою Bluetooth.

Точки доступу 4G Wi-Fi – GM, починаючи з моделі Chevy Malibu 2015 у червні 2014 року, пропонує 4G LTE у всіх своїх автомобілях. Audi A3 є технічно першим автомобілем, підключеним до 4G LTE, у США . Volvo також запропонує 4G LTE від AT&T влітку 2014 року.

контекстна допомога/пропозиції – нова арена в підключеній комп'ютерній системі вивчає переваги водія, а потім пропонує допомогу, наприклад, коли бензобак низький, показує найближчі АЗС. Голосові команди адаптуються до користувача, як у випадку з SYNC 2 , водій каже «Я голодний», і відображаються найближчі ресторани.

Оплата

Платежі – GM був першим виробником автомобілів у США, який запустив платежі з приладдя через Marketplace за пончики, каву та інші продукти швидкого приготування. Тоді водії автомобілів Chevrolet, які відповідають вимогам , зможуть оплачувати через сенсорний екран у своєму автомобілі, коли вони заправляються на заправках під брендом Shell, без використання кредитної картки або мобільного пристрою. Потім Hyundai оголосила, що дозволить здійснювати платежі через Xevo.

Ще на етапі оголошення ідея полягає в тому, що водієві не потрібно залишати автомобіль, щоб оплатити бензин чи інші послуги. DocuSign і Visa продемонстрували нову концепцію підтвердження, яка об'єднує безпечні контракти та платежі, які здійснюються онлайн через підключений автомобіль.

Наразі не існує жодної домінантної операційної системи для комп'ютерів головного пристрою чи інших пристроїв, які підключаються до iPhone чи Android, зокрема Airbiquity, QNX, Mirrorlink, WEBLINK та інші. QNX має найбільшу частку ринку. Раніше в 2014 році був створений Open Automotive Alliance на базі операційної системи Android від Google.

MirrorLink — це система від Car Connectivity Consortium, де те, що відображається на смартфоні, відображається на екрані приладової панелі, яка наразі пропонує LBS-локатор Glympse і Parkopedia.

У березні 2014 року Apple анонсувала CarPlay , який працює на iPhone 5/5c/5S через кабель Lightning з більшим переглядом значків, який працює з Siri. До 2017 модельного року CarPlay впроваджують у Hyundai , Ferrari,

Mercedes-Benz, Volvo, Ford, Honda, майже всі моделі GM, Buick та Cadillac, BMW тощо.

У червні 2014 року Google представила Android Auto, систему для смартфонів Android, подібну до CarPlay, яка використовує голосові команди та кнопки на кермі. Виробники автомобілів, які впровадять Android Auto , включають Hyundai, Volvo, Honda та інші.

Ще одним конкурентом CarPlay є WEBLINK . QNX — популярна ОС для серверної системи, яка запускає підключені автомобільні системи із сертифікацією безпеки.

2.2 Висновки до розділу 2

Функції підключеного автомобіля відіграють ключову роль у трансформації автомобільної індустрії та надають користувачам інноваційні можливості та підвищують якість водіння та взаємодії з транспортним засобом. Ці функції, забезпечені технологіями Інтернету речей (IoT) та вбудованими системами зв'язку, створюють інтелектуальне автомобільне середовище, спрямоване на забезпечення безпеки, комфорту та ефективності.

Однією з ключових функцій є здатність підключеного автомобіля до Інтернету, що відкриває широкий спектр можливостей для збору, обробки та обміну даними. Це дозволяє впровадження таких інновацій, як системи навігації в режимі реального часу, віддалене керування, оновлення програмного забезпечення та інші сервіси, що покращують функціональність та зручність використання автомобіля.

Функції безпеки, такі як системи виявлення зіткнень, контроль сліпих зон, адаптивний круїз-контроль та системи автоматизованої паркування, сприяють покращенню безпеки водіїв та пасажирів. Технології взаємодії з водієм та пасажирами, такі як голосове керування та інфотейнмент-системи, роблять кожну поїздку більш інтерактивною та розважливою.

Зростання популярності підключених автомобілів також відкриває двері для розвитку автономних транспортних засобів, що потребує обміну величезним

обсягом даними між автомобілями та навколишнім середовищем для забезпечення безпеки та координації руху.

У цілому, функції підключеного автомобіля визначають нові стандарти в сучасній автомобільній індустрії, надаючи користувачам унікальний досвід водіння та створюючи перспективи для подальшого розвитку автомобільної мобільності.

3 АНАЛІЗ ІСНУЮЧИХ ЗАГРОЗ, СУТНІСТЬ ТА ПОНЯТТЯ КІБЕРБЕЗПЕКИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

3.1 Сучасна ситуація в області кіберпідключеного автомобіля

Сьогоднішні автомобілі - це, по суті, комп'ютер на колесах, що складається зі складних і часто взаємопов'язаних наборів автомобільних систем, таких як гальмування, електричні замки, кермо, системи розваги, управління вікнами та інші особливості.

На додаток до цих всіх можливостей, автомобілі наступного покоління додають безліч функцій, від автономної роботи до вдосконалених систем допомоги водієві (ADAS), які тільки збільшують загальну складність. [7]

3.1.2 Система ADAS

Що являє собою система ADAS, її функції

ADAS (Advanced Driver Assistance System) – це ряд функцій, які передбачені в комплектації авто, або додаються додатково і призначення їх - допомога водію. Система повідомляє про наявність проблематичної ситуації яка виникла, або може виникнути на дорозі, тобто автоматизує і підвищує рівень безпеки транспортного засобу.

Укомплектована система наступними основними складовими:

-Системою екстреного водіння;

-Системою рульового автоуправління;

-Системою управління авто педалями;

-Системою безперешкодного виклику по телефону.

-Всі системи підрозділяються на види, відповідно до принципу функціонування.

Існують такі види ADAS:

1)Адаптивна – пристосовується до роботи з урахуванням даних, отриманих із зовні.

2)Автоматизована – здійснює функції, які недоступні для безпечного виконання водієм.

3)Моніторингова – оцінює обстановку поблизу авто, при необхідності приймає рішення про втручання в процес водіння. Для спостереження та оцінки використовуються спеціальні датчики, відеокамери.

4)Попереджувальна – повідомляє про наявність ймовірну небезпеку на дорозі.

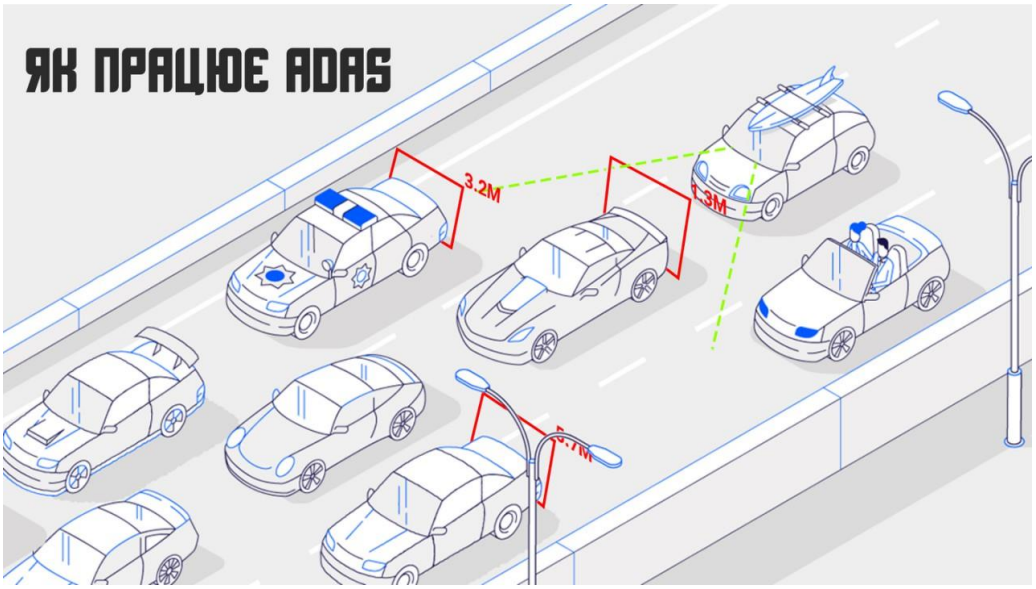


Рисунок 3.1 - Приклад роботи ADAS [14]

Основні елементи системи ADAS

Forward Collision Warning System (FCWS). Функція елемента полягає в контролі швидкості зближення з іншим авто. Він повідомляє про небезпеку зіткнення, якщо даний показник перевищує 30 км / год.

Lane Departure Warning System (LDWS). Функція стеження проходження авто точно за обраною смугою траси. У разі порушення кордонів розмітки, пристрій їх фіксує і повідомляє водія. Функція розпізнає трасу і дороги міста виключно при їзді на швидкості не менше 60 км / год, і тільки тоді починає працювати.

Forward Vehicle Stop Alarm (FVSA). Функція незамінна в разі потрапляння в пробку або при русі в щільному потоці машин. Вона повідомляє про своєчасність старту, якщо водій пропустив момент початку руху машини, що попереду.

Pedestrian Detection Warning System (PDW). Елемент виявляє пішоходів і повідомляє про їх можливу появу перед автомобілем за кілька секунд до того, як може відбутися зіткнення. Особливо корисна функція в нічний час або в туман. Здійснюється вона завдяки установці вузькооптичної відеокамери.

Blind Spot Detection (BSD). Повідомляє про наявність об'єктів в сліпих зонах. Здійснюється завдяки установці двоканального відеореєстратора, камер і детекторів.

Movingcardetection (MCD). Система попереджає про наявність неконтрольованого руху по похилій, перевищенні швидкості автомобілів які рухаються попереду. Встановлюється система в реєстратор з GPS модулем.

Rearview camera. Транслює на екран автореєстратора ситуацію на дорозі позаду автомобіля, по суті функціонує як паркувальна камера.

Emergency call, аварійна кнопка SOS. Спрацьовує при різких поворотах, гальмуваннях, ударах, сприймаючи їх як ознаки ДТП. Система передає сигнал в екстрену службу через телефонне повідомлення або інтернет.[14]

В цілому, стрімке зростання кількості електронних блоків управління (ЕБУ). Навіть найпростіші автомобілі мають не менше 30 ЕБУ, а дорожчі моделі містять понад 100 ЕБУ, з'єднаних між собою лабіринтом різноманітних цифрових шин - Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST) , Ethernet. Додавання нових комунікаційних інтерфейсів у транспортних засобах є широким полем можливостей для хакерів.

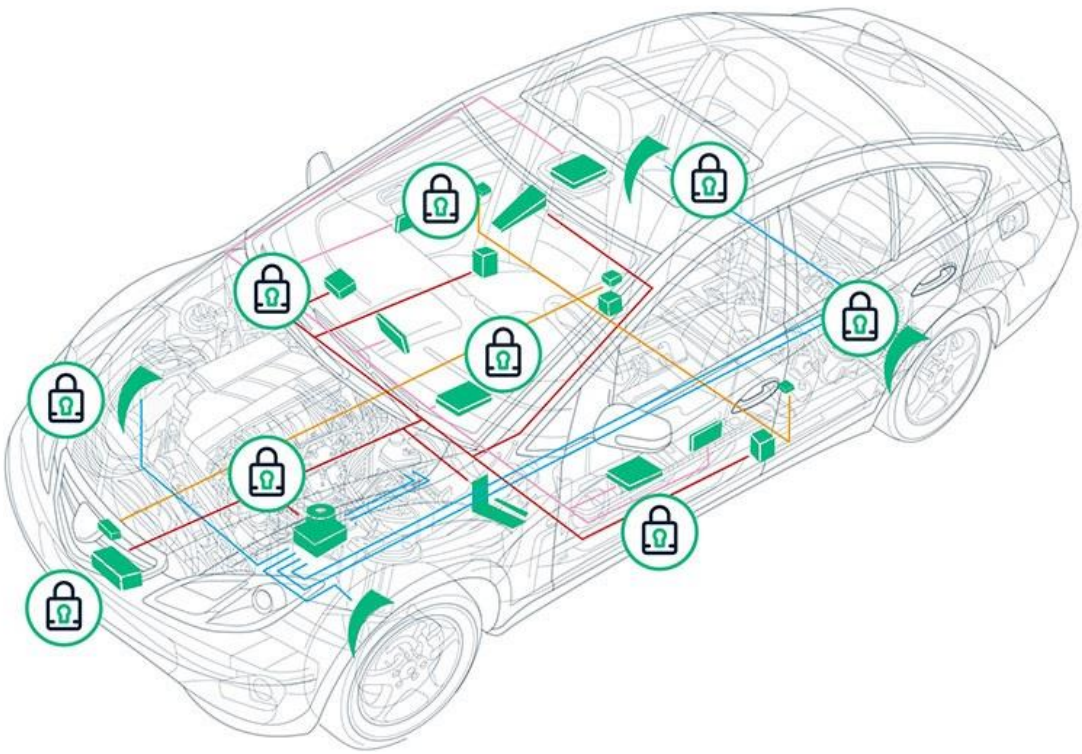


Рисунок 3.2 - Вразливі точки автомобіля[7]

Багато автомобілів вже отримують дані з супутників, а в майбутньому очікується, що в регіонах з поганим покриттям мобільного зв'язку супутники будуть використовуватися для передачі даних.

Більшість нових моделей автомобілів мають підтримку eSIM, що дозволяє передавати телематичні дані, взаємодіяти з серверами хмар, створювати точки доступу Wi-Fi, отримувати інформацію про дорожню обстановку в режимі реального часу, відправляти місцезнаходження для аварійних служб.

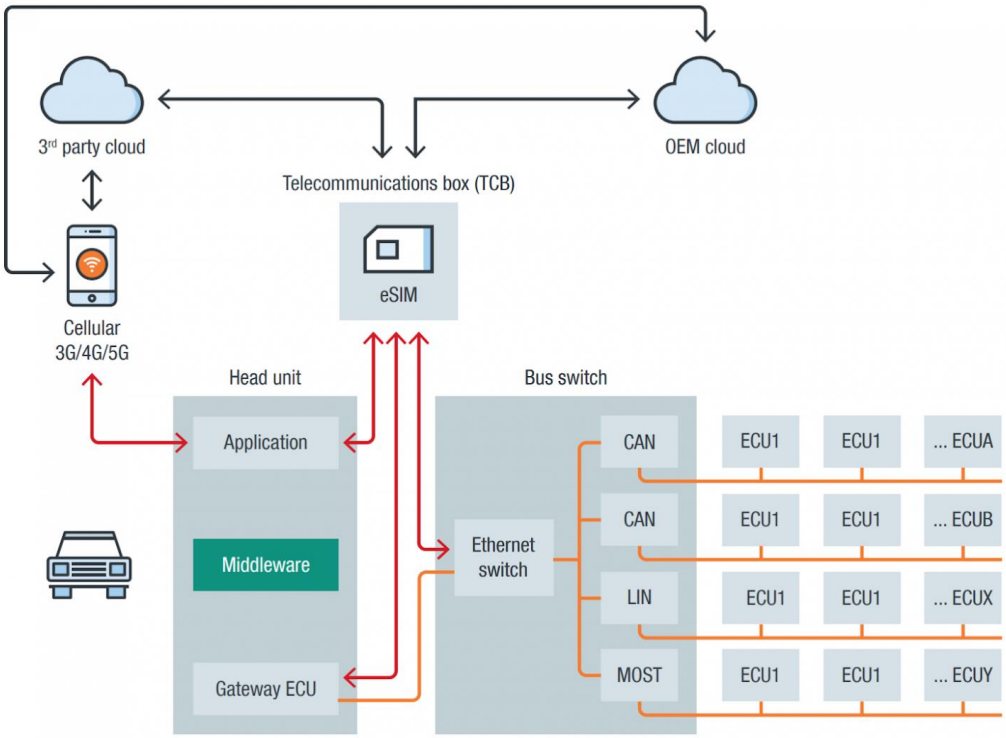


Рисунок 3.3 - Хмарна екосиситема підключених автомобілів[7]

Експерти з безпеки приділяють все більше уваги зростаючій кількості підключених до мережі автомобілів. Очікується, що до 2030 року на дорогах з'явиться понад 18 млн. нових автоматизованих транспортних засобів (Frost & Sullivan). Якщо виробники та постачальники автомобілів не будуть прагнути до забезпечення їх безпеки з самого початку, цей приплив підключених автомобілів нестиме підвищені ризики, як на особистому, так і на комерційному рівні.

