НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра інформаційно-комунікаційних технологій та систем

«На правах рукопису»
УДК 004.72

«До захисту допущено»
ВО завідувача кафедри
_____ Аліна МОШИНСЬКА
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Система сертифікації кібербезпеки підключеного автомобіля»

Виконала:
студентка ІІ курсу, групи ТС-11мп
Дорошенко Анна Сергіївна _____

Керівник:
Доктор технічних наук, професор
Горицький В. М. _____

Рецензент:
Старший Викладач СК №5 ІСЗЗІ
Мітін С.В. _____

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

Київ – 2022 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра інформаційно-комунікаційних технологій та систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (освітня програма) – 172 «Телекомунікації та радіотехніка» («Системи та мережі електронних комунікацій»)

ЗАТВЕРДЖУЮ

В.О. завідувача кафедри

_____ Аліна МОШИНСЬКА

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Дорошенко Анні Сергіївні

1. Тема дисертації «Система сертифікації кібербезпеки підключеного автомобіля», науковий керівник дисертації Горицький Віктор Михайлович, д.т.н., професор, затверджені наказом по університету від, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації: «_06_» «_12_»2022р.

3. Об’єкт дослідження – кіберзахист підключеного автомобіля, системи сертифікації кібербезпеки.

4. Предмет дослідження – регламенти, директиви, стандарти що гарантують кіберзахист підключеного автомобіля.

5. Перелік завдань, які потрібно розробити:

1) Аналіз інсуючих систем сертифікації

2) Дослідження концепції підклюяеного автомобіля

3) Аналіз інсуючих мінжародних стандартів регулювання кібербезпеки підключеного автомобіля

4) Формування системи сертифікації

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: Презентація Microsoft PowerPoint

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1.	Затвердження теми науковим керівником	01.11.2021 – 15.01.2022	виконано
2.	Робота над першим розділом	16.01.2022 – 27.03.2022	Виконано
3.	Робота над другим розділом	03.04.2022 – 15.09.2022	Виконано
4.	Робота над третім розділом	16.09.2022 – 15.10.2022	виконано
5.	Робота над четвертим розділом	16.10.2022 – 06.12.2022	Виконано
6.	Оформлення дипломної роботи		Виконано
7.	Отримання допуску до захисту		

Студент Анна ДОРОШЕНКО

Науковий керівник дисертації Віктор ГОРИЦЬКИЙ

РЕФЕРАТ

Темою магістерської дисертації є розроблення системи сертифікації кібербезпеки підключеного автомобіля.

Робота містить 84 сторінки, зокрема 14 ілюстрацій, 4 таблиці та 42 джерел інформації.

Тема магістерської дисертації є актуальною, так як система сертифікації має на меті запобігання реалізації продукції небезпечною для життя, здоров'я та майна громадян та навколишнього середовища. У міру розвитку автономної мобільності наші транспортні засоби будуть все більше підключатися один до одного та до навколишньої інфраструктури та мереж, що створить нові вразливості, пов’язані з безпекою, в автомобільному секторі, що вимагає цілісного підходу.

Мета дисертації полягає в створення умов для міжнародного співробітництва та торгівлі, сприяння споживачеві у компетентному виборі продукції у сфері кібербезпеки підключеного автомобіля.

Об’єктом дослідження є кіберзахист підключеного автомобіля, системи сертифікації кібербезпеки.

Предметом дослідження є регламенти, директиви, стандарти що гарантують кіберзахист підключеного автомобіля.

У дисертації була запропонована схема сертифікація кібербезпеки підключеного автомобіля опираючись на вимоги до схеми з міжнародних стандартів Європейського Союзу. Були надані рекомендації щодо вимог розроблення системи сертифікації кібербезпеки підключеного автомобіля.

Ключові слова: сертифікація, акредитація, система сертифікації кібербезпеки, схема сертифікації, кібербезпека, підключений автомобіль.

ABSTRACT

The topic of the master's thesis is the development of a system of certification of cyber security of a connected car.

The work contains 84 pages, including 14 illustrations, 4 tables and 42 sources of information.

The topic of the master's thesis is relevant, as the certification system aims to prevent the sale of products dangerous to life, health and property of citizens and the environment. As autonomous mobility evolves, our vehicles will become increasingly connected to each other and to surrounding infrastructure and networks, creating new security vulnerabilities in the automotive sector that require a holistic approach.

The purpose of the dissertation is to create conditions for international cooperation and trade, to assist the consumer in the competent choice of products in the field of cyber security of the connected car.

The object of the research is the cyber protection of the connected car, the cyber security certification system.

The subject of the research are regulations, directives, standards that guarantee cyber protection of the connected car.

The dissertation proposed a scheme for cyber security certification of a connected car based on the requirements for the scheme from the international standards of the European Union. Recommendations were provided regarding the requirements for the development of a connected car cybersecurity certification system.

Keywords: certification, accreditation, cyber security certification system, certification scheme, cyber security, connected car.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 8
ВСТУП 9
1 АНАЛІЗ ІСНУЮЧИХ СИСТЕМ СЕРТИФІКАЦІЙ 11
1.1Закон України "Про технічні регламенти та оцінку відповідності" 11
1.1.1 Визначення термінів що вживаються сфері оцінки відповідності 12
1.1.2 Технічні регламенти та процедура оцінки відповідності 16
1.1.3 Вимоги до призначених органів 20
1.2 Система сертифікації транспортних засобів 22
1.3 Система сертифікації кібербезпеки 27
1.4 Висновки до розділу 1 32
2 ДОСЛІДЖЕННЯ КОНЦЕПЦІЇ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ 34
2.1 Сучасний стан світових тенденцій використання підключеного автомобіля 34
2.1.1Застосування підключених автомобілей 38
2.2 Ризики використання підключеного автомобіля та його кібербезпека 40
2.2.2 Нормативні вимоги щодо безпеки 43
2.2.3 Перспективи розвитку вимог до кібербезпеки підключеного автомобіля 44
2.3 Висновки до розділу 2 46
3 МІЖНАРОДНІ СТАНДАРТИ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ТРАНСПОРТНИХ ЗАСОБІВ 47
3.1 Організації, що забезпечують кібербезпеку підключеного автомобіля 48
3.2 Регламентація кібербезпеки підключеного автомобіля 52
3.3 Вимоги правил ЄЕК ООН щодо кібербезпеки підключеного автомобіля 54
3.4 Висновки до розділу 3 56
4 СИСТЕМА СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ 57

4.1 Документ ООН з кібербезпеки ECE/TRANS/WP.29/GRVA/2022/5. 57
4.2 Глобальна структура сертифікації продуктів. Послуг та процесів. 62
4.3 Розробка схеми сертифікації кібербезпеки підключеного автомобіля для України 66
4.4 Висновки до розділу 4 78
ВИСНОВКИ 79
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 81

ПЕРЕЛІК СКОРОЧЕНЬ

CSMS – Cyber Security Management System;

ISO – International Organization for Standardization;

SAE – Society of Automotive Engineers;

VTA – Vehicle Type Approval;

LAN – Local area network;

V2I – Vehicle-to-Infrastructure;

V2V – Vehicle-to-vehicle;

V2C - Vehicle to Cloud;

V2P - Vehicle to Pedestrian;

V2X - Vehicle to Everything;

VRM - Voltage Regulator Module;

GPS - Global Positioning System;

ADAS - Advanced driver-assistance systems;

NHTSA - National Highway Traffic Safety Administration;

ANPRM - Advance Notice of Proposed Rule Making;

DSRC - Dedicated short-range communications;

CAN - Controller Area Network;

MITM - Man-in-the-Middle;

ОС – Операційна система;

SOG-IS – Senior Officials Group Information Systems Security;

ДВЗ – Двигун внутрішнього згоряння;

EV – Electric Vehicle;

ЕБУ – Електронний блок управління;

ІКТ – Інформаційно-комунікаційні технології;

ШІ – Штучний інтелект;

WP – working party – Всесвітній форум;

ВСТУП

В сучасних умовах автомобільна індустрія, яку раніше вважали простою комбінацією фізичних частин, демонструє нову промислову парадигму, поширюючись на зв’язок між транспортними засобами та речами стикається з радикальними змінами швидкими темпами цифровізації все більше і більше електронних систем керування, інтелектуальних компонентів, вбудованих систем та інтерфейсів API знаходять свій шлях у транспортних засобах, що робить їх потужнішими, безпечнішими та розумнішими, ніж будь-коли раніше. Однак зростаюча залежність від електроніки також таїть в собі небезпеку. Четверта промислова революція та ера 5G постійно змінюються на основі базових технологій, таких як штучний інтелект, хмарні середовища, BigData та високошвидкісні мережі.

Із впровадженням інформаційно-комунікаційних технологій, таких як зв’язок V2X, штучний інтелект і автономне водіння, у світі будуються нові бізнес-моделі, такі як «розумний автомобіль», «самокерований автомобіль» і «підключений автомобіль».

Сертифікація підключених транспортних засобів – це процес забезпечення того, щоб компоненти системи, виготовлені відповідно до вимог сумісності підключених транспортних засобів, працювали належним чином. Сертифікація гарантує, що користувачі можуть бути впевнені, що компоненти працюватимуть у системі.

Метою сертифікаційних досліджень є робота у тісній співпраці з державними та приватними партнерами для встановлення відповідних сертифікаційних вимог до обладнання, додатків, пристроїв та систем.

У світі, де технології постійно розвиваються, автомобільна промисловість наполегливо працює, щоб залишатися попереду в кібербезпеці. Оскільки все більше автомобілів підключаються до Інтернету, важливо вжити заходів для захисту водіїв та їхніх даних.

Метою роботи є розроблення схеми сертифікації кібербезпеки підключеного автомобіля.

Об’єктом дослідження є кіберзахист підключеного автомобіля, системи сертифікації кібербезпеки.

Предметом дослідження є схеми сертифікації кіберзахисту підключеного автомобіля, які відповідають вимогам Угоди Україна – ЄС.

У дисертації була запропонована схема сертифікація кібербезпеки підключеного автомобіля опираючись на вимоги до схеми з міжнародних стандартів Європейського Союзу. Були надані рекомендації щодо вимог розроблення системи сертифікації кібербезпеки підключеного автомобіля.

1 АНАЛІЗ ІСНУЮЧИХ СИСТЕМ СЕРТИФІКАЦІЙ

1.1 Закон України "Про технічні регламенти та оцінку відповідності"

Система сертифікації має на меті запобігання реалізації продукції небезпечною для життя, здоров'я та майна громадян та навколишнього середовища. Створення умов для міжнародного співробітництва та торгівлі, сприяння споживачеві у компетентному виборі продукції.

Досвід проведення робіт із сертифікації у державній системі сертифікації показав затребуваність добровільної оцінки відповідності продукції, яка не підпадає під дію технічних регламентів, а споживач зацікавлений у отриманні достовірної інформації про неї.

Враховуючи наявні потреби у проведенні компетентної оцінки відповідності продукції третьою незалежною стороною, а також потреби суспільства у отриманні достовірної інформації щодо безпеки товарів та послуг

Відповідно до прийнятого Україною курсу на європейську інтеграцію нині завершено перехід від Державної системи сертифікації до підтвердження відповідності продукції технічним регламентам.

Технічний регламент - нормативно-правовий акт, в якому визначено характеристики продукції або пов'язані з ними процеси та методи виробництва, включаючи відповідні процедурні положення, додержання яких є обов'язковим. Він може також включати або виключно стосуватися вимог до термінології, позначень, пакування, маркування чи етикетування в тій мірі, в якій вони застосовуються до продукції, процесу або методу виробництва. Нормативно-правовий акт, що має ознаки технічного регламенту, вважається технічним регламентом незалежно від використання у назві такого акту слів "технічний регламент" [1].

Добровільна сертифікація здійснюється у законодавчо нерегульованій сфері відповідно до порядку, визначеного договором між заявником та

органом сертифікації. Система Добровільної Сертифікації відкрита всім зацікавлених, хто цінує свою репутацію.

Добровільна сертифікація регулюється законом України «Про технічні регламенти та процедури оцінки відповідності».

Цей Закон регулює відносини, що виникають у зв'язку з розробленням та прийняттям технічних регламентів і передбачених ними процедур оцінки відповідності, їх застосуванням стосовно продукції, яка вводиться в обіг, надається на ринку або вводиться в експлуатацію в Україні, а також здійсненням добровільної оцінки відповідності.

1.1.1 Визначення термінів що вживаються сфері оцінки відповідності

Згідно ЗУ «Про технічні регламенти та процедури оцінки відповідності». Для вживання у коректній формі терміни, що необхідні для аналізування систем сертифікації, подальші терміни будуть вживатись в такому значенні:

випробувальна лабораторія - орган з оцінки відповідності, який проводить випробування;

випробування - визначення однієї чи кількох характеристик об'єкта оцінки відповідності згідно з процедурою;

виробник - будь-яка фізична чи юридична особа (резидент чи нерезидент України), яка виготовляє продукцію або доручає її розроблення чи виготовлення та реалізує цю продукцію під своїм найменуванням або торговельною маркою. Положення цього Закону щодо виробників також застосовуються до монтажників ліфтів;

гармонізований європейський стандарт - стандарт, який прийнятий однією з європейських організацій стандартизації на основі запиту, зробленого Європейською Комісією, та номер і назву якого опубліковано в "Офіційному віснику Європейського Союзу";

документ про відповідність може бути:

- декларація (в тому числі декларація про відповідність),

- протокол (у тому числі протокол випробувань),
- звіт,
- висновок,
- свідоцтво,
- сертифікат (у тому числі сертифікат відповідності)
- або будь-який інший документ,

що підтверджує виконання визначених вимог, які стосуються об'єкта оцінки відповідності;

заінтересована сторона - будь-яка фізична чи юридична особа або громадське об'єднання без статусу юридичної особи (резидент чи нерезидент України), що має безпосередній або опосередкований інтерес стосовно діяльності з розроблення, прийняття та застосування технічних регламентів і передбачених ними процедур оцінки відповідності та/або використання результатів оцінки відповідності вимогам технічних регламентів;

знак відповідності технічним регламентам - маркування, за допомогою якого виробник вказує, що продукція відповідає вимогам, які застосовуються до зазначеної продукції та визначені в технічних регламентах, якими передбачене нанесення цього маркування;

інспектування - перевірка продукції, процесу, послуги чи установки або їх проектування та визначення їх відповідності конкретним вимогам або, на основі професійного судження, загальним вимогам;

модуль оцінки відповідності - уніфікована процедура оцінки відповідності чи її частина, визначена згідно з відповідним актом законодавства Європейського Союзу;

об'єкт оцінки відповідності - конкретний матеріал, продукція, установка, процес, послуга, система, особа чи орган, до яких застосовується оцінка відповідності;

орган з інспектування - орган з оцінки відповідності, який здійснює інспектування;

орган з оцінки відповідності - підприємство, установа, організація чи їх структурний підрозділ, що здійснює діяльність з оцінки відповідності, включаючи випробування, сертифікацію та інспектування;

орган із сертифікації - орган з оцінки відповідності, який є третьою стороною та управляє схемами сертифікації;

орган, що призначає, - центральний орган виконавчої влади, уповноважений призначати органи з оцінки відповідності (в тому числі визнані незалежні організації), обмежувати сферу їх призначення, тимчасово припиняти чи поновлювати дію рішень про призначення або анулювати ці рішення;

оцінка відповідності - процес доведення того, що визначені вимоги, які стосуються продукції, процесу, послуги, системи, особи чи органу, були виконані. Оцінка відповідності органу здійснюється шляхом акредитації органів з оцінки відповідності;

підтвердження відповідності - видача документа про відповідність, яка ґрунтується на прийнятому після критичного огляду рішенні про те, що виконання визначених вимог було доведене;

презумпція відповідності - припущення, яке визнається достовірним, поки не буде доведено інше, про те, що продукція, пов'язаний з нею процес або метод виробництва чи інший об'єкт відповідає вимогам відповідного технічного регламенту, що визначені в ньому, а орган з оцінки відповідності відповідає спеціальним вимогам до призначених органів з оцінки відповідності (далі - призначений орган) чи визнаних незалежних організацій;

призначення - надання органом, що призначає, органу з оцінки відповідності (в тому числі визнаній незалежній організації) права виконувати як третій стороні певні завдання з оцінки відповідності згідно з відповідним технічним регламентом;

продукція - речовина, препарат або товар, виготовлений у ході виробничого процесу;

процедура оцінки відповідності - будь-яка процедура, яка безпосередньо чи опосередковано використовується для визначення того, що визначені вимоги виконуються;

ризик - можливість виникнення та вірогідні масштаби наслідків негативного впливу протягом певного періоду часу;

розповсюдження - надання продукції на ринку України після введення її в обіг;

розповсюджувач - будь-яка інша, ніж виробник або імпортер, фізична чи юридична особа в ланцюгу постачання продукції, яка надає продукцію на ринку України;

сертифікація - підтвердження відповідності третьою стороною (особою, яка є незалежною від особи, що надає об'єкт оцінки відповідності, та від особи, що заінтересована в такому об'єкті як споживач чи користувач), яке стосується продукції, процесів, послуг, систем або персоналу;

система оцінки відповідності - правила, процедури та управління для проведення оцінки відповідності;

сфера призначення - перелік процедур оцінки відповідності та видів продукції, стосовно яких згідно з відповідним технічним регламентом призначено орган з оцінки відповідності;

технічна специфікація - документ, що встановлює технічні вимоги, яким повинна задовольняти продукція, процес або послуга;

технічне регулювання - правове регулювання відносин у сфері

- визначення та виконання обов'язкових вимог до характеристик продукції або пов'язаних з ними процесів та методів виробництва,
- а також перевірки їх додержання шляхом оцінки відповідності та/або державного ринкового нагляду і контролю нехарчової продукції чи інших видів державного нагляду (контролю);

У технічних регламентах та процедурах оцінки відповідності, застосування яких передбачене технічними регламентами, терміни та їх

визначення, зазначені у частині першій цієї статті, можуть доповнюватися та/або уточнюватися [1].

1.1.2 Технічні регламенти та процедура оцінки відповідності

Процедурні питання, пов’язані з розробленням та прийняттям технічних регламентів і процедур оцінки відповідності, застосування яких передбачене технічними регламентами, внесенням змін до них, визнанням їх такими, що втратили чинність, та їх скасуванням, які не визначені цим Законом, визначаються відповідними нормативно-правовими актами.

Законодавство про технічні регламенти та оцінку відповідності складається з цього Закону, міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, та інших нормативно-правових актів, що регулюють відносини в цій сфері.

У разі якщо міжнародним договором України, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені законодавством про технічні регламенти та оцінку відповідності, застосовуються правила міжнародного договору України.

Центральний орган виконавчої влади, забезпечує формування державної політики у сфері технічного регулювання:

• Визначення пріоритетних напрямів розвитку технологічного регулювання в Україні.

• Здійснює нормативно-правове регулювання у сфері регулювання технологій.

• Координує розроблення та перегляд технічних регламентів та процедур оцінки відповідності.

• Здійснення міжнародного співробітництва у сфері технічного регулювання з відповідними органами інших країн.

• Здійснення інших прав, визначених законодавством України.[1]

Центральні органи виконавчої влади, що реалізують державну політику у сфері технічного регулювання:

• Призначення органів з оцінки відповідності (у тому числі акредитованих незалежних організацій) на підставі пропозицій відповідних центральних органів виконавчої влади для виконання окремих завдань з оцінки відповідності як третіх осіб відповідно до Технічного регламенту, що передбачає застосування процедур оцінки відповідності. Залучення призначених органів або акредитованих незалежних організацій;

• Відповідний центральний орган виконавчої влади органу з оцінки відповідності, який подає заяву на призначення (далі - заявник на призначення), проводить оцінку (далі - оцінка) відповідності призначеного органу або визнаного незалежного органу вимоги. претенденти на призначення);

• Здійснювати моніторинг уповноважених органів та визнаних незалежних органів щодо дотримання ними вимог та виконання ними своїх обов’язків згідно з цим Законом та пов’язаними з ним нормативно-правовими актами із залученням відповідних центральних органів виконавчої влади; Технічний регламент (далі - Моніторинг призначених органів та визнаних незалежних організацій)

• Формує та веде базу даних технічних регламентів та реєстр призначених органів і визнаних незалежних організацій.

• Здійснення інших прав, визначених законодавством України.

Центральним органом виконавчої влади, що реалізує державну політику у сфері технічного регулювання, є Призначений орган

Законом можуть бути визначені й інші цілі прийняття технічних регламентів [2]

Технічні регламенти розробляються на основі:

• Міжнародні стандарти, або вже прийняті, або в стадії остаточної розробки, або їх частини. за винятком випадків, коли такі міжнародні стандарти або їх частини є неефективними або неадекватними засобами

досягнення конкретної мети прийняття технічних регламентів. зокрема через значні кліматичні чи географічні чинники або значні технічні проблеми;

• Регіональні стандарти, національні стандарти України чи інших країн, Європейського Союзу, інших економічних об'єднань чи інших держав або відповідні частини їхніх стандартів і законодавчих актів.

Технічні регламенти затверджуються законами, актами Кабінету Міністрів України та центральних органів виконавчої влади.

Технічні регламенти, що передбачають застосування процедур оцінки відповідності, затверджуються законами або актами Кабінету Міністрів України [2]

Відповідність продукції вимогам Технічного регламенту може бути забезпечена шляхом застосування національних стандартів та/або технічних умов, на які є посилання, що містяться у відповідних Технічних регламентах. Технічний регламент визначає, чи є продукція, яка відповідає таким національним стандартам та/або технічним умовам, єдиним чи одним із способів виконання відповідних вимог Технічного регламенту.

Технічним регламентом може бути встановлено, що відповідність продукції, пов’язаного з нею процесу, способу виробництва чи іншої одиниці переліку національних стандартів, затвердженому відповідним центральним органом виконавчої влади, або його частинам передбачає відповідність продукції щодо: процесу чи способу виробництва; або інший об'єкт, на який поширюються ці стандарти, або їх частини та відповідно до вимог зазначеного технічного регламенту, визначених у технічному регламенті [3].

Крім застосування стандартів з Переліку національних стандартів, виробники мають право приймати інші рішення щодо виконання вимог Технічного регламенту.

План розробки технічного регламенту формуватиметься на основі пропозицій зацікавлених сторін на період понад рік для забезпечення координації цієї діяльності.

Заінтересовані особи подають пропозиції довільної форми щодо розроблення технічного регулювання та, змінюючи їх або визнаючи такими, що втратили чинність, подають до центрального органу виконавчої влади, що забезпечує формування державної політики у сфері технологічного регулювання.

Центральний орган виконавчої влади, що забезпечує формування державної політики у сфері технічного регулювання:

Спільно з відповідними центральними органами виконавчої влади ми розглянемо та підтримаємо або відхилимо всі пропозиції, які надійдуть, на виконання вимог.