Будь-який новий пристрій інтернет речей (IoT) відкриває ще одну точку вразливості. Коли ці «пристрої» є транспортними засобами, що перевозять людей на високих швидкостях дорогами, ці вразливості стають загрозою безпеці.

Це не просто теоретична проблема для автомобілів майбутнього. Фактично, за даними Товариства виробників та трейдерів автомобілів (SMMT), дві третини нових автомобілів, зареєстрованих сьогодні у Великій Британії, вже підключені. Така можливість підключення відмінно підходить

для розширених служб телеметрії, оновлень бездротової мережі та доставки контенту для бортових інформаційно-розважальних систем (IVI). Це також означає, що автомобіль підключений до інтернету, тому спілкування між автомобілями, а також ризик – це вулиця із двостороннім рухом.

Хоча транспортний засіб може надсилати корисні дані про водія та автомобіль виробнику, механізми, що керують його рухом, такі як рульове управління, гальмування та прискорення, можуть бути зламані ворожими суб'єктами, якщо електронні блоки керування автомобіля не автентифіковані та не захищені належним чином.

Основна загроза полягає в тому, що ворожий суб'єкт проникає в комунікаційні або керуючі мережі, що з'єднують автомобілі, що дозволяє атакувати автопарк. Така атака потенційно може вимагати мало ресурсів і може завдати шкоди великій кількості пасажирів транспортних засобів та пішоходів.

3.2 Види підключень

Перед тим як розглянути загрози підключеного автомобіля, потрібно знати яку саме інформацію транспортний засіб збирає за час роботи, та які види підключень бувають.

V2V (Vehicle-to-vehicle) – система підключення одного автомобіля до іншого:

Бездротова система, головне завдання якої обмін інформацією між двома автомобілями. За допомогою цієї системи, підключений автомобіль може отримувати дані про швидкість руху, місцезнаходження іншого автомобіля тощо. Подібні системи здатні забезпечувати безпеку і контролювати трафік на дорогах.

Технічні аспекти V2V:

1. Радіо-зв'язок:

- DSRC або C-V2X: Системи V2V використовують радіо-зв'язок, такий як Dedicated Short-Range Communications (DSRC) або Cellular Vehicle-to-Everything (C-V2X). DSRC працює на частоті 5.9 ГГц, в той час як C-V2X може використовувати мережі 4G та 5G.

2. Антени та Датчики

- Вибір Антен: Різні транспортні засоби можуть вимагати різні типи антен для оптимального зв'язку. Всередині автомобіля, на даху чи вбудовані в кузов — вибір антени впливає на якість сигналу.

- Типи Датчиків: GPS, Лідари та радари, для отримання точної інформації про розташування та оточуюче середовище.

3. Стандарти та Протоколи:

- IEEE 802.11p: Стандарт DSRC, визначає характеристики фізичного та канального рівнів для забезпечення зв'язку між транспортними засобами.

- C-V2X та 3GPP: Стандарт C-V2X, розроблений 3GPP, використовує мережі 4G і 5G для забезпечення високошвидкісного та надійного зв'язку.

Безпека V2V:

1. Шифрування та Аутентифікація:

2. Захист від Вторгнень

3. Цілісність Даних:

- Хеш-функції

- Цифрові Підписи

4.Приватність та Анонімізація:

- Анонімізація Даних: можливість анонімізації особистої інформації у переданих даних.

- Обмеження Доступу: системи, що обмежують доступ до конфіденційних даних та інформації про учасників дорожнього руху.

[6]V2G (Vehicle-to-grid), система підключення автомобіля до енергосистем:

Система, що дозволяє підключати автомобілі в загальну електричну мережу для підзарядки машини або повернення зайвої електроенергії назад в

мережу. Учасники системи V2G зможуть продавати електроенергію в енергосистему – в ті години, коли машина не використовується, і заряджати автомобіль в години, коли електроенергія дешевша.

Технічні аспекти V2G:

1. Електрична Архітектура:

- Системи Зарядки: типи систем заряджання, такі як AC та DC, які використовуються в технології V2G.

-Потужність та Напруга: параметри електричної енергії, які можуть передаватися між електричним транспортним засобом і мережею.

2. Комунікаційні Протоколи:

- Стандарти обміну даними: протоколи комунікації між електричним транспортним засобом і мережевим оператором.

- Мережеві Технології:використання технологій, таких як Zigbee чи Інтернет речей (IoT) для забезпечення надійної комунікації.

3. Інфраструктура Мережі:

- Зарядні Станції: Розповсюдженість та характеристики зарядних станцій, спроектованих для інтеграції з мережею електропостачання.

- Смарт-мережі: використання смарт-мереж для моніторингу, керування та оптимізації електричної енергії.

4. Управління Енергією:

- Алгоритми Зарядки/Розрядки:алгоритми, що визначають розподіл потужності між транспортним засобом та мережею.

- Прогнозування Потреби Енергії: системи, які прогнозують споживання енергії для оптимального планування зарядки та розрядки.

Безпека V2G:

1. Шифрування та Аутентифікація

- Шифрування Даних: механізми шифрування для захисту від несанкціонованого доступу до даних про енергоспоживання та іншої інформації.

- Аутентифікація Сторін: протоколи аутентифікації для підтвердження легітимності електромобіля та зарядної станції.

2. Захист від Вторгнень:

- Моніторинг Зарядних Станцій: системи моніторингу, які виявляють аномалії у функціонуванні зарядних станцій та у разі необхідності вимикають їх.

- Кіберзахист: захист систем від кібератак, оскільки V2G може стати об'єктом кібернападів.

3. Цілісність та Надійність:

- Цифрові Підписи: цифрові підписи для перевірки цілісності та автентичності комунікації між транспортним засобом та мережею.

- Резервне Живлення: використання резервного живлення для збереження доступу до енергії навіть у випадку відмови в електромережі.

4. Обмеження Доступу:

- Рівні Доступу: різні рівні доступу до систем V2G для забезпечення, що кожен користувач має доступ лише до необхідних функцій та даних.

- Фізична Безпека: фізична безпеку зарядних станцій для уникнення можливих атак.

V2P (Vehicle-to-pedestrian), система взаємодії автомобіля з пішоходами (а точніше їх гаджетами):

Система, через яку автомобіль може взаємодіяти з поруч розташованими від нього пішоходами. Отримуючи доступ до частотного діапазону смартфонів, якими користуються пішоходи, сенсори автомобіля можуть дізнатися швидкість і напрямок руху мобільного гаджета і пішохода.

Технічні аспекти V2P:

1. Системи Виявлення:

- Використання Датчиків: технічні рішення, такі як камери, радари та лідари, для виявлення пішоходів навколо транспортного засобу.

- Обробка Зображень: методи обробки зображень для ефективного визначення та відстеження руху пішоходів.

2. Системи Комунікації:

- B2P Протоколи: протоколи, використовувані для обміну інформацією між транспортним засобом та пішоходами (наприклад, Wi-Fi Direct).

- Діапазон та Зони Покриття: технічні аспекти, пов'язані з визначенням діапазону та зон покриття систем V2P.

3. Взаємодія з Системами Інфраструктури:

- Інтеграція з Світлофорами: технічні рішення для інтеграції V2P зі світлофорами для оптимізації руху пішоходів.

- Геолокаційні Системи: використання геолокаційних систем для точного визначення місцезнаходження пішоходів.

Безпека V2P:

1. Автоматизовані Системи Уникнення Зіткнень:

- Взаємодія з Системами Автомобільної Безпеки: технічні аспекти взаємодії V2P з системами, що запобігають зіткненням у транспортних засобах.

- Визначення Траєкторій: технології визначення траєкторій для прогнозування руху пішоходів.

2. Захист Особистих Даних:

- Анонімізація Ідентифікаційних Даних: технічні методи для анонімізації ідентифікаційних даних пішоходів.

- Шифрування Даних: шифрування даних, щоб запобігти несанкціонованому доступу до особистої інформації.

3. Системи Екстреної Реакції:

- Реакція на Надзвичайні Ситуації: технічні аспекти систем автоматичної реакції на надзвичайні ситуації, наприклад, автоматичне гальмування у випадку небезпеки для пішоходів.

- Системи Визначення Загроз: системи, які визначають потенційні загрози для безпеки пішоходів.

4. Ефективність Систем V2P:

- Мінімізація Затримок: технічні методи для мінімізації затримок у передачі даних між транспортним засобом та пішоходом

V2I (Vehicle to Infrastructure), система підключення автомобіля до ресурсів інфраструктури:

Дана система зв’язку, збирає дані вироблені автомобілем і надає інформацію про інфраструктуру водієві. Дана система працює в комплексі з системами V2V і так само забезпечує можливість прорахунку найоптимальнішого маршруту і допомагає запобігти можливим ДТП (в автомобілях з автопілотом).

Технічні аспекти V2I:

1. Комунікаційна Інфраструктура:

- Мережеві Протоколи: протоколи комунікації, використовувані для взаємодії між транспортними засобами та інфраструктурою (наприклад, Dedicated Short-Range Communications - DSRC).

- Інтернет Речей (IoT): використання технологій IoT для створення розумних інфраструктурних систем.

2. Системи Світлофорів та Дорожні Знаки:

- Інтеграція з Світлофорами: технічні аспекти інтеграції транспортних засобів зі світлофорами для оптимізації руху.

- Розпізнавання Дорожніх Знаків: системи комп'ютерного зору та машинного навчання для розпізнавання дорожніх знаків.

Системи Дистанційного Управління Трафіком:

- Системи Управління Трафіком: технічні аспекти систем управління трафіком, які можуть взаємодіяти з транспортними засобами для оптимізації руху.

- Віддалене Управління Світлофорами: системи, які дозволяють дистанційне управління світлофорами з метою поліпшення ефективності трафіку.

4. Системи Паркування

- Сенсори та Камери: Розгляньте технічні засоби, такі як сенсори та камери, що допомагають визначати наявність вільних паркомісць.

- Інтеграція з Навігаційними Системами: технічні аспекти інтеграції систем паркування з навігаційними системами для покращення пошуку паркомісць.

Безпека V2I:

1. Шифрування та Аутентифікація:

- Шифрування Даних: технічні методи шифрування для захисту передаваних даних між транспортними засобами та інфраструктурою.

- Методи Аутентифікації: протоколи аутентифікації для перевірки легітимності інфраструктурних об'єктів.

2. Виявлення Зіткнень та Загроз:

- Системи Виявлення Зіткнень: технічні аспекти систем, які виявляють можливі зіткнення та надають відповідне попередження.

- Виявлення Загроз для Інфраструктури: системи, які виявляють потенційні загрози для інфраструктури та реагують на них.

Централізоване та Розподілене Управління:

- Централізоване Управління: системи централізованого управління, які координують взаємодію транспортних засобів із засобами інфраструктури.

- Розподілене Управління: технічні аспекти розподіленого управління, де транспортні засоби та інфраструктура взаємодіють без централізованого контролю.

4. Захист від Кіберзагроз:

- Мережеві Заходи Безпеки: заходи безпеки для мережі, що взаємодіє між транспортними засобами та інфраструктурою.

- Оновлення та Захист від Вразливостей: системи регулярних оновлень та захисту від вразливостей для інфраструктурних об'єктів.

V2C (Vehicle to Cloud), технологія підключення автомобіля до хмарних сервісів:

Подібний вид зв’язку автомобіля з хмарними засобами, створює канал передачі даних між автомобілем і сервісами, що збирають та зберігають дані вбудовані в різні додатки які користувач підключає до автомобіля (наприклад сервіси, що дозволяють отримувати доступ до музичної онлайн бібліотеки).

Vehicle-to-Cloud (V2C): Технічні аспекти та Безпека

Технічні аспекти V2C:

1. Збір та Передача Даних:

- Сенсори та Датчики: використання різноманітних сенсорів та датчиків, які вбудовані в транспортний засіб для збору інформації про стан транспортного засобу та його оточення.

- Модеми та Комунікаційні Модулі: використання модемів та комунікаційних модулів для передачі даних до хмарних платформ.

2. Хмарні Платформи та Системи Зберігання:

- Інтеграція з Хмарними Сервісами: технічні аспекти інтеграції транспортного засобу з хмарними платформами для зберігання та обробки даних.

- Безпека Хмарних Систем: заходи безпеки, що вживаються в хмарних сервісах для захисту переданих даних.

3. Аналіз та Обробка Даних:

- Аналітика та Штучний Інтелект: використання аналітики та штучного інтелекту для обробки великих обсягів даних, що збираються в реальному часі.

- Методи Зведення та Агрегації Даних: технічні аспекти зведення та агрегації даних для отримання цілісного зображення про стан автопарку.

4. Оновлення та Дистанційне Керування:

- Віддалене Оновлення Програмного Забезпечення: технічні аспекти впровадження систем віддаленого оновлення програмного забезпечення для транспортних засобів.

- Дистанційне Керування Функціями: можливості дистанційного керування різними функціями транспортного засобу через хмарні платформи.

Безпека V2C:

1. Шифрування та Захист Передачі Даних:

- SSL/TLS Протоколи: використання шифрування SSL/TLS для захисту передачі даних між транспортними засобами та хмарними платформами.

- VPN-з'єднання: можливість використання VPN-з'єднань для додаткового захисту комунікацій.

2. Управління Доступом та Ідентифікація:

- Механізми Управління Доступом: системи управління доступом для контролю доступу до хмарних платформ та збереження конфіденційності даних.

- Механізми Ідентифікації: механізми ідентифікації для перевірки автентичності транспортного засобу та власника

3. Виявлення та Захист від Кіберзагроз:

- Системи Виявлення Вторгнень: використання систем виявлення вторгнень для реагування на кібератаки та забезпечення безпеки даних.

- Firewall та Антивіруси: файрволи та антивіруси для захисту від несанкціонованого доступу та збереження цілісності даних.

4. Обмеження Доступу до Систем:

- Методи Ізоляції Даних: використання методів ізоляції даних для запобігання несанкціонованому доступу до конфіденційної інформації.

- Ролеве Управління Доступом: ролеве управління доступом для обмеження прав доступу користувачів до різних функцій та даних.

Середньостатистичний підключений автомобіль накопичує і обробляє такий обсяг даних:

1. Дані для розваг та зручності:

- Збір інформації щодо вибору радіостанцій, налаштувань аудіосистеми, вибору режимів кондиціонування тощо.

- Запам'ятовування улюблених маршрутів та налаштувань водійського сидіння.

2. Дані з внутрішніх та зовнішніх датчиків:

- Збирання даних від внутрішніх датчиків, таких як температурні, вологості та датчики давлення.

- Використання зовнішніх камер та датчиків для аналізу дорожньої обстановки та інших об'єктів.

3. Дані з систем безпеки:

- Запис даних з систем безпеки, таких як камери, під час виникнення подій або аварій.

- Збір інформації про реакцію систем безпеки, наприклад, активацію подушок безпеки.

4. Технічний стан автомобіля:

- Відстеження стану різних компонентів транспортного засобу, таких як гальма, паливна система, система охолодження і т. д.

- Відображення на панелі приладів інформації про необхідність технічного обслуговування.