Розробити план розробки технічного регламенту на основі підтриманих пропозицій та затвердити або внести відповідні зміни до плану. Розробка технічного регламенту та оприлюднення на офіційному веб-сайті протягом 5 робочих днів з дня затвердження плану змін.

Добровільна оцінка відповідності не передбачена технічними регламентами.

Добровільна оцінка відповідності проводиться в усіх формах, включаючи випробування, декларації про відповідність, сертифікацію та перевірки, а також добровільно на відповідність заявленим вимогам.

Органи з оцінки відповідності (включаючи призначені органи або визнані незалежні органи) беруть участь у проведенні добровільної оцінки відповідності згідно з умовами, визначеними в угоді між заявником і органом.

Наступні органи з оцінки відповідності повинні або можуть брати участь у виконанні завдань з оцінки відповідності технічним нормативним вимогам, якщо це зазначено у відповідних технічних регламентах або процедурах оцінки відповідності, наданих такими органами:

• призначені органи, якими є органи сертифікації та інспекції, а також випробувальні лабораторії для проведення окремих робіт з оцінки відповідності будівельної продукції;

• Акредитована незалежна організація – виконує визначені завдання з оцінки відповідності технології нероз’ємного з’єднання Технічному регламенту обладнання, що працює під тиском, персоналу, який виконує нероз’ємні з’єднання та/або неруйнівний контроль.

• Акредитовані випробувальні лабораторії виробника – для виконання певних завдань випробування (контролю) продукту, як визначено в деяких процедурах оцінки відповідності, ці процедури надають виробникам можливість вибору зв’язатися зі своїми акредитованими випробувальними лабораторіями або призначеними органами.

• Акредитована незалежна організація може бути призначеним органом.

• Ці випробувальні лабораторії повинні бути окремою та окремою частиною підприємства і не повинні брати участь у розробці, виробництві, постачанні, встановленні, використанні або обслуговуванні продукції, яку вони оцінюють.

Акредитовані випробувальні лабораторії виробників не підлягають призначенню. Підприємство, до складу якого входить акредитована випробувальна лабораторія виробника, або національний орган з акредитації України зобов'язані на вимогу призначеного органу надати призначеному органу інформацію про акредитацію випробувальної лабораторії [1]

1.1.3 Вимоги до призначених органів

Органи з оцінки відповідності можуть бути призначені для виконання окремих завдань з оцінки відповідності як третій особи згідно з відповідними технічними регламентами.

1) відповідає таким загальним вимогам до призначених органів:

• Юридична особа - резидент України незалежно від форми власності.

• Мати досвід роботи з оцінки відповідності продукції протягом останніх 3 років.

• Має власні акредитовані випробувальні лабораторії для проведення принаймні деяких типів випробувань продукції в межах свого призначення та має контракти з іншими акредитованими випробувальними лабораторіями в межах свого призначення для виконання типів випробувань продукції, які не проводяться його власними лабораторіями. Я зробив.

• Укладено договори обов'язкового страхування професійної відповідальності від можливих збитків третіх осіб.

2) участь призначеного органу відповідає спеціальним вимогам до призначеного органу, визначеним у відповідному технічному регламенті, що передбачає застосування процедури оцінки відповідності, і ці вимоги не визначені конкретним технічним регламентом; Особливі вимоги до призначених органів.

Визнання результатів оцінки відповідності, проведеної за межами України відповідно до статті 45

1. Результати оцінки відповідності вимогам технічного регулювання, проведені в інших країнах, приймаються та визнаються в Україні за умови, що процедура оцінки відповідності, що застосовується в цій країні, забезпечує такий самий рівень (навіть якщо він відрізняється від процедури в Україні). Відповідність вимогам відповідних технічних регламентів, наприклад Порядку оцінки відповідності України.

2. Документи про відповідність вимогам технічного регламенту, видані за результатами оцінки відповідності, проведеної в інших країнах, приймаються за умови укладення в Україні міжнародних договорів про взаємне визнання результатів робіт з оцінки відповідності. між Україною та іншими державами.

3. Призначені органи мають право визнавати результати оцінки відповідності вимогам технічного регулювання, проведеної іноземними акредитованими органами з оцінки відповідності на підставі договорів із цими органами з оцінки відповідності за умови дотримання таких умов:

- Національні органи з акредитації, які акредитують органи з оцінки відповідності в Україні та інших державах, є членами міжнародних чи регіональних органів з акредитації або уклали з такими органами угоди про взаємне визнання відповідних видів діяльності з оцінки відповідності.
- Призначені органи застосовують процедури оцінки відповідності або їх частини на основі документів про відповідність, виданих іноземними органами з оцінки відповідності, і видають документи про відповідність, передбачені цими процедурами, на власний ризик [1].

1.2 Система сертифікації транспортних засобів

Сертифікація підключених транспортних засобів — це процес перевірки того, що системні компоненти, виготовлені відповідно до вимог сумісності підключених транспортних засобів, функціонують належним чином. Автентифікація дозволяє користувачам перевірити, чи працює компонент у системі.

Метою сертифікаційних досліджень є тісна співпраця з державними та приватними партнерами для встановлення відповідних вимог до сертифікації обладнання, програм, пристроїв і систем.

Типова методологія оцінки ризику складається з восьми кроків.

• Визначення продукту: компанія визначає архітектуру для своїх продуктів, визначає середовище для роботи продукту та вимоги до створення середовища

• Ідентифікація активів: усі продукти, які мають цінність в організації, встановлюються як активи, а ті, що створюють сценарій збитків шляхом прогнозування збитків у разі аварії шляхом організації списку активів, які потребують кібербезпеки.

• Створення сценарію: після визначення вразливостей в активах створіть і перегляньте сценарії загроз для можливих ситуацій.

• Оцінка впливу: цінка впливу на основі результатів шкоди, коли виникає раніше написаний сценарій загрози.

• Визначення шляху атаки: шляхом аналізу сценарію загрози визначається шлях атаки, який сценарій може бути реалізований, а також визначення зв’язку шляху атаки та сценарію загрози.

• Оцінка здійсненності: на етапі оцінки здійсненності здійсненність оцінюється на основі порівняння середовища, в якому може бути реалізована атака за підготовленим сценарієм, і середовища фактичного активу, а також рівня складності кібератаки.

• Визначення ризику: оцініть ризик атаки на основі сценарію, створеного на попередньому кроці, здійсненності та впливу.

• Визначення того, як управляти ризиком: метод управління ризиком визначається шляхом перегляду результатів загальної оцінки ризику.

Існує чотири методи управління ризиками: прийняття ризику, зниження ризику, передача ризику та уникнення ризику.

Результати, обчислені на кожному кроці, можна застосувати до наступного кроку та остаточно визначити, як керувати ризиком для ідентифікованої загрози.

Визначення продукту: компанія визначає архітектуру продукту та визначає контекст і середовище, в якому працює продукт.

Ідентифікація активів: визначте всі цінні продукти, що зберігаються в організації, як активи, і створіть сценарій збитків, створивши список активів, які потребують кібербезпеки для прогнозування збитків у разі інциденту.

Створення сценарію: після визначення вразливостей активу створіть і перегляньте сценарії загроз для можливих ситуацій.

Оцінка впливу: оцінка впливу на основі наслідків збитків від виникнення раніше створених сценаріїв загрози

Ідентифікація вектора атаки: аналізуйте сценарії загроз, щоб ідентифікувати вектори атак, які можна застосувати, і визначити їхні взаємозв’язки.

Оцінка здійсненності: на етапі оцінки здійсненності оцінка здійсненності проводиться шляхом порівняння середовища, в якому може бути реалізована атака створеного сценарію, середовища фактичного активу та складності кібератаки.[3]

Необхідно визначити метод управління ризиками шляхом аналізу комплексних результатів оцінки ризиків

Існує чотири методи управління ризиком: прийняття ризику, зниження ризику, передача ризику та уникнення ризику.

У частині рекомендацій виробника зазначені заходи, які мають бути вжиті виробниками транспортних засобів відповідно до системи керування кібербезпекою. Аналогічно тому, як ISO/SAE 21434 визначає діяльність системи управління кібербезпекою транспортного засобу шляхом отримання оцінки ризику - процесу управління за допомогою TARA, посібник з кібербезпеки також визначає діяльність системи управління кібербезпекою за допомогою процесу, показаного на Рисунку 1.1.

Рисунок 1.1 – Діяльність системи управління кібербезпекою транспортних засобів

Рекомендується зробитин на етапі оцінки/управління ризиками виробник виконує ідентифікацію факторів, пов'язаних з автомобільною

кібербезпекою, оцінку ризиків і роботу з виявленими ризиками та управління ними. Оцінка/управління ризиками повинні враховувати різні загрози, які можуть існувати в транспортному засобі, такі як внутрішні/зовнішні системи та ланцюжки поставок, а також визначати та керувати прийнятними рівнями ризику та серйозністю ризику серед розрахованих ризиків .

На етапі заходів безпеки/моніторингу та реагування виробник повинен реалізувати заходи безпеки, такі як виявлення та запобігання, моніторинг та аналіз причин уразливостей, що існують у транспортному засобі. Заходи безпеки повинні бути в змозі захистити транспортний засіб від виявлених небезпек і повинні бути вжиті в найкоротший термін. Це повинно застосовуватися не тільки до транспортних засобів, але й до продуктів, пов'язаних з транспортними засобами, і повинні бути передбачені стандарти шифрування з достатнім ступенем безпеки для шифрування, що використовується для заходів безпеки.

На етапі випробування (випробування) безпеки рекомендується, щоб виробник провів випробування на об'єктивній основі для підтвердження рівня розроблених заходів безпеки [8].

На етапі управління записами безпеки слід записувати дані, пов'язані з кібербезпекою транспортного засобу, і, якщо вносяться зміни, слід керувати історією. Вміст, який має бути включений до запису безпеки, показано в Таблиці 1.1. Створені записи безпеки повинні зберігатися щонайменше 10 років із дати повної зупинки транспортного засобу, а разі їх знищення рекомендуються відповідні наступні заходи.

На етапі обміну інформацією рекомендується повідомляти автомобільному агентству про стан моніторингу та заходи безпеки для кібератак, а також про виявлення вразливостей та реагування на них не рідше одного разу на рік.

Таблиця 1.1 – Діяльність системи управління кібербезпекою транспортних засобів

Розділ	Зміст
Інформація про кібербезпеку	Інформація про систему керування кібербезпекою автомобіля
	Інформація про конфігурацію цільового автомобіля
	Системи, пристрої та архітектури транспортних засобів, пов’язані з кібербезпекою
	Взаємодія з іншими системами автомобіля та внутрішніми/зовнішніми системами, пов’язаними з кібербезпекою
	Інформація про оцінку ризику транспортного засобу
	Заходи безпеки та інформацію про управління ризиками, реалізовані в транспортних засобах
	Оцінювальна інформація щодо кібербезпеки автомобіля
	Питання кібербезпеки в ланцюжку постачання деталей, пристроїв, послуг тощо
	Записи про інциденти та аналіз інформації щодо кібербезпеки
	Деталі інших заходів кібербезпеки автомобілів

На етапі взаємної співпраці виробник повинен співпрацювати зі зв'язаними сторонами, такими як пов'язані виробники деталей, пов'язаних з транспортними засобами, та агентства автомобільної безпеки, і кожна організація обмінюється інформацією, пов'язаною з кібербезпекою, один з одним та оперативно встановлює заходи безпеки при виявленні ризику. Ви повинні працювати разом, щоб це сталося.