5. Збір даних для страхування:

- Застосування телематичних систем для збору інформації про стиль водіння, відстань та інші параметри для розрахунку страхових внесків.

6. Взаємодія з інфраструктурою доріг:

- Обмін інформацією з іншими підключеними автомобілями та інфраструктурою для оптимізації руху та попередження про можливі небезпеки.

7. Системи автономного водіння:

- Збір даних з лідарів, радарів та камер для реалізації функцій автономного водіння.

- Аналіз оточуючого середовища для безпечного та ефективного керування автомобілем.

8. Підключення до мобільних додатків:

- Забезпечення можливості взаємодії з автомобілем через мобільні додатки для віддаленого керування, відстеження стану автомобіля та інших функцій.

Ця інформація не лише слугує для поліпшення водійського досвіду та зручності, але також може бути використана для вдосконалення безпеки, ефективності та розуміння функціонування автомобіля. Однак важливо звертати увагу на аспекти приватності та кібербезпеки, щоб захистити особисті дані та запобігти можливим загрозам.

3.3 Висновки до розділу 3

Сучасна ситуація в області кіберпідключених автомобілів визначається швидким та невпинним розвитком технологій, що впливає на усі аспекти транспортної індустрії. Кіберпідключені автомобілі, базуючись на Інтернеті речей (IoT) та високотехнологічних системах, стають ключовим елементом трансформації автомобільного сектору.

З одного боку, ця трансформація вносить істотні позитивні зміни, такі як підвищення безпеки на дорозі завдяки системам допомоги водії, автоматизації та адаптивному керуванню. Розширення функціоналу автомобілів за допомогою підключених сервісів, віддаленого керування та інтеграції з іншими елементами IoT робить водіння більш зручним та ефективним.

З іншого боку, із зростанням підключених функцій збільшується ризик кіберзагроз та вразливостей. Потенційні атаки на системи автомобілів можуть впливати на їх безпеку та ефективність. Забезпечення кібербезпеки підключених автомобілів стає найважливішим аспектом для забезпечення безпеки водіїв та пасажирів.

У контексті швидкого розвитку цих технологій, регулятори, виробники автомобілів та інші учасники галузі повинні тісно співпрацювати для

розробки та впровадження стандартів кібербезпеки, які забезпечать стійкість автомобільних систем до сучасних і майбутніх кіберзагроз.

В цілому, сучасна ситуація в області кіберпідключених автомобілів відзначається динамічним розвитком технологій, який вимагає уваги до збалансованого підходу між інноваціями та кібербезпекою для створення безпечних, ефективних та інтелектуальних систем мобільності.

4 ПРОБЛЕМИ ТА ЗАГРОЗИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

[2]Загрози щодо бекенд-серверів, які обслуговують автомобілі під час руху:

1) Зловмисники можуть отримати привілейований чи фізичний доступ до внутрішніх серверів, захистити ці системи виявляється вкрай складно - по суті це шах і мат для захисних систем.

2) Не всі сервери вразливі через різницю у встановлених виправленнях — також відомі випадки, коли чутливі внутрішні сервери були доступні для будь-кого хто хоче отримати доступ через інтернет.

3) Може відбутися витік даних у хмарі, та використовувати їх у своїх цілях може бути непросто, а потенціал шкоди залежить від викрадених даних та ймовірності їх нецільового використання.

4) Злам внутрішнього серверу, кібератака на всю мережу буде вкрай малоймовірною, але знову ж таки не неможливою.

4.1 Система DREAD

Система DREAD є методологією для оцінки ризиків у сфері інформаційної безпеки. Цей підхід допомагає визначити потенційні загрози і оцінити їх вплив на систему чи програмне забезпечення.

Методологію DREAD було представлено в книзі "Writing Secure Code" (Письмовий захист коду), яку написав Майкл Говард разом із Девідом Літтлвудом. Перше видання цієї книги було опубліковано в 2002 році. У книзі розглядаються різні аспекти безпеки програмного забезпечення, і методологія DREAD стала одним з інструментів, щоб допомогти розробникам оцінювати та управляти ризиками в їхніх програмах.

Після цього представлення, DREAD отримала певну популярність в середовищі інформаційної безпеки і використовується як інструмент для оцінки ризиків у розробці програмного забезпечення

Акронім "DREAD" вказує на п'ять ключових аспектів оцінки ризиків:

Damage (Збиток): Оцінює ступінь збитків, які може завдати атака або вразливість. Це включає фінансові втрати, втрату репутації, втрату конфіденційності тощо.

Reproducibility (Відтворюваність): Вказує на те, наскільки легко атаку можна відтворити. Якщо атака легко відтворюється, це підвищує загрозу.

Exploitability (Використаність): Визначає, наскільки легко вразливість може бути використана для здійснення атаки. Використаність висока, якщо атака може бути виконана з легкістю.

Affected Users (Піддалі користувачі): Вказує на кількість користувачів чи систем, які можуть бути засмучені або постраждати через атаку чи вразливість.

Discoverability (Виявленість): Визначає, наскільки легко можна виявити атаку чи вразливість. Якщо вразливість легко виявляється, це збільшує ризик.

Кожному з цих аспектів надається бал від 0 до 10, де 0 - найнижчий ризик, а 10 - найвищий. Після того як кожен аспект оцінено, можна розрахувати загальний ризик.

Система DREAD дозволяє командам інформаційної безпеки об'єктивно оцінювати потенційні ризики і визначати пріоритети для виправлення вразливостей чи впровадження заходів безпеки.

4.2 Оцінка загрози щодо бекенд-серверів, які обслуговують автомобілі під час руху

Top-level threat	Threat Example	D	R	E	A	D	Rating
1. Back-end servers used as a means to attack a vehicle or extract data	1.1 Abuse of privileges by staff (insider attack)	3	3	2	2	2	High
	1.2 Unauthorized internet access to the server	3	2	2	2	2	Medium
	1.3 Unauthorized physical access to the server	3	3	2	2	2	High
2. Services from back-end server being disrupted, affecting the operation of a vehicle	2.1 Attack on back-end server stops it functioning	3	2	2	2	2	Medium
3. Vehicle related data held on back-end server being lost or compromised (data breach)	3.1 Abuse of privileges by staff (insider attack)	3	3	2	2	2	High
	3.2 Loss of information in the cloud	3	2	2	2	2	Medium
	3.3 Unauthorized internet access to the server	3	2	2	2	2	Medium
	3.4 Unauthorized physical access to the server	3	3	2	2	2	High
	3.5 Information breach by unintended sharing of data	3	1	2	2	3	Medium

Рисунок 4.1 - Оцінка загрози щодо бекенд-серверів, які обслуговують автомобілі під час руху [2]

4.3 Загрози щодо каналів зв'язку автомобілів

Загрози щодо каналів зв'язку автомобілів:

1) Атаки Сівіли, коли транспортний засіб імітує кілька інших автомобілів на дорозі, мають обмежений радіус загрози.

2) Підробка повідомлень шляхом видачі себе за іншого (наприклад, повідомлень 802.11P, V2X або GNSS) має бути дуже цілеспрямованою атакою, щоб стати успішною.

3) Для атак на канали зв'язку потрібні висококваліфіковані хакери, а атакувати автопарки дуже складно. Опубліковані тематичні дослідження

віддалених атак на Jeep, Tesla та Mercedes показали, що така атака дуже трудомістка.

4) Зламані або скомпрометовані маршрутизатори Wi-Fi або фемтосоти можуть бути використані для атак типу "людина посередині".

5) Перехоплення інформації, втручання в передачу, моніторинг комунікацій, отримання несанкціонованого доступу до файлів або даних, як правило, є пасивними атаками, що не впливають на безпеку дорожнього руху.

6) Атаки типу «відмова в обслуговуванні» (DoS) або «розподілена відмова в обслуговуванні» (DDoS) можуть завдати широкомасштабних неконтрольованих збитків екосистемі підключених автомобілів.

7) Атаки типу "чорна діра" (blackhole), які блокують сполучення між автомобілями, стають особливо руйнівними в автономних автомобілях, де водії не контролюють ситуацію.

8) Атаки шкідливого ПЗ можуть стати реальною загрозою лише за наявності проміжного ПЗ, що взаємодіє із системами автомобіля.

9) Зламана інфраструктура може бути використана для розповсюдження шкідливих повідомлень від інфраструктури до транспортного засобу (I2V) або V2X. По суті, це атака на екосистему по ланцюжку поставок даних. Це може мати критичне значення.

Загрози для процедури оновлення прошивок під'єднаних автомобілів:

1) Компрометація процедури оновлення програмного забезпечення OTA – це атака на ланцюжок постачання даних.

2) Компрометація локальної та/або фізичної процедури оновлення ПЗ може бути справою рук недобросовісного дилера або інсайдера, що працює у дилерському центрі.

4.4 Загрози для процедури оновлення прошивок під'єднаних автомобілів

Якщо транспортні засоби не оновляться, великої шкоди не буде. Як правило, нова прошивка не буде завантажена в пам'ять і процес оновлення не почнеться, доки не буде завершено повне завантаження та не буде розраховано та перевірено контрольну суму.

Top-level threat	Threat Example	D	R	E	A	D	Rating
12. Misuse or compromise of update procedures	12.1 Compromise of over the air software update procedures	3	2	2	3	1	Medium
	12.2 Compromise of local/ physical software update procedures	3	3	2	2	2	High
	12.3 The software is manipulated before the update process (and is therefore corrupted), although the update process is intact	3	2	2	3	1	Medium
	12.4 Compromise cryptographic keys of software provider to do invalid update	3	2	2	3	1	Medium
13. It is possible to deny legitimate updates	13.1 Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	1	2	3	3	3	High

Рисунок 4.2 - Оцінка загрози для процедури оновлення прошивок під'єднаних автомобілів [2]

4.5 Загрози, пов'язані з людським фактором

Загрози, пов'язані з людським фактором:

Безневинні жертви, яких обманом змушують ненавмисно завантажити шкідливе ПЗ, - це класична атака фішинга. Скомпрометувати головний пристрій руками водія легше, ніж переписати прошивку або встановити шкідливе ПЗ. Будь-яка недбалість у дотриманні встановлених виробником

процедур безпеки під час експлуатації або обслуговування автомобіля може призвести до його компрометації.

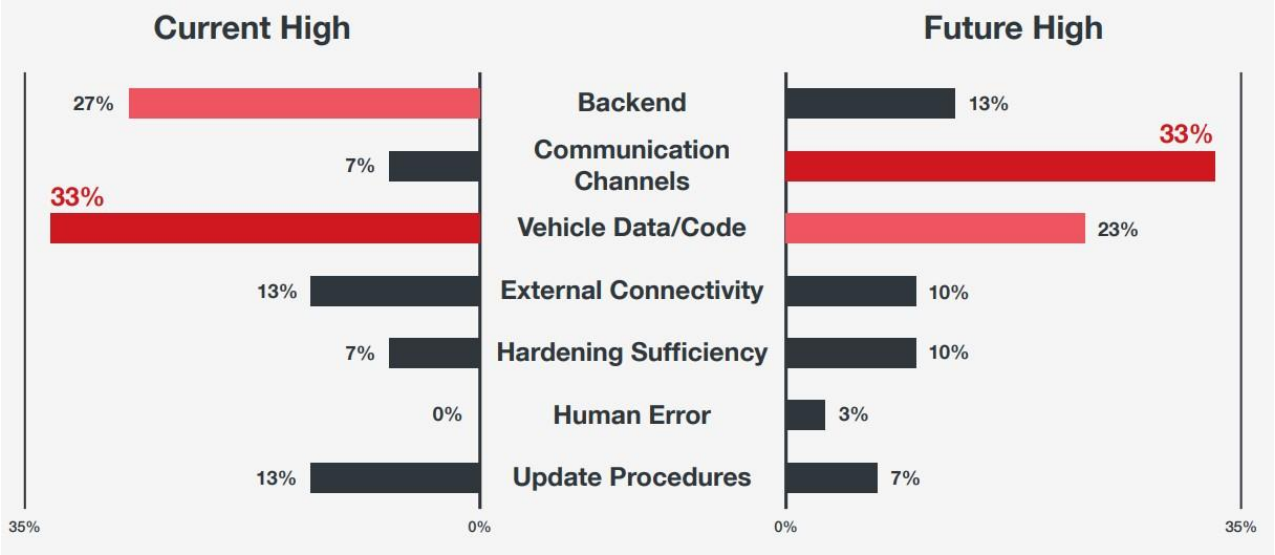


Рисунок 4.3 - Оцінка ймовірності загроз, на цей час і прогнози на майбутнє [2]

У 2015 році два американських IT-експерти продемонстрували потенційний вплив злому на Jeep Cherokee. Вони скомпрометували систему Uconnect, яка поєднує багато електронних функцій автомобіля від інформаційно-розважальної техніки до навігації. Він також служить інтерфейсом для мобільних пристроїв і відкриває точку доступу WLAN за запитом - іншими словами, має IP-адресу. Щоб продемонструвати свою майстерність, двоє хакерів запросили журналіста, якому через деякий час довелося безсило спостерігати, як він втратив контроль над транспортним засобом.

З відстані понад 1000 кілометрів хакери вперше включили кондиціонер і радіо через свій ноутбук. Потім вони бризкали водою зі склоочисників на лобове скло і нарешті просто вимкнули двигун – посеред міждержавної траси (еквівалент європейської автостради). Після цього першого доказу серйозних вразливостей в IT-інфраструктурі транспортних засобів вони навіть пішли трохи далі. На порожній стоянці вони продемонстрували, що можуть навіть

вплинути на кермове керування або відмінити гальма. Наслідками цього стало відкликання 1,4 мільйона транспортних засобів і штраф у розмірі 105 мільйонів доларів

4.6 Висновки до розділу 4

Існуючі загрози у підключених автомобілях стають невід'ємною частиною швидко розвиваючогося світу кіберпростору та Інтернету речей. Сучасні автомобілі, обладнані високотехнологічними системами та підключені до мережі, стають об'єктом потенційних кібератак, що вимагає серйозного уваги до забезпечення кібербезпеки в цьому сегменті транспортної індустрії.

Однією з основних загроз є можливість втручання в роботу автомобільних систем, що може призвести до небезпеки для життя водіїв та пасажирів. Вразливості в програмному забезпеченні та системах зв'язку можуть бути використані для здійснення різноманітних атак, включаючи віддалене керування автомобілем, втручання в системи безпеки та збирання конфіденційної інформації.

Крім того, ризик зловживання даними стає все більш актуальним, оскільки підключені автомобілі збирають та обробляють великі обсяги особистої інформації. Несанкціонований доступ до цих даних може призвести до порушення приватності, ідентифікації та інших негативних наслідків для власників автомобілів.

У світлі цих загроз важливо розглядати кібербезпеку як необхідний елемент при розробці, виробництві та експлуатації підключених автомобілів. Регулярні аудити безпеки, вдосконалення криптографічних методів та розробка стандартів безпеки є важливими кроками у напрямку створення стійких до кіберзагроз автомобільних систем.

Враховуючи постійний розвиток кіберзагроз та інтенсивність їхнього впливу на автомобільну промисловість, необхідно надавати пріоритет

кібербезпеці у всіх аспектах життєвого циклу підключеного автомобіля для забезпечення безпеки та надійності цієї технології.

5 МЕХАНІЗМИ ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ ПІДЛЮЧЕНОГО АВТОМОБІЛЯ

Вирішення проблем кібербезпеки в підключених автомобілях вимагає комплексного підходу, щоб забезпечити ефективний захист від потенційних кіберзагроз. Ось деякі механізми та стратегії для вирішення цих проблем:

5.1 Шифрування трафіку

Застосування механізмів шифрування для захисту комунікаційного трафіку між різними компонентами підключеного автомобіля, такими як контрольна система, сенсори, адаптивні системи та сервери облікових записів.

1)SSL/TLS (Secure Sockets Layer/Transport Layer Security): SSL і його більш сучасний нащадок TLS є протоколами шифрування, які використовуються для захисту комунікацій між різними компонентами автомобільної мережі та зовнішніми серверами чи сервісами. Вони забезпечують шифрування даних та аутентифікацію для забезпечення конфіденційності та цілісності інформації.

2)IPsec (Internet Protocol Security): IPsec використовується для захисту трафіку на рівні мережі. Він може забезпечити шифрування та аутентифікацію даних, які передаються між різними вузлами автомобільної мережі або між автомобільною мережею та іншими мережами.

3)WPA/WPA2/WPA3 (Wi-Fi Protected Access): У випадку використання бездротового зв'язку в підключених автомобілях, протоколи WPA (включаючи WPA2 та WPA3) використовуються для захисту бездротового трафіку. Ці протоколи надають шифрування та аутентифікацію для безпечної комунікації через бездротові мережі.

4)VPN (Virtual Private Network): Використання VPN дозволяє створювати безпечний тунель для передачі даних через неприязненні мережі.

Це може бути важливо для забезпечення конфіденційності та безпеки даних, особливо при використанні зовнішніх мереж або мереж мобільних операторів.

5)MACsec (Media Access Control Security): MACsec забезпечує шифрування на рівні мережевого доступу (Data Link Layer) та використовується для захисту комунікації на рівні фізичного з'єднання в Ethernet-мережах.

5.2 Безпека мережі

Використання захисних мережових протоколів та мережевих архітектур для уникнення несанкціонованого доступу та атак на мережевий рівень.

1) Secured Socket Layer/Transport Layer Security (SSL/TLS):

- Ці протоколи забезпечують шифрування трафіку між клієнтами та серверами для захисту конфіденційності та цілісності даних.
- Використовується для захисту комунікації між різними компонентами в автомобільній мережі та зовнішніми сервісами.

2) IP Security (IPsec):

- IPsec надає безпеку на рівні мережі, включаючи шифрування та аутентифікацію даних, що передаються між різними вузлами автомобільної мережі або між автомобільною мережею та іншими мережами.
- Використовується для захисту трафіку на рівні мережі в автомобільній системі.

3) Controller Area Network Security (CANsec):

- CANsec є набором протоколів та механізмів для захисту мережі CAN (Controller Area Network), яка є широко використовуваною в автомобільній електроніці.
- Забезпечує безпеку та аутентифікацію повідомлень в мережі CAN.

4) Ethernet Security (IEEE 802.1AE MACsec):

- IEEE 802.1AE (MACsec) забезпечує шифрування на рівні мережевого доступу (Data Link Layer) для захисту комунікації в Ethernet-мережах.

- Використовується в автомобільних Ethernet-мережах для захисту від несанкціонованого доступу та атак на рівні фізичного з'єднання.

5) Security Gateway:

- Використовується апаратний чи програмний шлюз безпеки, який фільтрує трафік та виконує інші заходи безпеки між внутрішніми та зовнішніми мережами.

- Захищає автомобільну мережу від несанкціонованого доступу та атак.

6) Intrusion Detection and Prevention Systems (IDPS):

- IDPS виявляє та уникати атаки на мережевому рівні, виявляючи підозрілі дії та блокуючи атаки.

- Застосовується для виявлення та запобігання кіберзагрозам в мережевому середовищі автомобіля.

7) Firewalls:

- Використовується для контролю доступу та фільтрації трафіку між різними частинами мережі.

- Захищає внутрішню мережу від несанкціонованого доступу та зовнішніх атак.

5.3 Оновлення програмного забезпечення

Забезпечення механізмів для регулярного та безпечного оновлення програмного забезпечення в підключених автомобілях для виправлення виявлених вразливостей та підвищення загальної кібербезпеки.

1) Віддалене Оновлення через Інтернет (OTA - Over-the-Air):

- Цей метод дозволяє виробникам автомобілів або постачальникам послуг віддалено встановлювати нове програмне забезпечення на

транспортний засіб через Інтернет без необхідності фізичного відвідування сервісного центру.

- Забезпечує швидке та ефективне оновлення без необхідності відвідування сервісного центру.

2) USB-Оновлення:

- Власники автомобілів можуть завантажити оновлення на флеш-накопичувач та вставити його в порт USB автомобіля для виконання процесу оновлення.

- Дозволяє власникам самостійно виконувати оновлення, але може вимагати фізичного доступу до транспортного засобу.

3) Сервісні Центри та Дилерські Автосервіси:

- Оновлення може бути виконано під час відвідання власником автомобіля сервісного центру чи дилера.

- Забезпечує можливість перевірки інших аспектів транспортного засобу та його обслуговування.

4) Мобільні Додатки:

- Деякі виробники автомобілів можуть надавати оновлення через спеціальні мобільні додатки, які власники можуть встановити на свої смартфони та синхронізувати з автомобілем.

- Зручний спосіб для власників виконувати оновлення та отримувати повідомлення.

5) Автоматичні Оновлення:

- Автомобіль може мати функцію автоматичного оновлення, яка завантажує та встановлює оновлення без втручання власника.

- Забезпечує найбільш беззавдатний спосіб оновлення.

Важливо відзначити, що безпека оновлень програмного забезпечення є критичним аспектом. Виробники автомобілів повинні приділяти особливу увагу заходам безпеки для забезпечення інтегрітету та безпеки транспортного засобу під час оновлень.

5.4 Ідентифікація та аутентифікація

Застосування сильних механізмів ідентифікації та аутентифікації для забезпечення того, що лише авторизовані користувачі та пристрої можуть отримувати доступ до систем автомобіля.

1) Ключі та Карти:

- Власник автомобіля може мати фізичний ключ або смарт-карту, які використовуються для запуску та відкриття транспортного засобу.
- Ідентифікація: Унікальність ключа або карти служить засобом ідентифікації.
- Аутентифікація: Власник представляється автомобілю, використовуючи фізичний ключ або смарт-карту.

2) RFID та NFC Технології:

- Використовуються безконтактні технології, такі як RFID (Radio-Frequency Identification) або NFC (Near Field Communication), для ідентифікації та аутентифікації користувачів.
- Ідентифікація: Унікальний ідентифікатор, що вбудований у RFID-карту чи смартфон, ідентифікує користувача.
- Аутентифікація: Перевірка ідентифікаційного ідентифікатора для надання доступу.

3) Biometric Authentication:

- Використовуються біометричні дані, такі як відбитки пальців, розпізнавання обличчя, для ідентифікації та аутентифікації користувачів.
- Ідентифікація: Біометричні дані унікально ідентифікують конкретного користувача.
- Аутентифікація: Система порівнює представлені біометричні дані зі збереженими для підтвердження особи.

4) Логін та Пароль:

- Класичний метод ідентифікації, що включає введення ім'я користувача та пароля.

- Ідентифікація: Ім'я користувача служить ідентифікатором.

- Аутентифікація: Пароль перевіряється для підтвердження ідентичності.

5) Ключі та Сертифікати для Зв'язку:

- Використовуються ключі та сертифікати для захищеного обміну інформацією між автомобілем та іншими системами (наприклад, хмарними серверами).

- Ідентифікація: Унікальні ключі та сертифікати визначають автомобіль чи систему.

- Аутентифікація: Використовуються для перевірки аутентичності у процесі зв'язку.

Ці методи можуть використовуватися окремо або в комбінації для забезпечення ефективної системи ідентифікації та аутентифікації в підключених автомобілях. Важливо забезпечити надійний та безпечний механізм ідентифікації та аутентифікації для захисту від несанкціонованого доступу.

5.5 Фізична безпека

Забезпечення фізичної безпеки елементів системи, таких як контрольні блоки та сенсори, для уникнення фізичних атак або недозволеного доступу до критичних компонентів.

1) Фізичний Доступ:

- Захищені корпуси та замки для запобігання фізичному доступу до електроніки автомобіля. Крім того, можуть використовуватися механізми для виявлення вторгнень або спроб несанкціонованого доступу.

2) Системи Замків та Запуску:

- Використання безпечних систем запуску та замків, які можуть включати в себе ключі з електронікою, RFID-карти, смартфони або біометричні методи.

3) Автомобільні Камери та Датчики:

- Системи відеоспостереження та сенсори, які можуть виявляти несанкціонований доступ або підозрілу діяльність поблизу автомобіля.

4) Захист Електроніки:

- Застосування захисних корпусів та ущільнень для запобігання втратам або пошкодженням електроніки внаслідок впливу води, пилу, ударів тощо.

5) Захист від Зловживання Даних:

- Фізичні заходи для захисту від зловживання доступу до електронних даних, таких як USB-порти чи роз'єми для читання карт пам'яті.

6) Виявлення та Відповідь на Вторгнення:

- Використання систем виявлення вторгнень, які можуть автоматично викликати захисні заходи в разі виявлення підозрілої або несанкціонованої діяльності.

7) Безпека Системи Дистанційного Керування:

- Додаткові заходи безпеки для систем дистанційного керування, щоб уникнути можливості несанкціонованого доступу через мережі або інші канали.

8) Антивандальність та Антидеструктивність:

- Використання матеріалів та конструкцій, які стійкі до фізичних нападів або деструктивної поведінки.

5.6 Моніторинг та виявлення вторгнень

Розгортання систем моніторингу та виявлення вторгнень для постійного відстеження діяльності в мережі та системі автомобіля та вчасного реагування на будь-які підозрілі події

1) Системи Виявлення Вторгнень (IDS):

- IDS призначені для виявлення підозрілої або аномальної активності в мережі або системі автомобіля.

- Системи IDS можуть використовувати різні методи, такі як сигнатурний аналіз, аномалійний аналіз, і навіть машинне навчання для виявлення нових, раніше невідомих загроз.

2) Системи Захисту від Вторгнень (IPS):

- IPS реагують на виявлені загрози, вживаючи заходів для блокування чи зниження впливу атак.

- Методи IPS може включати в себе фільтрацію пакетів, блокування певних дій або взаємодію з іншими системами для виявлення та ізоляції загроз.

3) Моніторинг Мережевого Трафіку:

- Аналіз та моніторинг мережевого трафіку для виявлення незвичайних змін чи надмірної активності.

- Використання алгоритмів аналізу трафіку для виявлення підозрілого або аномального звертання

4) Логування та Аналіз Журналів:

- Запис і аналіз подій, що сталися в системі, для виявлення незвичайної активності.

- Використання журналів подій для визначення та аналізу нормальної та надмірної системної активності.

5) Моніторинг Фізичних Систем:

- Виявлення незвичайної діяльності або фізичних аномалій в роботі компонентів автомобіля.

- Використання сенсорів, відеокамер та інших фізичних засобів для виявлення змін у роботі системи.

6) Машинне Навчання та Аналіз Поведінки:

- Використання машинного навчання для аналізу та виявлення аномалій в поведінці системи.

- Тренування моделей на базі нормальної поведінки та виявлення відхилень від цієї норми.

5.7 Безпека вбудованого програмного забезпечення

Використання безпечних методів програмування та аудиту вбудованого програмного забезпечення для запобігання вразливостям, які можуть бути використані для кібератак.

1) Кодування та Перевірка Коду:

- Використання надійних методів кодування, відповідність стандартам безпеки програмування. Застосування тестування коду на виявлення можливих вразливостей (статичний та динамічний аналіз).

2) Шифрування Даних:

- Шифрування конфіденційних даних, що передаються між різними компонентами автомобільної системи.

3) Моніторинг та Виявлення Вторгнень:

- Використання систем виявлення вторгнень для виявлення незвичайної або підозрілої активності в системі.

4) Обмеження Доступу:

- Використання принципу менеджменту прав доступу, обмеження привілегій користувачів та системних компонентів.

5) Оновлення та Патчі:

- Регулярне оновлення вбудованого програмного забезпечення для виправлення виявлених вразливостей та усунення можливих проблем безпеки.

6) Білд-Цикл та CI/CD

- Використання процесів білд-циклу та постійної інтеграції/поставки для автоматизації тестування та забезпечення безпеки в процесі розробки.

7) Безпека Входу та Виводу:

- Захист від введення невірних або шкідливих даних через входи, такі як датчики, інтерфейси вводу/виводу, мережеві з'єднання.

8) Використання Захисних Протоколів та Стандартів:

- Використання безпечних мережевих протоколів та дотримання стандартів безпеки, таких як Secure Boot.

9) Фізична Безпека Програмного Обладнання:

- Захист фізичних компонентів вбудованої системи від фізичного доступу, наприклад, захист від вилучення або модифікації елементів.

10) Моніторинг та Логування:

- Системи логування для реєстрації подій та активності системи для подальшого аналізу та виявлення можливих загроз.

Ці стратегії спільно взяті допомагають створити надійний та безпечний екосистему підключених автомобілів, зменшуючи загрози кібербезпеки та забезпечуючи захист для водіїв та пасажирів.

5.8 Висновки до розділу 5

Механізми вирішення проблем кібербезпеки в підключених автомобілях стають важливою ланкою в забезпеченні безпеки та стійкості цих транспортних засобів у світі, де кількість підключених автомобілів стрімко зростає. Засоби забезпечення кібербезпеки повинні ефективно впроваджуватися на різних рівнях, щоб захистити від потенційних загроз та атак.

Одним із ключових механізмів вирішення проблем є розробка та впровадження сучасних стандартів безпеки для підключених автомобілів. Такі стандарти повинні охоплювати всі аспекти кібербезпеки, включаючи захист від несанкціонованого доступу, шифрування даних, виявлення та відповідь на кібератаки.

Крім того, важливо вдосконалювати технічні засоби захисту, такі як системи виявлення вторгнень, фаєрволи, антивіруси та системи моніторингу безпеки мережі. Ці засоби взаємодіють для надійного виявлення та запобігання кіберзагрозам.

Співпраця між виробниками автомобілів, розробниками програмного забезпечення, кібербезпековими експертами та регуляторними органами грає важливу роль у створенні ефективних механізмів вирішення проблем. Обмін інформацією про загрози та вразливості дозволяє створювати швидкі та адаптивні заходи безпеки.

У цьому контексті, наголошення на навчанні та підвищенні кваліфікації фахівців у галузі кібербезпеки стає важливим компонентом ефективних механізмів вирішення проблем. Тільки через постійне вдосконалення та адаптацію можна забезпечити високий рівень захисту підключених автомобілів у світі, що постійно змінюється та еволюціонує в напрямку кібернетичних технологій.

6 РОЛЬ 5G У ПІДКЛЮЧЕНОМУ АВТОМОБІЛІ

6.1 Використання 5G у підключеному автомобілі

[3]Поява автономних мереж 5G (SA), які не залежать від існуючої інфраструктури LTE, зіграє велику роль в екосистемі підключених автомобілів. Таким чином, цілком реально очікувати, що архітектура E/E (Electric/Electronic architecture — електрична/електронна архітектура) розвиватиметься та використовуватиме переваги мереж наступного покоління 5G.

Під архітектурою E/E розуміється об'єднання електронного обладнання, мережевих комунікацій, програмних додатків та електричної проводки в єдину інтегровану систему, яка контролює практично всі функції та елементи транспортного засобу – керування, кузов та безпека, інформаційно-розважальна система, активна безпека та інші функції комфорту , мережеві підключення.

Ключові технології 5G для підключених автомобілів включають:

- програмно-визначені мережі (SDN);
- сегментацію мережі для поділу програм та управління якістю обслуговування (QoS);
- фокусування (beamforming) для швидкого зв'язку;
- додатки 5G для машинного навчання (ML) та штучного інтелекту (AI);
- множинний введення-виведення (MIMO);
- високу доступність (99,999%) та низьку затримку (1 мілісекунда);
- підтримку високої щільності підключених пристроїв та надвисоких швидкостей;
- низьке енергоспоживання.