Роль Агентства автомобільної безпеки пояснює функцію Агентства автомобільної безпеки, яка відповідає за сертифікацію системи управління кібербезпекою. Агентство автомобільної безпеки - це агентство, яке оцінює кібербезпеку виробників транспортних засобів, що відповідають вимогам ЄЕК ООН R-155, та трансформує агентство за твердженням, яке видає сертифікат CSMS відповідно до національного законодавства. Агентство має право перевіряти інформацію, пов'язану з кібербезпекою, надану виробником транспортного засобу, для управління рівнем ризику кібербезпеки транспортного засобу та за необхідності рекомендувати коригувальні дії [9].

1.3 Система сертифікації кібербезпеки

У січні 2021 року набрав чинності закон ЄЕК ООН щодо CS, а з липня 2022 року нові серійні автомобілі в 56 країнах в рамках ЄЕК ООН підпадатимуть під дію Системи управління кібербезпекою(Cyber Security Management System)(CSMS) не тільки по виробниках (OEM), а й по частинах.

ЄЕК ООН рекомендує використовувати CSMS, посилаючись на ISO/SAE 21434, а не на ISO 26262, поточний міжнародний стандарт транспортної безпеки. ISO/SAE 21434 — це міжнародний стандарт, призначений для визначення процесів кібербезпеки від планування автомобіля до виробництва та пост-продакшну. Виробник автомобілів (OEM), який отримав сертифікат CSMS, може виробляти автомобіль, отримавши схвалення типу транспортного засобу (VTA), як показано на Рисунку 1.. VTA перевіряє та аналізує функціональну безпеку та кібербезпеку для типів транспортних

засобів. Учасник тестування повинен задокументувати сертифікат CSMS і заходи з кібербезпеки (оцінка ризиків і результати тестування на безпеку), які відбуваються для кожного типу транспортного засобу, і надати їх установі з сертифікації типу або установі технічної підтримки.

Міжнародні стандарти включають ISO/SAE 21434, ISO 26262 та ISO/PAS 21448. ISO 26262 — це міжнародний стандарт, який зосереджується на несправностях у системах електричної та електронної архітектури (E/E), і надійність важливіша за безпеку, оскільки ISO/PAS 21448 також розглядає ризики, які можуть виникнути через безвідмовні функції, як це робить ISO 26262. не покривати. . Тому, у відповідь на потребу в міжнародних стандартах безпеки, SAE та ISO, які випустили J3061, вирішили випустити ISO/SAE 21434, щоб відповідати вимогам безпеки автомобільної промисловості.

Щоб знати CSMS, потрібно розуміти міжнародний стандарт ISO 21434, рекомендований ЄЕК ООН як довідковий. Як згадувалося вище, ISO 21434 — це міжнародний стандарт для процесів управління ризиками, який визначає, як налаштувати та керувати системою реагування для пом’якшення кібератак і збитків, які можуть виникнути на будь-якому етапі життєвого циклу автомобільної промисловості. Архітектура ISO 21434 складається з 15 розділів (Рисунок 1.2).

Розділи з 5 по 15 важливі, і виробники обладнання та постачальники повинні розробити та впровадити процеси управління кібербезпекою, які відповідають вимогам кожного розділу. .

Розділи 1-4 містять стислий виклад мети та історії публікацій ISO/SAE 21434 .

Розділ 1 посилання, цитовані при створенні документа.

Розділ 2 інформацію про терміни та скорочення, що використовуються в документі. Він складається з опису розділ 3 та загальних інструкцій щодо користування документом розділ 4.

Кожен розділ можна розділити на

- корпоративне управління,

- управління процесом виробництва автомобілів
- діяльність у сфері кібербезпеки ланцюга постачання, залежно від того, як розглядається управління.

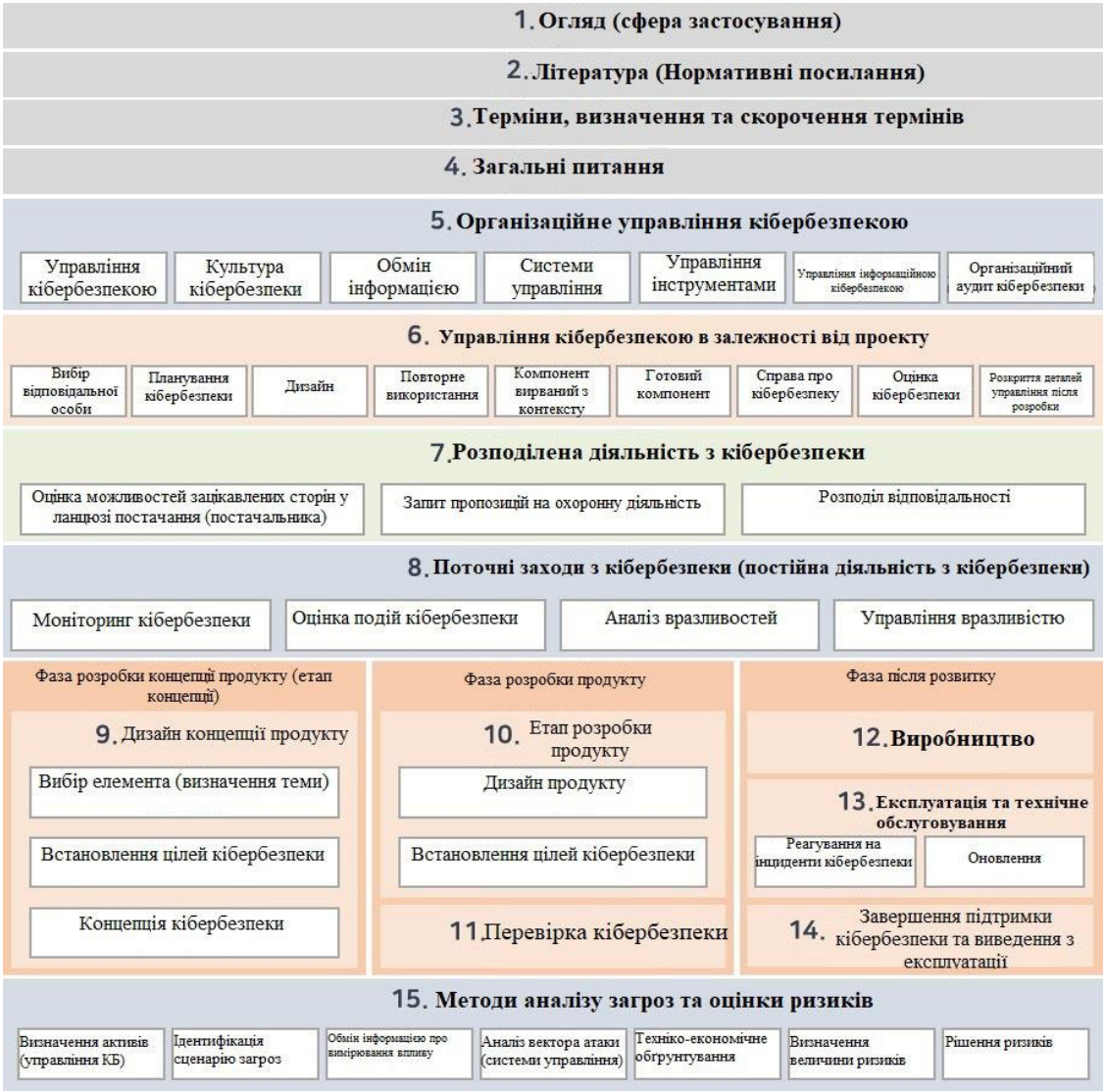


Рисунок 1.2 – Архітектура ISO 21434

Що стосується управління безпекою підприємства, виробники оригінального обладнання та постачальники повинні мати політику та процеси кібербезпеки транспортних засобів. Створення політики кібербезпеки вимагає визначення активів, визначення ризиків, що на них впливають, і управління виявленими ризиками. Розділи 5, 8 і 15 є елементами управління кібербезпекою з точки зору корпоративного управління.

Розділ 5 визначає управління кібербезпекою, яке мають здійснювати організаційні підрозділи всередині компанії. OEM-виробники та постачальники, як правило, повинні створити організацію з кібербезпеки, щоб створити та підтримувати власне управління кібербезпекою. Організація з кібербезпеки зазвичай складається з чотирьох груп: групи планування управління інформаційною безпекою, ради інформаційної безпеки, робочої групи інформаційної безпеки та групи реагування на інциденти. Структура кібербезпеки поділяється на адміністративну, фізичну та технічну безпеку. Після того, як організація з кібербезпеки сформована, управління кібербезпекою організації має бути реалізовано шляхом оперативного навчання для встановлення культури безпеки, аудитів безпеки та планів управління системами/пристроями [9].

Забезпечення кібербезпеки в Україні базується на таких принципах:

1) Верховенство права, законність, дотримання прав людини і основоположних свобод та їх захист у порядку, встановленому законом.

2) забезпечення національних інтересів України;

3) Відкритість, доступність, стабільність і безпека кіберпростору, розвиток Інтернету та відповідальна поведінка в кіберпросторі

4) широке поле співпраці з громадянським суспільством, державно-приватна взаємодія шляхом обміну інформацією, виконання спільних науково-дослідницьких проектів, навчання персоналу та підвищення кваліфікації в цьому відношенні, зокрема щодо інцидентів кібербезпеки, у сфері кібербезпеки та кіберзахист;

5) пропорційність та адекватність заходів кіберзахисту від реальних і потенційних ризиків та реалізацію невід’ємного права держав на самооборону відповідно до норм міжнародного права у разі агресивних дій у кіберпросторі;

9) міжнародне співробітництво для зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільного підходу до протидії кіберзагрозам, об’єднання зусиль з розслідування та запобігання кіберзлочинам, запобігання

терористам, військовому та іншому використанню кіберпростору в протиправних цілях;

10) Забезпечення демократичного цивільного контролю над утвореними відповідно до законодавства України збройними силами та правоохоронними органами, які здійснюють діяльність у сфері кібербезпеки.

Національна система кібербезпеки – це сукупність суб'єктів кібербезпеки та взаємопов'язаних заходів:

• політичного, науково-технічного, інформаційного чи освітнього характеру;

• організаційно-правові, оперативно-розшукові, розвідувальні, контррозвідувальні, оборонні, інженерно-технічні заходи;

• Заходи шифрування та технічного захисту національних інформаційних ресурсів, заходи кіберзахисту об'єктів критичної інформаційної інфраструктури.

Функціонування національної системи кібербезпеки забезпечується:

1) Розробка національної політики та операційних адаптацій у сфері кібербезпеки, спрямованих на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) Створення нормативної та термінологічної бази у сфері кібербезпеки, гармонізація нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу НАТО;

3) встановлює обов'язкові вимоги до інформаційної безпеки об'єктів критичної інформаційної інфраструктури, включаючи процеси створення, введення в експлуатацію, експлуатації та модернізації, з урахуванням особливостей галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури, та міжнародних стандартів;

4) Впровадження кращих світових практик та міжнародних стандартів функціонування систем аудиту інформаційної безпеки, кібербезпеки та кіберзахисту;

5) розвиток міжнародного співробітництва у сфері кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки в національних інтересах України, поглиблення співробітництва України з Європейським Союзом та НАТО у сфері кібербезпеки та використання кіберпростору, що проводиться в рамках під егідою Організації з безпеки та співробітництва в Європі [3-5].

1.4 Висновки до розділу 1

В першому розділі було проведено аналіз існуючих систем сертифікацій України з боку законодавчих нормативно правових актів та міжнародних стандартів на яких опирається існуюча міжнародна система сертифікації.