Підключені автомобілі будуть потребувати дуже низької затримки та високої швидкості передачі даних у великій смузі пропускання. Сегментація

мережі та SDN допоможе відокремити програми з високою швидкістю передачі даних в автомобілі від програм із наднизькою затримкою.

У майбутньому OEM-виробники зможуть перенести деякі функції ЕБУ автомобіля у хмару. Перенесення ЕБУ в хмару дає такі переваги, як спрощення архітектури E/E з меншою кількістю ЕБУ для керування всередині автомобіля та значне збільшення обчислювальної потужності за допомогою хмарних обчислень.

Поява 5G дозволила транспортним засобам стати більш підключеними, ніж будь-коли. Щоб дозволити цій еволюції безпечно проявитися, Всесвітній форум ЄЕК ООН з гармонізації правил щодо транспортних засобів (WP.29) представив Правила ООН № 155 у січні минулого року, і очікується, що понад 54 країни будуть дотримуватися мандату, починаючи з Липня 2022 року.

Цей регламент передбачає 69 векторів атак, які виробники зобов’язані захистити, хоча воно не містить конкретних контрзаходів. Методи безпеки та відповідні технології змінюються з часом, і часто на них впливають технології підключених автомобілів, що розвиваються, а також ландшафт загроз. Запровадження ефективної кібербезпеки означає проведення ретельного аналізу ризиків і визначення пріоритетів того, що необхідно досягти.

6.2 Висновки до розділу 6

Роль 5G у підключених автомобілях визначається як ключовим фактором у розвитку та впровадженні передових технологій в автомобільній промисловості. Введення мереж п'ятого покоління (5G) створює потужний фундамент для реалізації широкого спектру покращень, які впливають на безпеку, комфорт та функціональність підключених автомобілів.

Однією з ключових переваг 5G є висока швидкість передачі даних та низька затримка, що дозволяє в режимі реального часу обмінюватися

великим обсягом інформації між автомобілями та інфраструктурою. Це сприяє впровадженню розумних систем управління рухом, адаптивного керування та інших безпекових функцій, що вимагають миттєвого реагування.

5G також відкриває можливості для розвитку технологій автономного водіння, де величезний потік даних може бути оброблений та проаналізований на високому рівні, що є необхідним для безпечної та ефективної роботи автономних систем.

Забезпечення надійності та безпеки мереж 5G є важливим завданням, оскільки вони стають критично важливими для функціонування підключених автомобілів. Використання високопродуктивних шифрувальних методів, захист від несанкціонованого доступу та інші кіберзаходи стають ключовими компонентами стійкості та безпеки використання 5G в автомобільних мережах.

Загалом, 5G відіграє визначальну роль у реалізації концепції підключеного автомобіля, створюючи інноваційні можливості та покращуючи якість автомобільного досвіду через вдосконалені зв'язки та розширені функції.

7 МІЖНАРОДНІ ТА ГАЛУЗЕВІ СТАНДАРТИ КІБЕРБЕЗПЕКИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

[5]Рішення № 676/2002/ЄС Європейського Парламенту та Ради від 7 березня 2002 року про нормативну базу політики щодо радіочастот у Європейському Співтоваристві. Рада та Європейський парламент наголосили на важливості підвищення безпеки дорожнього руху в Європі. Інтелектуальні транспортні системи (ITS) є центральними в комплексному підході до безпеки дорожнього руху шляхом додавання інформаційно-комунікаційних технологій (ІКТ) до транспортної інфраструктури та транспортних засобів, щоб уникнути потенційно небезпечних ситуацій на дорозі та зменшити кількість аварій.

1) Ефективне та узгоджене використання радіочастотного спектру має важливе значення для розробки нового бездротового обладнання в Співтоваристві

2) ІТС включають кооперативні системи, засновані на комунікаціях між транспортними засобами, транспортними засобами та інфраструктурою та інфраструктурою для передачі інформації в реальному часі. Ці системи потенційно пропонують значні покращення ефективності транспортної системи, безпеки для всіх учасників дорожнього руху та комфорту пересування. Для досягнення цих цілей зв’язок між транспортними засобами та дорожньою інфраструктурою має бути надійним і швидким.

3) Враховуючи мобільність транспортних засобів і необхідність забезпечення досягнення внутрішнього ринку та підвищення безпеки дорожнього руху по всій Європі, спектр, який використовується спільними системами ІТС, повинен бути доступним узгоджено в усьому Європейському Союзі.

4) Відповідно до статті 4 Рішення № 676/2002/ЄС, 5 липня 2006 року Комісія видала мандат Європейській конференції поштових і телекомунікаційних адміністрацій (CEPT) на перевірку вимог до спектру для

критичних для безпеки додатків у контексті ITC і спільних систем, а також провести дослідження технічної сумісності між критичними для безпеки додатками ITC і радіослужбами, які потенційно постраждають у діапазонах частот, що розглядаються. CEPT також було запропоновано розробити оптимальні плани каналів для діапазонів, визначених для ITS.

5) Відповідні результати роботи, проведеної CEPT, становлять технічну основу для цього Рішення

CEPT у своїй доповіді від 21 грудня 2007 р. (Звіт 20 CEPT) зробив висновок, що діапазон 5 ГГц, зокрема діапазон 5 875–5 905 МГц, підходить для пов'язаних з безпекою додатків ITC, які покращують безпеку дорожнього руху шляхом збільшення інформації до водія і транспортного засобу на навколишнє середовище, інші транспортні засоби та інших учасників дорожнього руху. Крім того, ITS сумісні з усіма дослідженими службами в цій смузі, а також з усіма іншими існуючими дослідженими службами на частотах нижче 5 850 МГц і вище 5 925 МГц, якщо вони відповідають певним обмеженням викидів, визначеним у Звіті CEPT. Вибір цієї смуги також відповідатиме використанню спектру в інших регіонах світу і, таким чином, сприятиме глобальній гармонізації.

6) Гармонізований стандарт EN 302 571 завершується Європейським інститутом телекомунікаційних стандартів (ETSI) відповідно до досліджень сумісності CEPT з метою надання презумпції відповідності статті 3(2) Директиви 1999/5/EC Європейського Парламенту та Ради. від 9 березня 1999 р. щодо радіообладнання та телекомунікаційного кінцевого обладнання та взаємного визнання їх відповідності таким чином гарантуючи, що відповідне ITS обладнання запобігає створенню шкідливих перешкод. Очікується, що передавачі ITS максимізуватимуть використання спектру та керують своєю потужністю передачі до мінімального рівня, щоб ефективно використовувати спектр, виділений ITS, щоб уникнути шкідливих перешкод.

7) З наведеної вище причини стандарт передбачає, що регулювання потужності передавача (TPC) реалізується з діапазоном щонайменше 30 дБ з

урахуванням максимальної сумарної потужності передачі 33 дБм середня е.і.м.м. Якщо деякі виробники вирішили не використовувати методи, визначені в У цьому стандарті знадобляться будь-які альтернативні методи, щоб забезпечити принаймні еквівалентний рівень пом'якшення перешкод, який передбачений стандартом.

Автомобільна кібербезпека — це виклик сучасності для виробників автомобілів. Кожен додатковий комунікаційний інтерфейс і компонент є потенційною точкою атаки для кіберзлочинців. Потенціал шкоди від маніпуляцій швидко зростає, наприклад, стосовно автономно керованих транспортних засобів або електронно керованих функцій водіння та гальмування.

З цієї причини Організація Об’єднаних Націй зараз визначає базові рамки для автомобільної кібербезпеки за допомогою двох нових правил. Це кібербезпека UNECE Cyber Security (UN R 155), яка безпосередньо посилається на новий стандарт ISO/SAE 21434, та оновлення програмного забезпечення UNECE Software Updating (UN R 156). Правила стануть обов’язковими для нових типів транспортних засобів вже в липні 2022 року. Тому автомобільна промисловість стикається з серйозними проблемами – особливо через те, що багато виробників оригінального обладнання (OEM) і постачальники критикують нові правила як дуже загальні. Тут широко поширене бажання отримати конкретні рекомендації щодо дій щоб огородитися від ціх проблем.

Хоча міжнародний стандарт ISO 27001 є міжгалузевим підходом до інформаційної безпеки, термін автомобільна кібербезпека описує безпеку цифрових систем в автомобільній промисловості. Наші автомобілі все більше залежать від мережевих електронних систем і програмних додатків. Як наслідок, захист та убезпечення цих компонентів стає все більш важливим – у всій галузі. Це починається з виробника транспортного засобу, продовжується з постачальниками та постачальниками інженерних послуг і поширюється на постачальників програмного забезпечення та

інфраструктури ІСТ. Два нових правила Організації Об’єднаних Націй, спрямовані на виробників та їхніх постачальників, призначені для забезпечення безпеки автомобільних ІТ

ISO 27001 - класика інформаційної безпеки

ISO/IEC 27001 є провідним міжнародним стандартом для впровадження цілісної системи управління інформаційною безпекою.

Сьогодні вибіркових заходів уже недостатньо для цілісного захисту транспортних засобів. Натомість потрібні системні та стратегічні підходи, які визначають чіткі вимоги до обсягу, продуктивності та аудиту системи безпеки. Стратегічний підхід повинен охоплювати весь життєвий цикл продукту. Тут, наприклад, потрібно зосередитися на довгостроковій доступності оновлень програмного забезпечення або на інтеграції всього ланцюжка поставок.

Щоб створити належну основу для автомобільної кібербезпеки, Всесвітній форум з гармонізації транспортних правил (World Forum for Harmonization of Vehicle Regulations) Європейської економічної комісії ООН (UNECE) влітку 2020 року вперше прийняв два обов’язкових правила. Опубліковано під абревіатурами UNECE R 155 та UNECE R 156, правила стосуються ІТ-безпеки та оновлення програмного забезпечення в транспортних засобах, і, таким чином, тісно пов’язані між собою.

Положення набули чинності на початку 2021 року. З липня 2022 року їх дотримання стане обов’язковим для нових типів транспортних засобів. Виробники, які не відповідають вимогам, зіткнуться з не реєстрацією відповідних типів транспортних засобів. Нарешті, з липня 2024 року правила будуть застосовуватися до всіх нових транспортних засобів.

Регламенти, по суті, вимагають впровадження заходів у чотирьох сферах:

1)Управління кіберризиками для транспортних засобів

2)Захист транспортних засобів відповідно до підходу безпеки за проектом для зменшення ризиків у ланцюжку створення вартост

3)Виявлення та захист від атак у всьому автопарку

4)Надання оновлень програмного забезпечення з точки зору безпеки та запровадження правової основи для ефірних оновлень (O.T.A. - over-the-air updates) програмного забезпечення транспортних засобів

Правила ООН передусім говорять про те, що виробники транспортних засобів повинні виконувати нові вимоги. Однак це включає моніторинг та аудит кібербезпеки по всьому ланцюгу поставок, щоб продемонструвати дотримання правил у будь-який час. Тому виробник зобов'язаний стежити за постачальниками. І тому кібербезпека, швидше за все, вимагатиме від своїх постачальників також впровадження нових стандартів.

Ці два правила застосовуються до легкових автомобілів, мікроавтобусів, вантажівок і автобусів, якщо вони обладнані автоматичними функціями водіння. Ця категорія також включає нові типи автоматизованих капсул, човників або порівнянних транспортних засобів. Крім того, правила також поширюються на причепи, які містять принаймні один електронний блок управління.

7.1 Впровадження CSMS

UNECE R 155 визначає вимоги щодо захисту транспортних засобів від кібератак. Ключовим моментом тут є впровадження системи управління кібербезпекою (CSMS) у всіх компаніях, які виставляють транспортні засоби на ринок. Цікавим є те, що ця вимога змінює погляди виробників. Їхня діяльність з розвитку більше не закінчується з початком виробництва (SOP - start of production). Натомість існує постійне зобов'язання перевіряти системи безпеки протягом усього життєвого циклу транспортного засобу, включаючи будь-які необхідні вдосконалення.

Таким чином, законодавець враховує високодинамічний характер розробки програмного забезпечення та забезпечення програмного забезпечення. Крім того, система управління призначена для забезпечення

відповідності вимогам безпеки по ланцюжку поставок. Це непросте завдання з огляду на той факт, що на даний момент на постачальників припадає понад 70 відсотків обсягу програмного забезпечення. Щоб забезпечити наскрізну безпеку, незважаючи на ці складнощі — від розробки до готового автомобіля на дорозі — важливо думати про CSMS цілісно. Крім того, транспортні засоби повинні бути розроблені на основі підходу «безпека за проектом». Намір з самого початку зробити шлюз для зловмисників якомога меншим.

Основними характеристиками CSMS є:

1) Управління ризиками: організація використовує процеси для виявлення, оцінки та зменшення ризиків від кіберзагроз.

2) Управління ризиками охоплює весь життєвий цикл продукту - від розробки до етапу експлуатації у кінцевого споживача.

3) Моніторинг нових вразливостей і відомих атак для відповіді новими оновленнями.

4) Дозволяє незалежну оцінку акредитованим інститутом тестування.

Важливий плюс на практиці: систематизація кібербезпеки, яка супроводжується запровадженням CSMS, робить обов’язковим для компаній вирішувати питання інформаційної безпеки у ризик-орієнтований спосіб. Це включає повне визначення та оцінку ризиків, а також продумування ймовірності їх виникнення. Ця оцінка ризику забезпечує надійну відправну точку для зниження конкретної потенційної шкоди до прийнятного рівня – перевірений і прагматичний підхід.

Система управління кібербезпекою (CSMS) відноситься до систематичного підходу, що ґрунтується на ризиках, для встановлення організаційних процесів, відповідальності та керівництво в управлінні ризиками, пов’язаними з кіберзагрозами для транспортних засобів, та захисту транспортних засобів від кібератак.

Оскільки повністю автономні транспортні засоби також будуть брати участь у транспорті в найближчому майбутньому, надзвичайно важливо підтримувати програмне забезпечення автомобіля належним чином і постійно оновлювати його, наприклад, за допомогою виправлення помилок або оновлень. Таким чином, R 156 наказує запровадження та функціонування відповідної стандарту Системи керування оновленням програмного забезпечення (SUMS - Software Update Management System) для всіх транспортних засобів. Він призначений для забезпечення постійної безпеки протягом усього життєвого циклу транспортного засобу.

Навіть через багато років чи десятиліть має бути можливість безпечно та надійно встановлювати оновлення. Крім того, R 156 закладає юридичну основу для так званих "повітряних" оновлень (O.T.A.), які дозволяють оновлювати транспортні засоби в короткі терміни в будь-який час, незалежно від їх розташування.

Правила ООН № 156 - Уніфіковані положення щодо затвердження транспортних засобів щодо оновлення програмного забезпечення та системи керування оновленням програмного забезпечення [2021/388].

Для порівняння, нинішні виробники мобільних телефонів дають мало впевненості щодо того, скільки майбутніх поколінь програмного забезпечення вони підтримуватимуть або протягом яких періодів часу на старі пристрої все ще будуть надаватися оновлення безпеки. Якщо виробники мобільних телефонів, які схильні до IT, хочуть уникнути проблем, пов’язаних із життєвим циклом своєї продукції, якомога раніше, то це чітко свідчить про проблеми, пов’язані з IT, з якими зараз стикається автомобільна промисловість у зв’язку з тривалим життєвим циклом продукції.

Згідно з правилами ЄС, виробники повинні завжди забезпечувати функціональність своїх систем управління та детально документувати статус всього свого програмного забезпечення

Щоб забезпечити сертифікований стандарт функціональності CSMS, Міжнародна організація зі стандартизації (ISO) разом із Товариством

автомобільних інженерів (SAE) опублікували ISO/SAE 21434 у серпні 2021 року. У професійних колах очікується, що ISO/SAE 21434 стане основою, визнаною органами сертифікації для впровадження системи управління кібербезпекою у виробника транспортних засобів.