Система сертифікації має на меті запобігання реалізації продукції небезпечною для життя, здоров'я та майна громадян та навколишнього середовища. Створення умов для міжнародного співробітництва та торгівлі, сприяння споживачеві у компетентному виборі продукції.

Досвід проведення робіт із сертифікації у державній системі сертифікації показав затребуваність добровільної оцінки відповідності продукції, яка не підпадає під дію технічних регламентів, а споживач зацікавлений у отриманні достовірної інформації про неї.

Враховуючи наявні потреби у проведенні компетентної оцінки відповідності продукції третьою незалежною стороною, а також потреби суспільства у отриманні достовірної інформації щодо безпеки товарів та послуг

Метою сертифікаційних досліджень є тісна співпраця з державними та приватними партнерами для встановлення відповідних вимог до сертифікації обладнання, програм, пристроїв і систем.

Національна система з боку кібербезпеки забезпечує:

1) Розробку національної політики та операційних адаптацій у сфері кібербезпеки, спрямованих на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) Створення нормативної та термінологічної бази у сфері кібербезпеки, гармонізація нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу НАТО;

3) Встановлює обов'язкові вимоги до інформаційної безпеки об'єктів критичної інформаційної інфраструктури, включаючи процеси створення, введення в експлуатацію, експлуатації та модернізації, з урахуванням особливостей галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури, та міжнародних стандартів;

4) Впровадження кращих світових практик та міжнародних стандартів функціонування систем аудиту інформаційної безпеки, кібербезпеки та кіберзахисту;

5) Розвиток міжнародного співробітництва у сфері кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки в національних інтересах України, поглиблення співробітництва України з Європейським Союзом та НАТО у сфері кібербезпеки та використання кіберпростору, що проводиться в рамках під егідою Організації з безпеки та співробітництва в Європі;

2 ДОСЛІДЖЕННЯ КОНЦЕПЦІЇ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

2.1 Сучасний стан світових тенденцій використання підключеного автомобіля

У міру розвитку автономної мобільності наші транспортні засоби будуть все більше підключатися один до одного та до навколишньої інфраструктури та мереж. Хоча це матиме позитивний вплив на безпеку, це також створить нові вразливості, пов’язані з безпекою, в автомобільному секторі, що вимагає цілісного підходу [10].

Автономні та підключені транспортні засоби покращать транспортний потік і безпеку, а також стануть новими цілями для кіберзлочинців. Зростаюча різноманітність програмного забезпечення та комунікаційних інтерфейсів збільшує як складність, так і підключення, роблячи майбутні транспортні засоби ще більш вразливими до хакерських атак. Будь-яке порушення безпеки може призвести до втрати конфіденційності даних, негативно вплинути на безпеку автомобіля або навіть спричинити аварію. Тому необхідні як відповідні заходи безпеки, так і ефективні та надійні рішення кібербезпеки.

Підключені та самокеровані автомобілі мають складну структуру, поєднуючи різні функції автономного керування та комунікаційні інтерфейси. Зовнішні зловмисники, які порушують ці функції, можуть не лише поставити під загрозу безпеку учасників дорожнього руху, але й завдати значної шкоди конфіденційності підприємствам і водіям, а також завдати фінансової та операційної шкоди. Збільшення зв’язку між транспортними засобами збільшує потенційний ризик кібератак.

Доповнюючи оцінку безпеки прототипів транспортних засобів, необхідно забезпечити відповідне пом’якшення загроз, що впливають на безпеку та конфіденційність учасників дорожнього руху, а також на бізнес-модель та інтелектуальну власність водія.

Виконання оцінки кібербезпеки для автономних транспортних засобів дає такі переваги:

• Зменшення ризиків для безпеки та захисту, підтвердження концепції кібербезпеки та докази того, що системи систематично перевіряються, можуть підсилити обґрунтування схвалення автономних транспортних засобів.

• Захист учасників дорожнього руху та підприємства, дотримуючись найновіших стандартів і найкращих практик щодо загроз кібербезпеці.

• Розробляючи автономні системи з урахуванням безпеки та захисту, можна розробити безпечні передові технології автономного водіння.

• Кнкурентна перевага, співпрацюючи з міжнародними експертами, які знають найновіші загрози кібербезпеки, вразливості та стандарти.

Оцінка кібербезпеки для затвердження прототипу проводиться в три етапи.

1. Визначення критичних активів належним чином зменшить ризики кібербезпеки.

2. Переконатись, що система ключів автомобіля використовує ефективні та правильні заходи безпеки.

3. Забезпечити проведення комплексного тестування для перевірки реалізованих механізмів безпеки

Відповідно до даних аналізу ринку підключених автомобілів, оголошених Statista (Рисунок 2.1), розмір світового ринку підключених автомобілів досягне 64,8 мільярда доларів США в 2021 році та, як очікується, зросте до 191,8 мільярда доларів США до 2028 року.

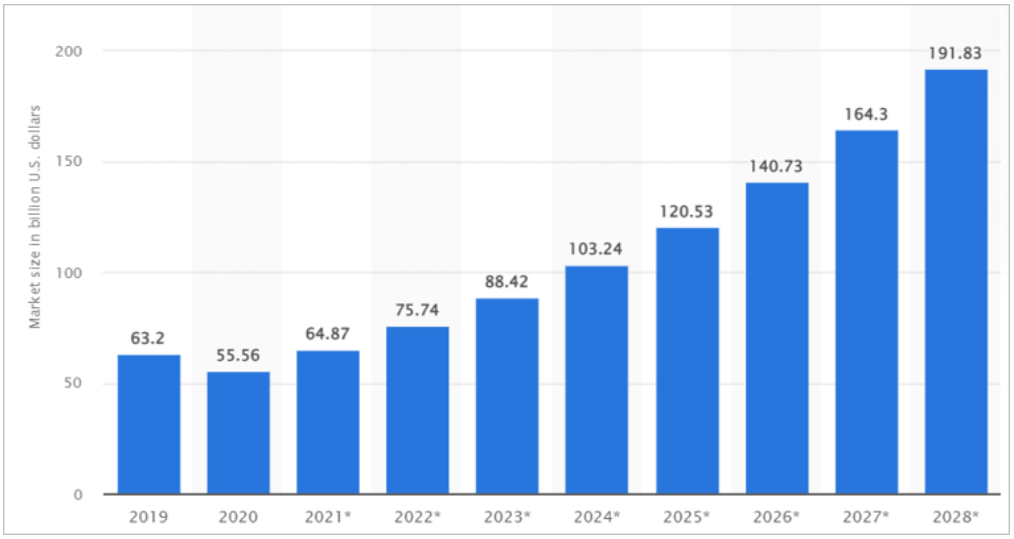


Рисунок 2.1 – Розмір світового ринку підключених автомобілів [1]

Зрозуміло, що ринок автотранспорту буде зростати на користь підключених автомобілей.

Підключений автомобіль є транспортним засобом, який вбудований інтелектуальними системами, а також має послуги для виходу в Інтернет.

Підключений автомобіль (Connected car) - це автомобіль, який може взаємодіяти в двосторонньому напрямку з іншими системами за межами автомобіля (LAN). Це дозволяє автомобілю ділитися доступом до Інтернету, а отже, і даними з іншими пристроями як усередині, так і ззовні автомобіля. Очікується, що для критичних для безпеки додатків автомобілі також будуть підключатися за допомогою спеціальної зв'язку ближнього радіусу дії (DSRC) або стільникових радіостанцій, які працюють у діапазоні 5.9 ГГц, надані FCC з дуже низькою затримкою.[10]

Обидва варіанти США та ЄС зосереджені на зв'язку 5,9 ГГц, проте сценарій ЄС має більш чіткий шлях до використання гібридного зв'язку (через запропонований підхід CALM), ніж сценарій США. Таким чином, сценарій ЄС вважається більш інтегрованим та масштабованим. Разом з іншими новітніми транспортними технологіями, такими як автоматизоване водіння, електромобілі та спільна мобільність, підключені транспортні засоби вносять свій внесок у новий тип мобільності майбутнього, яким є автономні, підключені, електричні та спільні транспортні засоби.

Технологія «Підключений автомобіль» відкриває безмежні можливості для операторів мобільного зв'язку, виробників чіпів, апаратних засобів та програмного забезпечення. Розробниками операційних систем для підключеного автомобіля бажають стати світові гіганти на кшталт Google, Apple та Linux Foundation [11].

Існує 5 способів підключення транспортного засобу до оточення та обміном данними з ним (Рисунок 2.2):

- V2I «Vehicle to Infrastructure»: технологія збирає дані, згенеровані транспортним засобом, і надає водієві інформацію про інфраструктуру.

Технологія V2I передає інформацію про безпеку, мобільність або умови, пов'язані з навколишнім середовищем.

- V2V " Vehicle to Vehicle " "Від транспортного засобу до транспортного засобу ": технологія передає інформацію про швидкість і положення навколишніх транспортних засобів за допомогою бездротового обміну інформацією. Мета полягає в тому, щоб уникнути аварій, зменшити затори та позитивно вплинути на навколишнє середовище.
- V2C " Vehicle to Cloud ": Технологія обмінюється інформацією про та для застосування автомобіля з хмарною системою. Це дозволяє автомобіль використовуючи інформацію від інших, хоча хмари пов'язано такими галузі, як енергетика, транспорт і розумних будинку і використання робить з IoT .
- V2P «Vehicle to Pedestrian»: технологія сприймає інформацію про навколишнє середовище та передає її іншим транспортним засобам, інфраструктурі та персональним мобільним пристроям. Це дає змогу транспортному засобу спілкуватися з пішоходами та має на меті покращити безпеку та мобільність на дорозі.
- V2X «Vehicle to Everything»: технологія з'єднує всі типи транспортних засобів та інфраструктурних систем з іншими. Це сполучення включає автомобілі, шосе, кораблі, потяги та літаки [12].

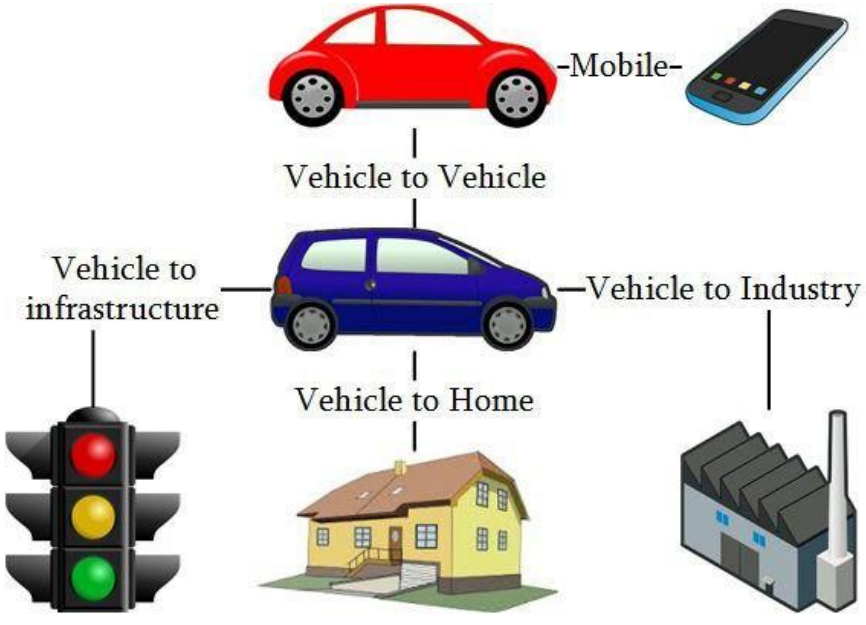


Рисунок 2.2 – Концепція підключених автомобілей

2.1.1 Застосування підключених автомобілей

Сучасні автомобілі включають в себе вбудовані навігаційні системи, інтеграцію смартфонів та мультимедійні пакети. Як правило, підключений автомобіль, виготовлений після 2010 року, має головний пристрій, систему розваг автомобіля, вбудовану систему з екраном, з якого водій може бачити роботу з'єднань або керувати ними. Типи функцій, які можна створити, включають відтворення музики/аудіо, програми для смартфонів, навігацію, допомогу на дорозі, голосові команди, контекстну допомогу/пропозиції, програми для паркування, керування двигуном та діагностику автомобіля.