Німецька асоціація автомобільної промисловості (VDA) створила додаткову основу для тестування цього стандарту, яку виробник транспортного засобу може використовувати для перевірки CSMS свого постачальника або постачальника інженерних послуг. Таким чином, CSMS виробника може мати позитивний ефект у сенсі правил UNECE аж до рівня постачальника.

Для сертифікації системи керування оновленням програмного забезпечення стандартом має стати ISO 24089. Однак на даний момент (січень 2022 року) дизайн цього стандарту все ще відкритий.

7.2 Диференціація від TISAX

TISAX є процедурою тестування інформаційної безпеки в автомобільній промисловості. І подібно до атестації, виконання вимог можна підтвердити через оцінку. Однак TISAX в першу чергу орієнтований на постачальників послуг або постачальників в автомобільній промисловості, які повинні довести своїм клієнтам, що вони відповідають певним вимогам інформаційної безпеки. Одним із прикладів є безпечна обробка даних та інформації, наданих постачальнику замовником для процесу розробки та виробництва, наприклад. ISO/SAE 21434, з іншого боку, спрямований на виробників транспортних засобів, тобто на виробників оригінального обладнання (OEM).

ISO/SAE 21434 як засіб підвищення репутації

Підхід ISO 21434, аналогічний загальноприйнятим системам менеджменту, таким як ISO 27001, вимагає впровадження процесів і процедур з урахуванням визначених ризиків.

Заявленою метою стандарту є забезпечення безпеки всіх електричних і, перш за все, електронних систем обробки даних протягом усього життєвого циклу продукту транспортного засобу, аж до його утилізації. При цьому він прагне стати загальновизнаним та обов'язковим стандартом якості для кібербезпеки в автомобільному секторі.

Щоб задовольнити цей цілісний підхід, стандарт визначає CSMS для сфер проектування безпеки, розробки продуктів, обслуговування продукту, виявлення ризиків, зменшення небезпеки, утилізації продукту та пов’язаних з ними поточних процесів. Він також включає положення щодо відповідальності у разі розподіленої розробки продуктів між виробниками та постачальниками, без прописування конкретних технологій чи рішень у конкретних термінах.

Виробники та постачальники транспортних засобів не повинні розглядати впровадження стандарту ISO 21434 як додатковий тягар для свого щоденного бізнесу. Навпаки, сертифікація пропонує реальну додану вартість у багатьох сферах – ключових словах: кіберстрахування, кібервідповідальність та ринкова репутація. У результаті вони іноді навіть можуть стати конкурентною перевагою. Зрештою, найсучасніша IT-безпека, підтверджена незалежними експертами, і підтверджений захист даних все частіше вважаються важливими якісними характеристиками в галузі.

IATF 16949

Автомобільна промисловість прагне до відмінної якості процесу, постійного вдосконалення, найвищих стандартів та інновацій. IATF 16949 є стандартом для систем управління якістю постачальників в автомобільній промисловості.

TISAX є загальноприйнятою процедурою тестування та обміну для автомобільного сектора. Він заснований на опитувальнику «ISA – Information Security Assessment» (Оцінка інформаційної безпеки), розробленому Німецькою асоціацією автомобільної промисловості (VDA). Це, у свою

чергу, містить основні аспекти міжнародного стандарту ISO/IEC 27001 і розширює їх за допомогою моделі зрілості.

ISO 26262

Реалізація стандарту призначена для забезпечення функціональної безпеки системи з електричними або електронними компонентами в автомобілі. Стандарт складається з дванадцяти частин:

Частина 1: Словниковий запас,

Частина 2: Управління функціональною безпекою,

Частина 3: Етап концепції,

Частина 4: Розробка продукту на системному рівні,

Частина 5: Розробка продукту на апаратному рівні,

Частина 6: Розробка продукту на рівні програмного забезпечення,

Частина 7: Виробництво, експлуатація, обслуговування та виведення з експлуатації,

Частина 8: Допоміжні процеси,

Частина 9: Аналіз, орієнтований на рівень цілісності автомобільної безпеки (ASIL) і орієнтований на безпеку,

Частина 10: Інструкції щодо ISO 26262,

Частина 11: Інструкції із застосування ISO 26262 до напівпровідників

Частина 12: Адаптація для мотоциклів.

ISO 26262-1(bis 12):2018-12 - Дорожні транспортні засоби - Функціональна безпека.

Каталог вимог UNECE широкий і на перший погляд може бути вражаючим. Наступні три контрольні списки повинні дати стислий огляд правил - і перше враження про те, чи існуючі системи управління вже відповідають правилам UNECE.

7.3 Вимоги до автовиробників

Відповідно до Положення UNECE про кібербезпеку та системи управління кібербезпекою, для того, щоб отримати схвалення типу, виробники повинні відповідати наступним вимогам.

1)Вимоги до Системи управління кібербезпекою (CSMS)

2)CSMS є на місці, і його можна застосовувати на етапах розробки, виробництва та пост-виробництва дорожніх транспортних засобів.

3)Аналіз оцінки ризиків виконується і служить своїй меті.

4)Визначено заходи щодо зниження ризиків.

5)Функціональність пом'якшення ризиків можна перевірити шляхом тестування.

6)Вживаються заходи для виявлення та захисту від кібератак.

7)Криміналістична експертиза методичних даних дозволяє аналізувати успішні атаки.

8)Застосовані заходи для підтримки можливостей моніторингу відповідних загроз, вразливостей та кібератак.

9)Виробник транспортного засобу звітує перед органом із затвердження принаймні один раз на рік.

Відповідно до Положення UNECE щодо оновлень програмного забезпечення та систем керування оновленням програмного забезпечення, для того, щоб отримати схвалення типу, виробники повинні відповідати наступним вимогам.

1)Вимоги Системи керування оновленнями програмного забезпечення

2)Створена система керування оновленням програмного забезпечення, яку можна застосувати до дорожніх транспортних засобів.

3)Виробник повністю документує оновлення.

4)Механізм доставки оновлень захищений від несанкціонованого доступу, а цілісність і автентичність оновлень можна гарантувати.

5)Ідентифікаційні номери програмного забезпечення або версії програмного забезпечення захищені від несанкціонованої зміни.

6)Ідентифікаційний номер програмного забезпечення читається з автомобіля через інтерфейс.

Вимоги до бездротового оновлення програмного забезпечення:

1)Функція відновлення існує, якщо оновлення не вдається.

2)Програмне забезпечення оновлюється лише за наявності достатньої потужності джерела живлення.

3)Безпечне виконання оновлень може бути гарантовано.

4)Користувачі отримують сповіщення про кожне оновлення та про його завершення.

5)Оновлення виконуються лише тоді, коли автомобіль здатний це робити (наприклад, деякі оновлення неможливо виконати під час руху).

6)Користувачі інформуються, коли потрібен механік.

Інформаційна безпека та захист даних – це складні питання, які виходять далеко за межі IT-безпеки. Вони охоплюють технічні, організаційні та інфраструктурні аспекти та стосуються вимог законодавства. Система управління інформаційною безпекою (ISMS - information security management system) відповідно до ISO/IEC 27001 підходить для ефективних захисних заходів, і вона може бути ідеально доповнена системою управління конфіденційною інформацією (PIMS - privacy information management system) відповідно до ISO/IEC 27701. ISO 21434, у свою чергу, може стати основою для системи управління кібербезпекою (CSMS - Cyber Security Management System), яка незабаром знадобиться органам ліцензування.

7.4 Висновки до розділу 7

Міжнародні та галузеві стандарти кібербезпеки для підключених автомобілів є критично важливими компонентами для забезпечення стандартів безпеки та стійкості в цьому швидкорозвиваючому сегменті

транспортної індустрії. Ці стандарти визначають нормативи та вимоги, які виробники та розробники повинні враховувати при розробці, виробництві та експлуатації підключених автомобілів.

Міжнародні стандарти, такі як ISO/SAE 21434 та ISO 27001, надають рамки та методології для впровадження ефективних систем управління кібербезпекою та врахування кіберризиків на різних етапах життєвого циклу автомобіля. Ці стандарти сприяють створенню єдиної системи, яка дозволяє розробникам та виробникам враховувати кібербезпеку від початкового проектування до виходу автомобіля на дороги.

Галузеві стандарти, такі як SAE J3061, спеціально орієнтовані на автомобільну галузь та надають конкретні вимоги та рекомендації для забезпечення безпеки в автомобільних системах. Ці стандарти враховують особливості транспортної індустрії та визначають вимоги до кібербезпеки, які враховують специфіку автомобільних мереж та екосистем.

Налагодження співпраці між міжнародними та галузевими стандартами є ключовим елементом успішного впровадження норм безпеки в автомобільні технології. Спільні зусилля у розробці та підтримці стандартів сприяють створенню єдиної та універсальної системи безпеки, яка враховує виклики та ризики підключених автомобілів на глобальному рівні.

Загалом, ці стандарти визначають керовані та структуровані підходи до кібербезпеки, що є критичними для забезпечення довіри споживачів, ефективної роботи автомобілів та запобігання потенційним кіберзагрозам у цьому важливому секторі транспортної індустрії.

8 ПРОБЛЕМИ СЕРТИФІКАЦІЇ ПІДЛЮЧЕНОГО АВТОМОБІЛЯ

[8] За останні десятиліття у світі була створена безліч систем та оціночних стандартів, які застосовуються для сертифікації інформаційної та кібербезпеки. Системи та стандарти сертифікації знаходять здебільшого в галузевих схемах сертифікації, рідше в національних схемах і деякі з них, наприклад SOG-IS, групами країн. Таке різноманіття створює потужні технічні бар'єри у визнанні відповідних оцінок (сертифікатів). Крім того, у більшості випадків існування або використання різних вимог і процедур у тих секторах, які функціонують як глобальні і комплексні сфери, може являти собою підвищений ризик.

У світі останні 20 – 25 років з метою усунення технічних бар'єрів для визнання оцінок відповідності та сертифікатів створена глобальна система, яка створює умови для взаємного визнання сертифікатів. Ця система – акредитація органів з оцінки відповідності (далі – ООВ), до яких відносяться й органи з сертифікації. Акредитація ООВ сьогодні є невід'ємною частиною процесів надання довіри до результатів сертифікації в будь-якій сфері. У сучасному технічному регулюванні акредитація є одним з основних інститутів інфраструктури, поряд зі стандартизацією та метрологією.

Спорідненими схемами оцінки відповідності для сертифікації кібербезпеки ІКТ для України (далі – схеми сертифікації) можуть бути різноманітні застосування процедур оцінки відповідності, залежно від умов сертифікації в кіберпросторі, ризиків для суспільства і громадян, відношення до певних ІКТ технологій (наприклад, хмарні сервіси) тощо.

У схемах сертифікації слід використовувати певні правила, процедури та менеджмент, які можуть бути притаманні лише даній схемі або які можуть бути визначені у системі сертифікації продукції, яка застосовується до низки схем. Система сертифікації повинна створюватись з врахуванням всіх важливих факторів та умов. Що стосується сертифікації кібербезпеки для України, серед них необхідно виділити три системоутворюючих фактори:

- необхідність дотримання вимог Угоди Україна

- ЄС та статті 56 цієї Угоди;

- підписанні Угоди про визнання у сфері акредитації органів з сертифікації;

- наявність в ЄС Регламенту 2019/881 щодо сертифікації кібербезпеки, основні засади якого з часом повинні будуть імплементовані в Національну систему кібербезпеки України. Система сертифікації кібербезпеки повинна охопити наступні елементи, які, утворюючи одне ціле, знаходяться у відносинах і зв'язках один з одним:

- вимоги для оцінювання (стандарти чи інші нормативні документи);

- акредитація ООВ;

- механізми взаємного визнання сертифікатів (Угоди про визнання);

- управління системою сертифікації кібербезпеки; рівні гарантій сертифікатів кібербезпеки;

- наявність регулятора (Національного органу з сертифікації кібербезпеки).

- призначення органів з сертифікації кібербезпеки.

Для створення дієвої та гнучкої Системи сертифікації кібербезпеки України, яка в майбутньому буде складатись з низки схем сертифікації кібербезпеки для ефективного реагування викликам з кібербезпеки, потрібно перш за все систематизувати два основних елементи Системи:

- вимоги для оцінювання (принципи посилань на стандарти чи інші нормативні документи);

- механізми взаємного визнання сертифікатів (Угоди про визнання).

Це можливо шляхом введення уніфікованих моделей, які базуються на глобальних механізмах усунення технічних бар’єрів у торгівлі та сучасному стані системи технічного регулювання України:

- ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки;

- ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки.

8.1 Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки

Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки (далі – Модель Стандартів). Модель дозволяє упорядити визначення та застосування стандартів чи інших нормативних документів, стандартів та схем з можливими комбінаціями для розробки схем сертифікації.

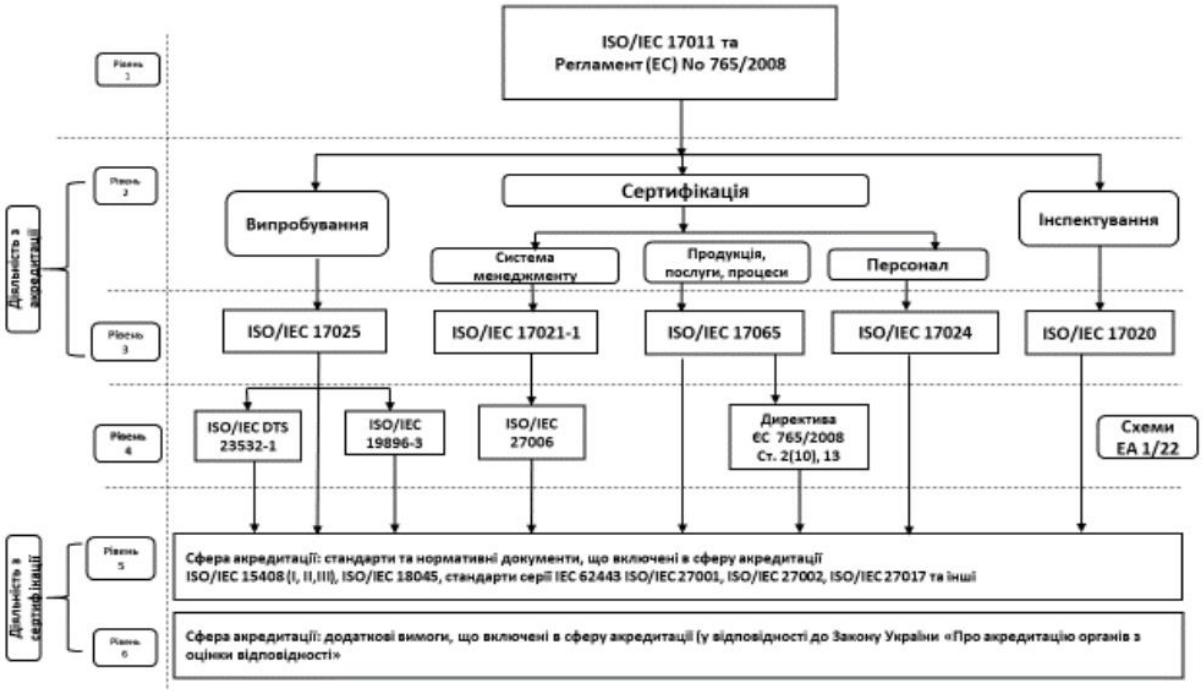


Рисунок 8.1 - Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки[8]

Модель складається з 6 рівнів, системне розподілення оціночних стандартів за якими створює гнучкість для розробників схем сертифікації кібербезпеки.