Все частіше підключені автомобілі (і особливо електромобілі) використовують переваги розвитку смартфонів, а програми доступні для взаємодії з автомобілем з будь-якої відстані. Користувачі можуть розблокувати свої автомобілі, перевірити стан акумуляторів на електромобілях, знайти місцезнаходження автомобіля або дистанційно активувати систему клімат-контролю.

Нововведення, які представлені до 2025 року, включають повну інтеграцію додатків для смартфонів, таких як зв'язування календаря смартфона, його відображення на лобовому склі автомобіля та автоматичний пошук адреси в навігаційній системі для записів у календарі. У довгостроковій перспективі навігаційні системи будуть інтегровані в лобове скло і за допомогою доповненої реальності проектуватимуть цифрову інформацію, як-от оповіщення та інформацію про дорожній рух, на реальні зображення з точки зору водія.

Найближчі інновації щодо керування зв'язками з транспортними засобами (VRM) передбачають розширені віддалені послуги, такі як відстеження GPS та персоналізовані обмеження використання. Крім того, розробляються послуги з технічного обслуговування, такі як облачні налаштування, що вимагають співпраці автодилерів, OEM-виробників і сервісних центрів.

Незважаючи на різні чинники ринку, існують також бар'єри, які заважали остаточному прориву підключеного автомобіля протягом останніх кількох років. Одним з них є той факт, що клієнти неохоче платять за додаткові витрати, пов'язані з вбудованим підключенням, і замість цього використовують свої смартфони як рішення для своїх потреб підключення в автомобілі. Оскільки цей бар'єр, ймовірно, збережеться, принаймні в короткостроковій перспективі, виробники автомобілів звертаються до інтеграції смартфонів, щоб задовольнити попит споживачів на підключення.

Ці послуги стосуються удосконаленої системи допомоги водію (ADAS), які залежать від сенсорного введення більш ніж одного транспортного засобу та забезпечують миттєву реакцію за допомогою автоматичного моніторингу, попередження, гальмування та керування. Вони залежать від миттєвого зв'язку між транспортним засобом, а також від інфраструктури, функціонуючи між брендами та національними кордонами та забезпечуючи міжбрендові та транскордонні рівні конфіденційності та безпеки. З цієї причини Національна адміністрація безпеки дорожнього руху США (NHTSA) у своєму попередньому сповіщенні про запропоновану нормотворчість (ANPRM) щодо зв'язку V2V виступила за регулювання у Конгресі США. NHTSA розпочав процес формування правил 13 грудня 2016 року, запропонувавши застосувати спеціальні технології зв'язку малої дальності (DSRC) у нових легких транспортних засобах. Згідно з цим пропонованим правилом, транспортні засоби транслюватимуть певний пакет даних, «базове повідомлення безпеки» (BSM) до десяти разів на секунду, вказуючи місце розташування транспортного засобу, курс і швидкість. У березні 2017 року GM став першим автовиробником у США, який представив DSRC як стандартне обладнання для серійного автомобіля Cadillac CTS. У США також діють відповідні стандарти — IEEE 802.11p — і правила частоти . У Європі частота гармонізована для безпеки транспорту і діє гармонізований стандарт, який називається ETSI ITS-G5. У ЄС немає жодного обмеження, щоб зобов'язувати

виробників транспортних засобів вводити Connect. Тривають обговорення нормативної бази для конфіденційності та безпеки.

2.2 Ризики використання підключеного автомобіля та його кібербезпека

Аналіз питань інформаційної безпеки на автомобільному транспорті вже давно є предметом не тільки аналізу, але й розробки рішень безпеки. По-перше, оскільки електронні компоненти використовуються для керування сучасними автомобілями, вони можуть бути вразливими з точки зору інформаційної безпеки [13]. У різних роботах, доступних у відкритому доступі, наводяться приклади успішних комунікаційних атак на системи сучасних автомобілів. Поява безпілотних автомобілів лише загострила проблему інформаційної безпеки [13]. У результаті виклики, пов’язані з можливостями сучасних транспортних засобів, були додані до їх викликів як безпілотних транспортних засобів. Як наслідок, це ускладнило розуміння проблем інформаційної безпеки та пов’язаних з ними вимог.

Впровадження систем V2X ще більше ускладнює завдання забезпечення кібербезпеки. В екосистемі буде більше елементів і нових учасників у процесі взаємодії з автомобілями. На рисунку 2.3 показана загальна діаграма екосистеми V2X зі списком найбільш актуальних кіберзагроз.

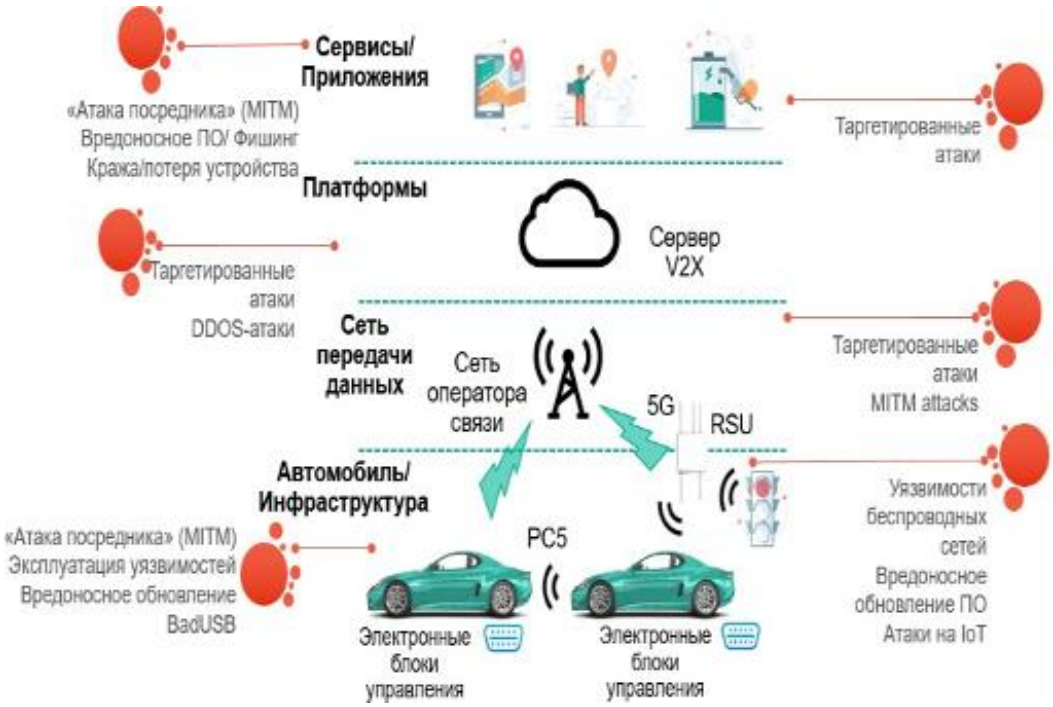


Рисунок 2.3 – Актуальні загрози інформаційній безпеці підключеного автомобіля

На практиці зловмисники мають багато можливостей отримати несанкціонований доступ до системи. Наприклад, виробники автомобілів зосереджуються на розвитку кібербезпеки в автомобілях, але в той же час вони не приділяють достатньо уваги розробці додатків, які взаємодіють з автомобілями з точки зору інформаційної безпеки. Дослідження показують, що розробникам додатків бракує розуміння поточних загроз для мобільних платформ під час розробки додатків та створення інфраструктури.

Концепція базується на цікавому поєднанні вимог безпеки, які потребують певних деталей та тлумачення.

Перший пункт, з якого починається аналітичний розділ концепції, — це вимога щодо однозначної фізичної ідентифікації користувачів безпілотних транспортних засобів.

Наприклад, нинішнім користувачам послуг таксі чи громадського транспорту не потрібно ідентифікуватись, вони лише фактично підвозять анонімних пасажирів і оплачують проїзд. Для безпілотних автомобілів прийнята зовсім інша концепція. Перевезення анонімними користувачами не

дозволяється [14]. Концепція тепер передбачає надання потенційними пасажирами біометричних даних. У цьому випадку використовується термін автентифікація, а не ідентифікація. Перевірка достовірності наданих даних повинна бути здійснена до початку поїздки.

При цьому концепція одразу передбачає, що отримані персональні дані не можуть бути використані третіми особами, тому необхідно передбачити низку заходів щодо забезпечення інформаційної безпеки, починаючи з введення (подання) в безпілотні транспортні системи. Обробка та зберігання в системах операторів безпілотного транспорту. Це означає, як мінімум, що оператор безпілотного транспортного засобу стає оператором персональних даних.

Другою важливою вимогою концепції є запобігання придушенню або перехопленню управління дроном. Іншими словами, придушення або можливе розкрадання функцій управління неприпустимі. Розглянемо вимоги щодо запобігання перехоплення контролю в безпілотних транспортних засобах.

Є дві можливі реалізації цієї ідеї. У першому випадку зловмисник може підключитися до шини CAN безпілотного автомобіля. Це означає, що роз’єми повинні бути не тільки фізично захищені, але й мати систему захисту, яка повідомляє про спроби несанкціонованого фізичного доступу. Другий варіант передбачає виключення можливості підключення дрона до центру управління та каналу взаємодії. Тобто слід виділити факт атаки MITM по каналу радіозв'язку. Водночас ця концепція відноситься до мінімізації ризику, що передбачає застосування ризик-орієнтованого підходу до контрольного перехоплення.

Іншими словами, концепція представляє потенційний ризик неконтрольованого перехоплення транспортного засобу, що означає прийняття можливої шкоди, пов’язаної з крадіжкою, за статистичною шкалою. При аналізі цього розділу концепції варто звернути увагу на одночасне використання термінів «інформаційна безпека» та «кібербезпека».

Очевидно, що вимоги до функціональної, промислової та кібербезпеки для безпілотних транспортних засобів залишаються, але з точки зору кібербезпеки вимога щодо контролю без перехоплення є.

Наступний ключовий пункт концепції: Обов'язкова вимога – своєчасне та швидке оповіщення водіїв про наявність загрози інформаційній безпеці. Щоб усунути загрозу або наслідки пограбування, потрібен час, тому коригувальні дії повинен вжити водій або система автономного водіння. З точки зору експертів з інформаційної безпеки, була прийнята концепція, згідно з якою неможливо розрізнити появу збою системи та збій через фізичне пошкодження та збій. Це результат аналізу подій, який зазвичай виконується постфактум. Результатом нападу може бути, наприклад, відмова гальмівної системи. На промислових підприємствах мінімізація наслідків події (незалежно від причини) часто реалізується як звичайна функція зупинки. Це означає, що ці концепції потрібно буде впроваджувати в безпілотних автомобілях, а дороги по всій довжині оснащувати спеціальними «кишенями», на зразок «пасток» для гірських перевалів.

2.2.2 Нормативні вимоги щодо безпеки

Як зазначено в концепції, враховуються стандарти, що застосовуються до безпеки транспортних засобів, враховуючи, що «звіти про кібербезпеку, засновані на єдиних стандартах, повинні бути серед документів, необхідних для дозволу на експлуатацію високоавтоматизованих транспортних засобів».

Питання функціональної безпеки розглядаються в серії стандартів ISO 26262, яка, судячи з наявних даних, була значно оновлена в 2018 році. У цій серії I SO 26262-10 Second edition 2018-12 Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262 - містить огляд і подальше пояснення інших стандартів серії. Питання безпеки розглядаються на основі стандартного підходу з точки зору захисту інформації і на практиці зводяться до коректності та надійності програмного забезпечення.

Питання кібербезпеки охоплюються спеціальними стандартами. Аналіз іноземної нормативної бази показав, що ISO/SAE DIS 21434 Road Vehicles – Cybersecurity Engineering. Структура стандарту, що розглядається, наведена на рисунку 2.4.

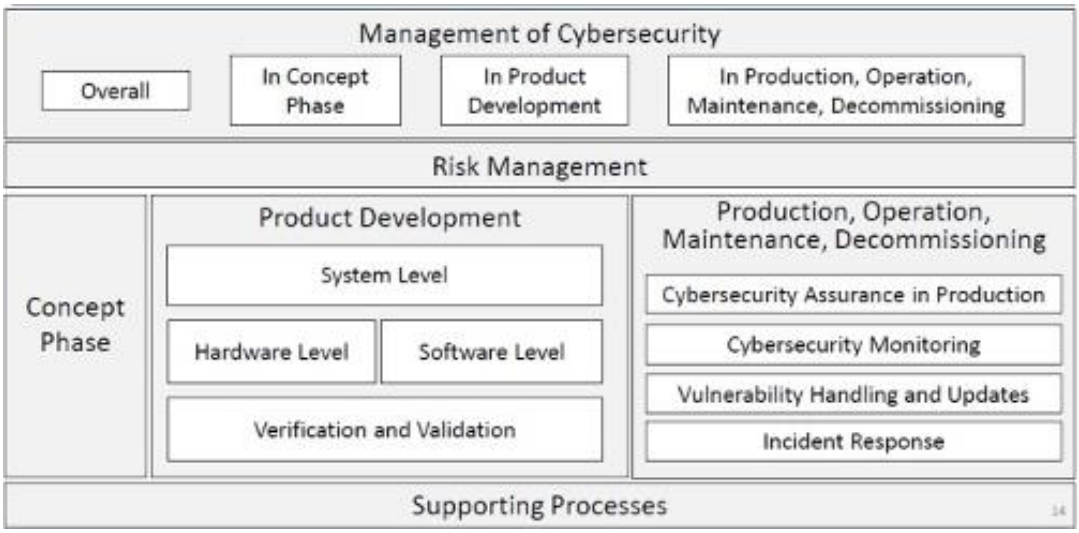


Рисунок 2.4 – Структура стандарта ISO/SAE 21434.

2.2.3 Перспективи розвитку вимог до кібербезпеки підключеного автомобіля

Розвиток систем автономного водіння, електрифікації, підключеного автомобіля до мережі і систем загального користування справили фундаментальний вплив на галузь. В даний час в автомобільній промисловості відбувається серйозна зміна підходів до налаштування електроніки автомобіля [16].

У сучасному автомобілі електроніка побудована на децентралізованій архітектурі та використовується понад 100 різних електронних пристроїв. Загальною тенденцією майбутнього є консолідація електроніки за доменами (4-е покоління) з наступною централізацією та використанням високопродуктивних контролерів (5-е покоління). Дійсно, в автомобілях майбутнього буде набагато менше електронних компонентів, але завдяки високій продуктивності та технологіям віртуалізації один і той же контролер

може виконувати різні завдання та запускати програми з різними вимогами до функціональності та забезпечення кібербезпеки.

Централізація архітектури тягне за собою поділ апаратної та програмної платформ. Системи всередині транспортного засобу створені за багаторівневою архітектурою з чіткими точками абстракції на рівні операційної системи (ОС) і проміжного програмного забезпечення. Зросте кількість рядків коду в електронних блоках, що також вплине на підхід до забезпечення кібербезпеки.

Європейська економічна комісія ООН (ЄЕК ООН) підготувала дві нові статті:

- Уніфіковані правила схвалення транспортних засобів, пов’язані з системами кібербезпеки та управління кібербезпекою

- Процес оновлення програмного забезпечення автомобіля та системи керування оновленнями програмного забезпечення.

Після того, як ці документи будуть прийняті державами-членами ЄЕК ООН і Всесвітнім форумом з гармонізації правил щодо транспортних засобів, автовиробники повинні будуть запровадити певні методи кібербезпеки та оновити програмне забезпечення. Згідно з проектом документа WP.29 ЄЕК ООН, стандарти кібербезпеки та оновлення програмного забезпечення повинні включати:

• Автовиробники повинні з першого кроку розробляти безпечні транспортні засоби, використовуючи найсучасніші методи розробки апаратного та програмного забезпечення, проектувати, виробляти та тестувати транспортні засоби та пов’язані з ними компоненти екосистеми з точки зору кібербезпеки та забезпечувати всю кібербезпеку. Ризики належним чином зменшені.

• Виявлення та реагування. Виробники транспортних засобів повинні мати можливість виявляти технічні вразливості та проблеми безпеки, які можуть вплинути на безпеку чи безпеку їхніх транспортних засобів.

• Безпечні та надійні оновлення. Автомобільні гравці повинні мати можливість реагувати на будь-яку виявлену подію безпеки та надавати оновлення програмного забезпечення для вирішення проблем безпеки.

2.3 Висновки до розділу 2

У другому розділі було досліджено тенденції розвитку підключеного автомобіля зрозуміло, що ринок автотранспорту буде зростати на користь підключених автомобілей. Проаналізовано концепцію підключеного автомобіля, як технологія «Підключений автомобіль» відкриває безмежні можливості для операторів мобільного зв'язку, виробників чіпів, апаратних засобів та програмного забезпечення. Розробниками операційних систем для підключеного автомобіля бажають стати світові гіганти на кшталт Google, Apple та Linux Foundation [11].

– Учасники ринку зобов’язані забезпечити комплексне управління ризиками та визначити суміжні компоненти екосистеми, які можуть вплинути на транспортний засіб, а також на безпеку. Необхідно вжити заходів для зменшення таких ризиків.

– Виробники транспортних засобів повинні мати можливість виявляти технічні вразливості та проблеми безпеки, які можуть вплинути на безпеку чи безпеку їхніх транспортних засобів.

3 МІЖНАРОДНІ СТАНДАРТИ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ТРАНСПОРТНИХ ЗАСОБІВ

Прогнози втрат світового виробництва автомобілів через нестачу напівпровідників продовжують зростати. У січні аналітики прогнозували, що через дефіцит буде вироблено на 1,5 мільйона автомобілів менше; до квітня це число збільшилося до більш ніж 2,7 мільйона одиниць, а до травня — до 4,1 мільйона одиниць.

Дефіцит напівпровідників не лише підкреслив крихкість ланцюжка поставок для автомобілів, а й привернув увагу автомобільної промисловості до десятків прихованих комп'ютерів, які сьогодні вбудовані в автомобілі.

У найближчі роки відбудуться ще більші зміни, оскільки все більше автовиробників зобов'язуються поступово відмовлятися від своїх автомобілів з двигунами внутрішнього згоряння (ДВЗ) для досягнення глобальних цілей щодо запобігання зміні клімату, замінюючи їх електромобілями (EV), які зрештою будуть здатні працювати автономно.

Колись програмне забезпечення було лише частиною машини. Наразі програмне забезпечення визначає вартість автомобіля. Успіх автомобіля набагато більше залежить від програмного забезпечення, ніж від механічного боку. Майже всі інновації, вироблені автовиробниками або виробниками оригінального обладнання (OEM) тепер прив'язані до програмного забезпечення.

Кількість програмного забезпечення, розробленого для виявлення неналежної поведінки для забезпечення якості та безпеки, збільшується. Третина програмного забезпечення ЕБУ була спрямована на забезпечення якості роботи десять років тому, тепер більш як наполовину або більше, спрямована на безпеку критично важливих систем.

Останнім часом спостерігається зростання кількості дефектів компонентів, пов'язаних з автомобільною електронікою, яка переходить від

зручності власника до компонентів, критично важливих для безпеки(Рисунок 3.1)

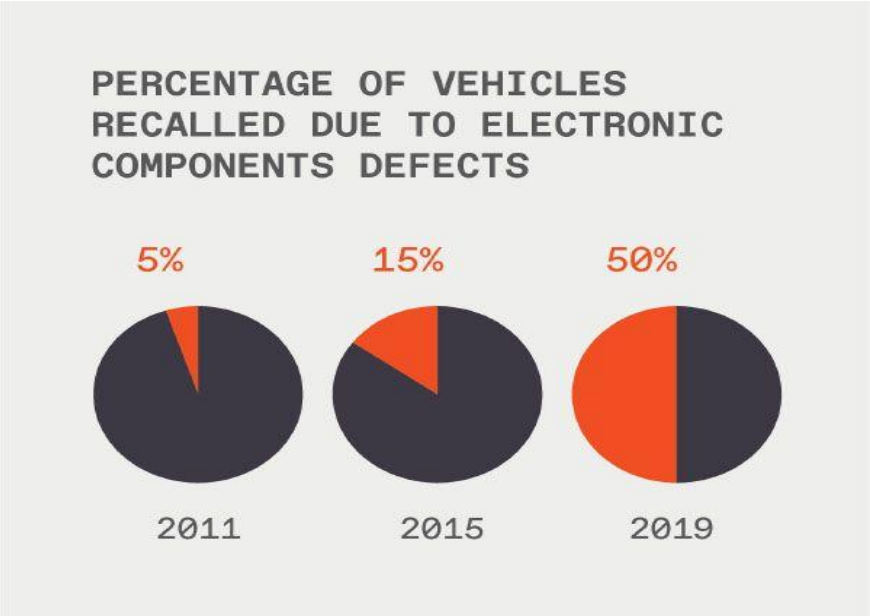


Рисунок 3.1 – Відсоток відкликаних автомобілів через дефекти електронних компонентів

3.1 Організації, що забезпечують кібербезпеку підключеного автомобіля

У автомобілебудуванні приблизно шість років тому серйозно взялись за кібербезпеку, почали інвестувати у проектування та розгортання кіберзахисних рішень. Сьогодні в автомобільній індустрії кібербезпека забезпечується як апаратними, так і програмними рішеннями, але чекає довгий шлях, перш ніж всі до одного ECU (електронні блоки управління) в машині будуть захищені від кібератак, що активізуються.

Кібербезпека в автомобілебудуванні набагато складніша, ніж на смартфонах та ПК, з двох основних причин:

1. Десятки ЕБУ в кожній машині, з'єднані безліччю електронних шин і відповідають за різні швидкості та характеристики.

2. Безліч потенційних точок доступу, як розташованих усередині автомобіля, так і віддалених, зокрема, OBDII, USB і SD-порти, безключовий доступ, Bluetooth та Wi-Fi, вбудований модем, датчики, інфотейнмент або

програми для смартфонів, а також безліч підключень із застосуванням телематики та інших хмарних систем, що мають доступ до систем автомобіля.

Формується кілька стандартів та регламентів, що регулюють кібербезпеку, що додатково сприяє розгортанню кіберзахисних рішень у всіх підключених автомобілях.