1 рівень – вимоги до органів з акредитації, які акредитують органи, задіяні в сертифікації кібербезпеки. Визначені у стандарті ISO/IEC 17011, в Регламенті (ЄС) 765/2008 та, якщо необхідно, додаткові вимоги, визначені в обов'язкових документах EA та в документах IAF та/або ILAC (затверджених EA як обов'язкові для ЄС)

2 рівень – діяльність з оцінки відповідності ООВ, яким органи акредитації надають акредитацію відповідно до стандартів, включених до рівня 3 (далі – діяльність з оцінки відповідності). Це, як правило, визначається у схемі сертифікації. Для сертифікації кібербезпеки в цій Системі, залежно від схеми сертифікації, можуть бути задіяні: органи сертифікації продукції, послуг та процесів; органи з сертифікації систем менеджменту; органи з сертифікації персоналу; випробувальні лабораторії; органи з інспектування.

3 рівень – гармонізовані стандарти (або інші нормативні документи), що містять загальні вимоги до ООВ, що виконують діяльність з оцінки відповідності кібербезпеки, включених до рівня 2 (далі – стандарти оцінки відповідності). Це наступні оціночні стандарти: ISO/IEC 17025; ISO/IEC 17020; ISO/IEC 17065; ISO/IEC 17021-1; ISO/IEC 17024. 4 рівень – документи, що містять додаткові критерії до стандартів 3-го рівня

4 рівень застосовується лише там, де існують документи, що доповнюють стандарти 3-го рівня (це означає, що рівень 5 часто безпосередньо пов'язаний зі стандартом рівня 3). Такими документами для ЄС є: галузеві стандарти або інші нормативні документи (далі – галузеві стандарти); галузеві схеми, як зазначено у Регламенті (ЄС) 765/2008 Статті 2 (10) та 13; схеми оцінки відповідності згідно з EA-1/22 (далі – схеми). Так, галузевим стандартом, який без сумнівів буде у Системі, є ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for

bodies providing audit and certification of information security management systems. Також високоймовірним є присутність у Системі сертифікації кібербезпеки Додаткових критеріїв з Регламенту ЄС 2019/881.

5 рівень – сфера акредитації органу з сертифікації: стандарти або інші нормативні документи, що використовуються акредитованим ООВ відповідності для визначеної акредитованої сфери оцінки відповідності. Може включати, наприклад, конкретні методи випробувань та конкретні вимоги до системи управління (наприклад: ISO/IEC 27001), критерії кібербезпеки (ISO/IEC 15408), методику оцінки кібербезпеки (ISO/IEC 18045) тощо.

6 рівень – сфера акредитації органу з сертифікації: додаткові вимоги до сфери акредитації, які можуть бути встановлені в державі. Визначені в законі України «Про акредитацію органів з оцінки відповідності»

8.2 Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки

Запропонована 6-рівнева Ієрархічна Модель оціночних стандартів Системи Сертифікації кібербезпеки є інструментарієм, який надає можливість створення гнучких схем сертифікації кібербезпеки з забезпеченням транскордонного визнання результатів оцінки відповідності у сфері кібербезпеки (випробування та сертифікації). Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки повинна відображати рівні й обсяг визнання з боку міжнародних організацій з акредитації, досяжність яких Національним органом України з акредитації ООВ визначає й обсяг визнання результатів сертифікації кібербезпеки, формуючи механізми взаємного визнання сертифікатів для Системи сертифікації кібербезпеки. Чотирирівнева Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки (MLA для IAF і MRA ILAC), де на національному рівні представлений Національний орган України з акредитації – Національне

агентство з акредитації України (далі – НААУ). В моделі присутні національний, регіональний, міжнародний та глобальний рівні, надані відповідними організаціями з акредитації та типами Угод про визнання. Для оперування моделлю при розробці Системи необхідним додатком є самі Угоди та визначені в них сфери визнання діяльності з акредитації. Модель має методологічне значення та дозволяє при розробці Системи та схем сертифікації кібербезпеки визначатись зі змістом відповідних розділів щодо оціночних стандартів, рівнів гарантій сертифікатів кібербезпеки, акредитації ООВ, взаємного визнання сертифікатів тощо.

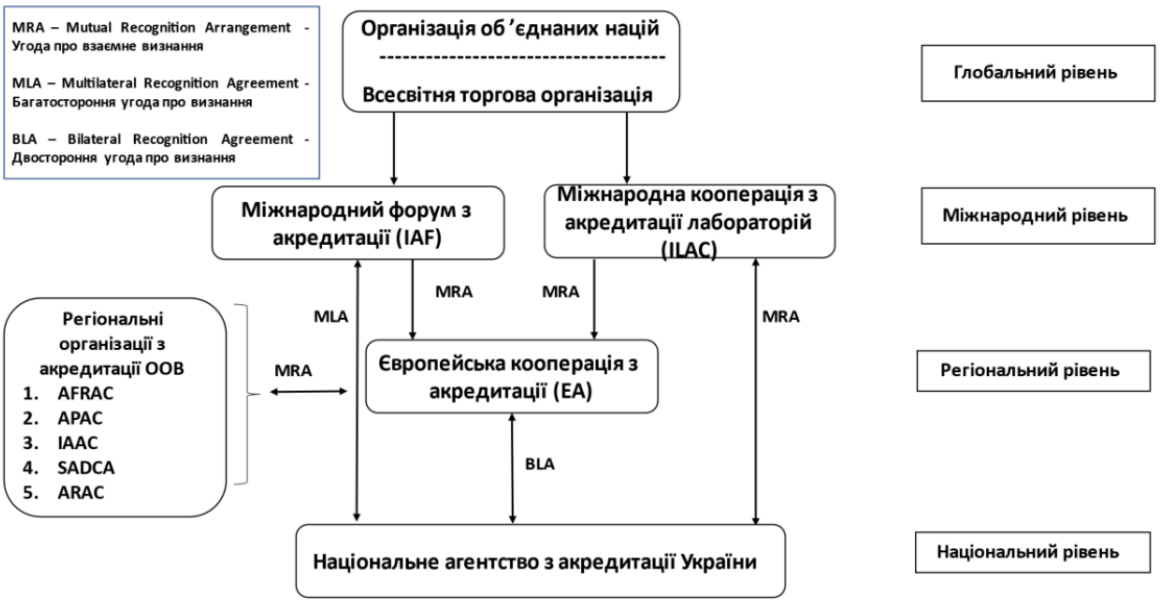


Рисунок 8.2 - Ієрархічна Модель Угод про взаємне визнання сертифікатів кібербезпеки[8]

Для створення ефективної Системи Оцінки Відповідності Кібербезпеки ІКТ України доцільним є аналіз Угод, які є чинними для НААУ у системі ЕА та IAF/ILAC. Слід зазначити, що такий аналіз може дати наступні важливі сценарії для імплементації Системи сертифікації в Національну систему кібербезпеки України:

- наявність Угод достатня для створення Системи та Схем сертифікації відповідно до міжнародних стандартів і стандартів ЄС та НАТО

- наявність Угод недостатня і потребує додаткових зусиль з боку України та НААУ в напрямку розширення сфер визнання у системі ЕА та IAF/ILAC;

- наявність Угод недостатня і потребує створення Системи на національному чи галузевому рівнях без намірів на транскордонне визнання результатів сертифікації, але відповідно до міжнародних стандартів і стандартів ЄС та НАТО. Там же надані витяги з сайтів ILAC та IAF з зазначенням сфер акредитації, які охоплені відповідними Угодами. Аналіз діючого статусу Угод НААУ та сфер акредитації, в яких ці Угоди діють, надає можливість виділити можливі оціночні стандарти та інші стандарти для наповнення Моделі Стандартів та формування Системи сертифікації кібербезпеки.

1. Вимоги для оцінювання (стандарти чи інші нормативні документи). Сертифікат кібербезпеки повинен надаватися після успішної оцінки належним чином з застосуванням відповідних Схем сертифікації. Це може бути сертифікація органом, акредитованим на відповідність вимогам стандарту ISO/IEC 17065 та з залученням лабораторії, акредитованої згідно зі стандартом ISO/IEC 17025. Залежно від рівня гарантій, схема сертифікації кібербезпеки повинна вказувати, чи слід видавати сертифікат кібербезпеки приватним чи державним органом. Схеми сертифікації кібербезпеки базуються (сфера сертифікації) на загальних Критеріях та розглядають питання сертифікації кібербезпеки на основі: загальних Критеріїв - ISO/IEC 15408; загальній Методології Оцінки Безпеки Інформаційних Технологій – ISO/IEC 18045. Схеми сертифікації кібербезпеки можуть передбачати проведення оцінки відповідності під виключною відповідальністю виробника або постачальника продуктів ІКТ.

2. Акредитація органів з оцінки відповідності (сертифікації). Після того, як буде прийнята схема сертифікації кібербезпеки, виробники або

постачальники продуктів ІКТ повинні мати можливість подавати заявки на сертифікацію своїх продуктів ІКТ до ООВ на їх вибір. ООВ повинні бути акредитовані національним органом з акредитації. Національні органи з акредитації повинні обмежувати, призупиняти або анулювати акредитацію ООВ, якщо умови акредитації не виконуються.

3. Механізми взаємного визнання сертифікатів (угоди про визнання). З метою подальшого сприяння торгівлі та визнання того, що ланцюжки постачання ІКТ є глобальними, Україна може укласти угоди про взаємне визнання сертифікатів кібербезпеки. Кожна схема сертифікації кібербезпеки даної Системи сертифікації кібербезпеки повинна передбачати конкретні умови для таких угод про взаємне визнання з третіми країнами. Тому, система сертифікації кібербезпеки України повинна передбачати участь в Угоді про взаємне визнання результатів оцінки відповідності, яка базується на Регламенті ЄС № 2019/881 .

4. Управління системою сертифікації кібербезпеки. Управління Системою сертифікації кібербезпеки враховує належне залучення зацікавлених сторін та встановлює роль органу чи органів управління (далі – Орган управління) під час планування та пропонування, запитування, підготовки, прийняття та перегляду схем сертифікації кібербезпеки. Орган управління системою сертифікації кібербезпеки створюється регулятором (національним органом влади) чи за його погодженням. Орган управління повинен створити Робочу програму для створення та, за необхідністю, адаптацію розроблюваних Схем сертифікації кібербезпеки. Робоча програма повинна бути базовим документом, який дозволяє промисловості, національним органам влади та органам стандартизації заздалегідь підготуватися до майбутніх Схем сертифікації кібербезпеки. 5. Рівні гарантій сертифікатів кібербезпеки. Для забезпечення узгодженості системи сертифікації кібербезпеки схема сертифікації кібербезпеки повинна мати можливість визначати рівні гарантій сертифікатів кібербезпеки та декларацій про відповідність, виданих відповідно до цієї схеми. Кожен сертифікат

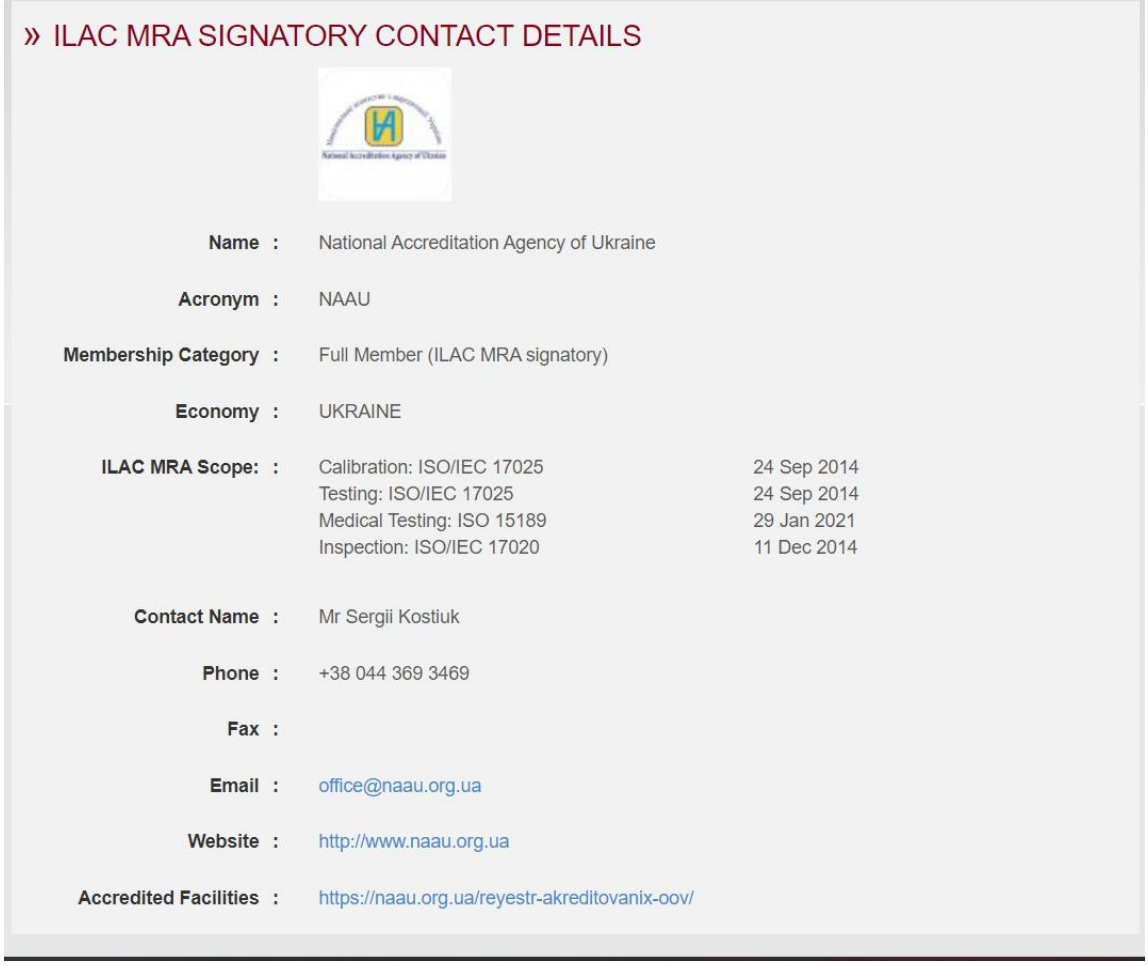
кібербезпеки може посилатися на один із рівнів гарантій: базовий, суттєвий чи високий, тоді як декларація відповідності може стосуватися лише рівня базового.

6. Національні органи з сертифікації кібербезпеки. Цей елемент системи не є обов’язковим, але його доцільність полягає в гармонізації з вимогами Регламенту ЄС 2019/881. Необхідно призначити один або кілька національних органів з сертифікації кібербезпеки для нагляду за дотриманням зобов'язань, що містяться у Системі сертифікації кібербезпеки. Національним органом з сертифікації кібербезпеки може бути існуючий (за наявності) або новий орган. Національний орган з сертифікації кібербезпеки як мінімум повинен: контролювати виконання зобов’язань про відповідність кібербезпеці; допомагати національним органам з акредитації у моніторингу та нагляді за діяльністю органів з сертифікації, надаючи їм досвід та відповідну інформацію.

» ILAC MRA SIGNATORY CONTACT DETAILS

Name :	National Accreditation Agency of Ukraine	
Acronym :	NAAU	
Membership Category :	Full Member (ILAC MRA signatory)	
Economy :	UKRAINE	
ILAC MRA Scope: :	Calibration: ISO/IEC 17025	24 Sep 2014
	Testing: ISO/IEC 17025	24 Sep 2014
	Medical Testing: ISO 15189	29 Jan 2021
	Inspection: ISO/IEC 17020	11 Dec 2014
Contact Name :	Mr Sergii Kostiuk	
Phone :	+38 044 369 3469	
Fax :		
Email :	office@naau.org.ua	
Website :	http://www.naau.org.ua	
Accredited Facilities :	https://naau.org.ua/reyestr-akreditovanix-oov/	

Рисунок 8.3 – Угода MRA та сфера в ILAC



» ILAC MRA SIGNATORY CONTACT DETAILS

Name :	National Accreditation Agency of Ukraine	
Acronym :	NAAU	
Membership Category :	Full Member (ILAC MRA signatory)	
Economy :	UKRAINE	
ILAC MRA Scope: :	Calibration: ISO/IEC 17025	24 Sep 2014
	Testing: ISO/IEC 17025	24 Sep 2014
	Medical Testing: ISO 15189	29 Jan 2021
	Inspection: ISO/IEC 17020	11 Dec 2014
Contact Name :	Mr Sergii Kostiuk	
Phone :	+38 044 369 3469	
Fax :		
Email :	office@naau.org.ua	
Website :	http://www.naau.org.ua	
Accredited Facilities :	https://naau.org.ua/reyestr-akreditovanix-oov/	

Рисунок 8.4 – Угода MRA та сфера в IAF

Цей проект Системи сертифікації кібербезпеки ІКТ для України побудований на попередньому аналізі та баченні ЄС з цього питання, яке викладено в Акті з кібербезпеки ЄС . Як зазначено вище, Система сертифікації формується з 7 основних елементів.

1. Вимоги для оцінювання (стандарти чи інші нормативні документи). Сертифікат кібербезпеки повинен надаватися після успішної оцінки належним чином з застосуванням відповідних Схем сертифікації. Це може бути сертифікація органом, акредитованим на відповідність вимогам стандарту ISO/IEC 17065 та з залученням лабораторії, акредитованої згідно зі стандартом ISO/IEC 17025. Залежно від рівня гарантій, схема сертифікації кібербезпеки повинна вказувати, чи слід видавати сертифікат кібербезпеки

приватним чи державним органом. Схеми сертифікації кібербезпеки базуються (сфера сертифікації) на загальних Критеріях та розглядають питання сертифікації кібербезпеки на основі: загальних Критеріїв - ISO/IEC 15408; загальній Методології Оцінки Безпеки Інформаційних Технологій – ISO/IEC 18045. Схеми сертифікації кібербезпеки можуть передбачати проведення оцінки відповідності під виключною відповідальністю виробника або постачальника продуктів ІКТ.

2. Акредитація органів з оцінки відповідності (сертифікації). Після того, як буде прийнята схема сертифікації кібербезпеки, виробники або постачальники продуктів ІКТ повинні мати можливість подавати заявки на сертифікацію своїх продуктів ІКТ до ООВ на їх вибір. ООВ повинні бути акредитовані національним органом з акредитації. Національні органи з акредитації повинні обмежувати, призупиняти або анулювати акредитацію ООВ, якщо умови акредитації не виконуються.

3. Механізми взаємного визнання сертифікатів (угоди про визнання). З метою подальшого сприяння торгівлі та визнання того, що ланцюжки постачання ІКТ є глобальними, Україна може укласти угоди про взаємне визнання сертифікатів кібербезпеки. Кожна схема сертифікації кібербезпеки даної Системи сертифікації кібербезпеки повинна передбачати конкретні умови для таких угод про взаємне визнання з третіми країнами. Тому, система сертифікації кібербезпеки України повинна передбачати участь в Угоді про взаємне визнання результатів оцінки відповідності, яка базується на Регламенті ЄС № 2019/881 .

4. Управління системою сертифікації кібербезпеки. Управління Системою сертифікації кібербезпеки враховує належне залучення зацікавлених сторін та встановлює роль органу чи органів управління (далі – Орган управління) під час планування та пропонування, запитування, підготовки, прийняття та перегляду схем сертифікації кібербезпеки. Орган управління системою сертифікації кібербезпеки створюється регулятором (національним органом влади) чи за його погодженням. Орган управління

повинен створити Робочу програму для створення та, за необхідністю, адаптацію розроблюваних Схем сертифікації кібербезпеки. Робоча програма повинна бути базовим документом, який дозволяє промисловості, національним органам влади та органам стандартизації заздалегідь підготуватися до майбутніх Схем сертифікації кібербезпеки. 5. Рівні гарантій сертифікатів кібербезпеки. Для забезпечення узгодженості системи сертифікації кібербезпеки схема сертифікації кібербезпеки повинна мати можливість визначати рівні гарантій сертифікатів кібербезпеки та декларацій про відповідність, виданих відповідно до цієї схеми. Кожен сертифікат кібербезпеки може посилатися на один із рівнів гарантій: базовий, суттєвий чи високий, тоді як декларація відповідності може стосуватися лише рівня базового.

6. Національні органи з сертифікації кібербезпеки. Цей елемент системи не є обов’язковим, але його доцільність полягає в гармонізації з вимогами Регламенту ЄС 2019/881 . Необхідно призначити один або кілька національних органів з сертифікації кібербезпеки для нагляду за дотриманням зобов'язань, що містяться у Системі сертифікації кібербезпеки. Національним органом з сертифікації кібербезпеки може бути існуючий (за наявності) або новий орган. Національний орган з сертифікації кібербезпеки як мінімум повинен: контролювати виконання зобов’язань про відповідність кібербезпеці; допомагати національним органам з акредитації у моніторингу та нагляді за діяльністю органів з сертифікації, надаючи їм досвід та відповідну інформацію; призначати ООВ виконувати свої завдання, якщо такі органи відповідають додатковим вимогам, встановленим схемою сертифікації кібербезпеки; слідкувати за відповідним розвитком у галузі сертифікація кібербезпеки.

7. Призначення органів з сертифікації кібербезпеки. Призначення – надання органом, що призначає, ООВ (в тому числі визнаній незалежній організації) права виконувати як третій стороні певні завдання з оцінки відповідності згідно з відповідним технічним регламентом . Вимоги до

призначених органів з сертифікації кібербезпеки повинні бути відповідними вимогам закону України «Про технічні регламенти та оцінку відповідності», який, у свою чергу, гармонізований acquis до законодавства ЄС щодо нотифікованих ООВ. Органи з сертифікації кібербезпеки можуть бути призначені для виконання ними як третіми сторонами певних завдань з оцінки відповідності згідно з відповідними технічними регламентами за умови, що вони відповідають додатковим вимогам, встановленим схемою сертифікації кібербезпеки чи технічним регулятором . Наприклад, мають власні акредитовані випробувальні лабораторії для проведення принаймні деяких видів випробувань продукції ІКТ в межах сфери призначення.

8.3 Схема сертифікації кібербезпеки підключеного автомобіля

Методологічною базою для розробки схем сертифікації кібербезпеки є міжнародний стандарт ISO/IEC 17067:2013 Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes . Повна версія схеми сертифікації, згідно зі стандартом, повинна мати у своєму складі 17 елементів. У статті досліджено та визначені найбільш важливі та системоутворюючі елементи деяких схем сертифікації кібербезпеки. Такі версії схем будемо називати робочими (далі – Схема П1, Схема Х1). Також зазначимо, що дослідження спрямовано на гармонізацію національних схем сертифікації кібербезпеки з імовірними схемами сертифікації кібербезпеки ЄС . Спочатку розглянемо робочу версію Схеми сертифікації кібербезпеки продукції ІКТ (Схема П1). В цій версії визначимо 4 елементи:

1. Предмет та обсяг схеми сертифікації. Схема сертифікації кібербезпеки базується на Загальних Критеріях (Common Criteria або CC) та повинна дозволяти сертифікацію продуктів ІКТ згідно зі стандартом ISO/IEC 15408.

Схема може охоплювати будь-який тип ІКТ-продукту.

Схема повинна охоплювати оцінку вразливостей криптографічних реалізацій до функціональних можливостей безпеки продукту ІКТ відповідно до вимог критеріїв оцінки та методології, визначених у стандарті ISO/IEC 15408.

2. Оціночні стандарти. Оцінки повинні базуватися за такими стандартами: – загальні Критерії Оцінки Безпеки Інформаційних Технологій, відповідно до їх відповідної версії стандарту ISO/IEC 15408 (відомі ще як Загальні Критерії або Common Criteria - CC);

– загальна Методологія Оцінки Безпеки Інформаційних Технологій (відома ще як Загальна Методологія Оцінки або Common Evaluation Methodology - CEM) згідно з її відповідною версією стандарту ISO/IEC 18045. Оцінка також враховує допоміжні елементи, створені для забезпечення гармонізованого тлумачення цих стандартів. Такі елементи повинні бути або обов’язковими допоміжними елементами, інтегрованими як додатки до цієї схеми, або допоміжними документами, що надаються Національним органом з сертифікації кібербезпеки. Крім того, для акредитації ООВ, які виконують діяльність з оцінки та сертифікації, застосовуються такі стандарти:

– ISO/IEC 17065 для ООВ або національного органу, що відповідає за діяльність із сертифікації, надалі визначений органом з сертифікації;

– ISO/IEC 17025 для сторонніх ООВ або національних органів влади, або

субпідрядника ООВ або національних органів, які відповідають за діяльність з оцінки, надалі визначена випробувальною лабораторією

3. Самооцінка відповідності. Схема не дозволяє проводити самооцінку відповідності.

4. Конкретні вимоги, що застосовуються до ООВ. Орган з сертифікації має бути акредитований відповідно до стандарту ISO/IEC 17065. Випробувальна лабораторія, включаючи її персонал, що проводить оцінки

для органу з сертифікації повинна бути технічно компетентною для відповідних завдань. Для рівня гарантій суттєвий – ця технічна компетентність повинна оцінюватися шляхом акредитації випробувальної лабораторії відповідно до стандарту ISO/IEC 17025. Додатково для діяльності лабораторій слід визначити як керівництво схемою та використовувати такі потенційно відповідні стандарти:

– ISO / IEC 19896-3: 2018 Методи IT-безпеки – Вимоги до компетентності для тестувальників та оцінювачів інформаційної безпеки Частина 3: Вимоги до знань, навичок та ефективності для оцінювачів ISO/IEC 15408;

– ISO/IEC DTS 23532-1 Інформаційна безпека, кібербезпека та захист конфіденційності

– Вимоги до компетентності лабораторій випробувань та оцінки IT-безпеки – Частина 1: Оцінка за ISO/IEC 15408. Робоча версія схеми сертифікації кібербезпеки хмарних сервісів (Схема X1) обмежується 1 елементом – визначенням оціночних стандартів. Схема X1 буде базуватись на акредитації органу з сертифікації, використанні Ієрархічних моделей оціночних стандартів Системи сертифікації кібербезпеки і Угод про взаємне визнання сертифікатів кібербезпеки та спиратись на наступну низку стандартів і технічних специфікацій сфери акредитації:

– міжнародні стандарти ISO/IEC 17788, ISO/IEC 17000 та ISO/IEC 27000;

– міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017 ;

– міжнародний стандарт ISO/IEC 15408-3;

– міжнародний стандарт ISO/IEC ISO/IEC 27032 .

Методологія акредитації органу з сертифікації для Схеми X1 буде базуватись на міжнародному стандарті ISO/IEC 17065:2012 Conformity assessment – Requirements for bodies certifying products, processes and services.

8.4 Висновки до розділу 8

Проблеми сертифікації підключених автомобілів визначаються великою мірою швидким розвитком технологій та постійними змінами у сфері кібербезпеки та автомобільних систем. Сертифікація в цьому контексті стає викликом, оскільки необхідно враховувати різноманітні технологічні аспекти та забезпечувати високий рівень безпеки та стійкості підключених автомобілів.

Однією з ключових проблем є нестача єдиної та всеосяжної системи сертифікації, яка б узгоджувала стандарти та вимоги на міжнародному рівні. Різні регіональні та галузеві стандарти можуть викликати ускладнення в процесі сертифікації та призводити до недостатньої узгодженості вимог до безпеки та якості підключених автомобілів.

Ще однією важливою проблемою є динаміка швидкого розвитку технологій. Сертифікаційні органи повинні швидко адаптуватися до нових технологій, враховуючи їхню безпеку та відповідність стандартам. Спрощення та прискорення процесів сертифікації є ключовим елементом у забезпеченні безпеки та розвитку підключених автомобілів.

Також, виникає проблема визначення стандартів та критеріїв для оцінки кібербезпеки, особливо в умовах зростання кількості підключених систем та об'єму зібраної інформації. Визначення обов'язкових стандартів та нормативів, що стосуються якості та безпеки підключених автомобілів, є ключовим завданням для подолання цієї проблеми.

У цілому, вирішення проблем сертифікації підключених автомобілів вимагає тісної співпраці між галузевими гравцями, створення єдиних стандартів, які враховують глобальні та локальні особливості, а також швидкого реагування на зміни в технологічному середовищі та кіберзагрозах.

ВИСНОВКИ

Сучасні автомобілі все більше схожі на високотехнологічні гаджети. Вони напхані комп'ютерами та мультимедійними системами, інтенсивно обмінюються даними з хмарними сервісами, іншими автомобілями та дорожньою інфраструктурою. Цифровізація транспорту додає до звичних небезпек ще й ризики, пов'язані з кіберзагрозами. З кожним роком число підключених автомобілів зростає, так за оцінками експертів до 2026го року більша частина авто буде підключена до мережі. Разом цим росте загроза кібератаки. Виробники транспортних засобів рекомендують своїм клієнтам, не вносити багато особистою інформації до системи свого автомобіля. Та це не змінить того що нагальною потребою для оптимального функціювання всієї системи є швидка та повноцінна сертифікація та стандартизація процесів роботи мережі, побудови платформ та операційних систем що встановлюються в підключених автомобілях. Якщо всі складові системи підключеного автомобіля будуть уніфіковані та систематично оновлюватись, це допоможе уникнути великої кількості кібератак, та кардинально скоротить кількість аварій які зараз, нажаль, є невідємною частиною трафіку на автомобільних дорогах. Хоч технології підключеного автомобіля вже 26 років, та все ж вона далеко не ідеальна і потребує багато роботи для того щоб переміщення автомобільним транспортом стало справді безпечним та захищенним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/
2. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/a-roadmap-to-secure-connected-cars
3. https://habr.com/ru/company/trendmicro/blog/590209/
4. https://energycommerce.house.gov/hearings-and-votes/hearings/vehicle-vehicle-communications-and-connected-roadways-future
5. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0671
6. https://legalitgroup.com/gdpr-ta-avtopilot/
7. https://ev-auto.ru/naskolko-vazhna-kiberbezopasnost-sovremennogo-avtomobilya
8. УДК 004.056 СИСТЕМА СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ Цвілій О.О.
9. https://www.automaster.net.ua/artykuly/zabezpechennya-bezperervnogo-obminu-danimi-mizh-avtomobilyami-ta-inshimi-uchasnikami-dorozhnogo-ruhu,51800?wyslij=51800
10. https://uk.avtotachki.com/sistemy-navigaczii-avtomobilya/
11. https://auto.24tv.ua/avtopilot_otsiniuiemo_riven_samostiinosti_avtomobilia_n2355
12. https://af.khadi.kharkov.ua/fileadmin/F-AUTOMOBILE/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%BE%D0%B1%D1%96%D0%BB%D1%96%D0%B2/%D0%9D%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D1%96_%D0%BF%D1%80%D0%B0%D1%86%D1%96_%D1%81%D1%82%D1%83%D0%B4%D0%B5%D0%BD%D1%82%D1%96%D0%B2/2017/%D0%BA%D0%B0%D1%84_%D1%82%D0%B5%D1%81%D0%B0/TESA_Yalovenko.pdf
13. https://itsider.com.ua/informatsijno-rozvazhalni-systemy-dlya-avto/

14. https://audiosources.com.ua/adas-sho-ce-chi-potribna-cya-sistema-v-avtomobilnomu-videoreestratori