У таблиці 3.1 узагальнено аспекти кібербезпеки. Організації, що забезпечують кібербезпеку:

- ISAC в автопромі

У більшості галузей сформовано організації для боротьби за кібербезпеку; зазвичай їх називають "Центрами обміну інформацією та аналізу" (ISAC). Організація Auto-ISAC створена у серпні 2015 року; вона оперує центральним вузлом з обміну, відстеження та аналізу виявлених даних про кіберзагрози, уразливості та інциденти, пов'язані з підключеними транспортними засобами. Її штаб-квартира знаходиться у Вашингтоні, округ Колумбія, На організації, що перебувають у Auto-ISAC, припадає понад 99% легкових автомобілів, проданих у Північній Америці; також ця організація включає понад 45 глобальних виробників обладнання (OEM) та постачальників. Членство в Auto-ISAC розширилося, у ньому вже беруть участь виробники запчастин для важких вантажівок та їх постачальники, а також сектор комерційного транспорту, зокрема таксопарки. До постачальників належать компанії вищого ешелону, такі як Argo, Intel, Motional і Waymo. Також триває кооперація з іншими організаціями. Auto-ISAC координує роботу з 23 іншими ISAC, які контролюють ключові інфраструктурні сфери, зокрема охорону здоров'я, авіацію, телекомунікації та фінансові послуги.

- ENISA

Агентство з мережевої та інформаційної безпеки Євросоюзу (ENISA) – це орган ЄС, який займається забезпеченням кібербезпеки в масштабах Європи. ENISA бере участь у формуванні кіберполітики ЄС, сприяє підвищенню довіри до продукції ІКТ, послуг та процесів, пов'язаних із

сертифікацією кібербезпеки. ENISA активно діє в галузі кіберзахисту автомобілів та випустило кілька важливих звітів.

Таблиця 3.1 – Автомобільна кібербезпека: поточний стан

Тема	Ключова інформація
Статус загроз, щодо кібербезпеки	Попередній звіт з робіт у галузі автомобілебудування Посилання на звіт: https://upstream.auto/2021report/ Частка black hat-атак від загальної кількості збільшується
Організації, що забезпечують кібербезпеку	Auto-ISAC: хаб для обміну інформацією про кібербезпеку ENISA: агентство ЄС з питань кібербезпеки
Регламентація кібербезпеки	Документ WP.29 ЄЕК ООН: незабаром значно вплине на галузь Фреймворк IEEE Uptane; кіберзахист для оновлень OTA
Документ WP.29 ЄЕК ООН, присвячений кібербезпеці	Регулюючий документ WP.29 прийнято у червні 2020 року CSMS: системи управління кібербезпекою SUMS: системи управління оновленнями програм Впровадження починається у 2021 та 2022 роках

Продовження таблиці 3.1

Огляд технологій кібербезпеки	Апаратне забезпечення кібербезпеки Вбудоване програмне забезпечення для кібербезпеки Хмарне відстеження кібербезпеки
Гравці на ринку кібербезпеки	Компанії, зайняті розробкою кіберзахисного ПЗ Огляд кібербезпеки в компаніях 1-го ешелону Захищені чіпи для процесорів
Потенціал ринку кібербезпеки	Програмні клієнти для кібербезпеки Хмари для кібербезпеки, що надаються як SaaS

У лютому 2021 року ENISA опублікувало документ «Виклики кібербезпеки, пов'язані із впровадженням штучного інтелекту в автономному керуванні». Звіт дозволяє скласти враження про виклики кібербезпеки, пов'язані з використанням ШІ-технологій в автомобілях. Проблема описана в контексті політики, що реалізується як на європейському, так і на широкому міжнародному рівні.

У листопаді 2019 року ENISA опублікувало документ «Рекомендації щодо забезпечення інформаційної безпеки розумних автомобілів». У цьому звіті визначено рекомендовані практики щодо забезпечення безпеки підключених автомобілів та напівавтономних транспортних засобів. У 2017 році ENISA опублікувало документ «Кібербезпека та надійність розумних автомобілів», в якому основну увагу приділено практикам, що рекомендуються, для виробників автомобільних комплектуючих і для постачальників з метою захистити вбудовані автомобільні системи від кібератак.

Основна вимога до стандартів та регламентів у галузі кібербезпеки – захистити автомобіль протягом усього його життєвого циклу, від проектування, до виробництва та далі до використання клієнтом.

3.2 Регламентація кібербезпеки підключеного автомобіля

Після дворічної підготовки та редагування ООН 24 червня 2020 року ухвалила документ WP.29 ЄЕК, який регулює питання кібербезпеки. WP.29 діє у 54 країнах, у тому числі ЄС, Великобританії, Японії та Південній Кореї. На ці 54 країни припадає близько 35% світового виробництва автомобілів. У багатьох інших країнах приймаються автомобілі, які відповідають нормам ООН. США не входять до цих 54 країн. Усі виробники, у тому числі, автовиробники зі США, які продають автомобілі на цих ринках, повинні дотримуватися вимог кібербезпеки, викладених у WP.29, стосовно всієї їх продукції та процесів.

Регламенти ООН юридично забезпечені. Якщо країна або регіон приймає регламент WP.29, то всім виробникам комплектуючих, що діють у ній, потрібен доказ відповідності для проходження обов'язкової сертифікації та подальшого права роботи на ринку. У Європі проходження обов'язкової сертифікації потребує взаємного визнання відповідності нормам на рівні всього автомобіля. Якщо виробник отримує сертифікат на автомобіль певного типу в одній країні ЄС, може продавати таку модель у всіх країнах ЄС без подальших перевірок.

Регламент WP.29 складається з двох основних директив з кібербезпеки автомобілів.

ISO/SAE 21434 розробляє новий стандарт кібербезпеки для транспортних засобів з акцентом на додаткове забезпечення кібербезпеки на етапі інженерного опрацювання автомобіля. Цей стандарт описує вимоги щодо управління ризиками, пов'язаними з кібербезпекою, наголошуючи на вибудовуванні процесу та загальної термінології для обміну інформацією

щодо таких ризиків та їх усунення. Стандарт не містить опису конкретних технологій або пропозицій щодо конкретних рішень, пов'язаних з кібербезпекою.

Цей стандарт розроблено спільною робочою групою від організацій ISO та SAE та буде опубліковано обома. Понад 25 автовиробників та 20 постачальників вищого ешелону беруть участь у розробці стандарту. Чистову версію стандарту ISO/SAE 21434 було підготовлено у березні 2021 року. Ймовірно, що публікація стандарту відкладається до 2022 року.

Роботи зі стандартизації, що проводяться ISO/SAE 21434, пов'язані та розробляються у координації з діяльністю ЄС та ЄЕК за документом WP.29.

Ще один важливий стандарт – Uptane, розроблений для оновлень програм OTA. Uptane офіційно запроваджено у січні 2017. Альянс Uptane утворено у 2018. Це некомерційна організація під егідою Галузевої організації IEEE за стандартами та технологіями (ISTO). Uptane було оформлено у вигляді стандарту IEEE/ISTO 6100 у липні 2019, тоді вийшла версія 1.0. Альянс Uptane забезпечуватиме нагляд над новими стандартами Uptane, так, версія Uptane 1.1 була введена в січні 2021. Багато компаній пропонують програмні продукти, що відповідають стандарту Uptane. software products.

У червні 2020 року було прийнято дві нові регулюючі норми ООН з кібербезпеки, в рамках документа WP.29. Обидві регулюючі норми застосовуються до транспортних засобів усіх типів, оновлені в березні 2021. Впровадження цих норм у деяких країнах розпочнеться у 2021 та 2022 роках, ширше впровадження – у 2023 та 2024 роках.

3.3 Вимоги правил ЄЕК ООН щодо кібербезпеки підключеного автомобіля

До вимог правил ЄЕК ООН відносять:

- Впровадження процесів управління кібербезпекою в рамках розробки автомобілів:

У пункті 7.2.2.1. Правил ЄЕК дження ООН 155 вказується вимога до автовиробників запровадити процес безпечної розробки на етапі розробки, етапі виробництва та етапі постпродакшну. Загалом автовиробник може брати зразки побудови цих процесів з рекомендацій стандарту ISO 21434:2021.

- Впровадження процесів управління ІБ та кібер-ризиками компанії в цілому:

Пункт 7.2.2.2. розділ А вказує на необхідність автовиробника проводити ризик-менеджмент, підготувавши необхідну документацію (наприклад, провести Threat Analysis and Risk Assessment відповідно до вимог ISO 21434:2021).

- Впровадження моніторингу інцидентів та вразливостей, а також реагування на них

Пункт 7.2.2.4 вказує на необхідність проведення постійного моніторингу інцидентів та уразливостей транспортних засобів та IT екосистеми загалом. Саме для реалізації цієї вимоги Правил ООН, нами було розроблено AutoVisor-SIEM (гіперпосилання на сторінку на сайті).

- Впровадження процесів управління кібербезпекою в рамках розробки автомобілів:

У пункті 7.2.2.1. Правил ЄЕК ООН 155 вказується вимога до автовиробників запровадити процес безпечної розробки на етапі розробки, етапі виробництва та етапі постпродакшну. Загалом автовиробник може брати зразки побудови цих процесів з рекомендацій стандарту ISO 21434:2021.

- Впровадження процесів управління ІБ та кібер-ризиками компанії в цілому:

Пункт 7.2.2.2. розділ А вказує на необхідність автовиробника проводити ризик-менеджмент, підготувавши необхідну документацію (наприклад, провести Threat Analysis and Risk Assessment відповідно до вимог ISO 21434:2021).

- Впровадження моніторингу інцидентів та вразливостей, а також реагування на них

Пункт 7.2.2.4 вказує на необхідність проведення постійного моніторингу інцидентів та уразливостей транспортних засобів та IT екосистеми загалом. Саме для реалізації цієї вимоги Правил ООН, нами було розроблено AutoVisor-SIEM (гіперпосилання на сторінку на сайті).

- Впровадити процес детекції кібератак

У пункті 7.3.7. вказується на необхідність автовиробника реалізувати комплекс заходів, спрямованих на виявлення та запобігання інформаційним атакам на транспортні засоби, проводити моніторинг подій безпеки та проводити розслідування за результатами інцидентів. Для реалізації вимог Правил ЄЕК ООН 155 у цій частині, нами було розроблено AutoVisor-IDS (гіперпосилання) – Система виявлення кібератак, яка може передавати дані для аналізу у AutoVisor-SIEM (гіперпосилання)

- Впровадження безпечних процесів оновлення

Окрему увагу приділено питанням організації процесу безпечного оновлення. Так, Таблиця B2 у додатку до Правил ЄЕК ООН повністю присвячена опису заходів щодо усунення загроз, пов'язаних із «Процесом оновлення» (OTA). Більш детальна інформація щодо заходів кібербезпеки, які необхідно зробити під час побудови процесу оновлення програмного забезпечення, описані в пункті 9.3. Правил ЄЕК ООН 156.

Процес впровадження вимог ЄЕК ООН зображен на рисунку 3.4.

Рисунок 3.4 – Процесс впровадження вимог

Виконання вимог правил підтверджується двома документами:

Сертифікат CSMS – Cyber Security Management System (сертифікат, що підтверджує наявність системи керування кібербезпеки у OEM). Сертифікат видається на OEM загалом та діє протягом 3-х років.

Сертифікат VTA - Vehicle Type Approval (сертифікат, що підтверджує те, що автомобіль розроблений з урахуванням вимог кібербезпеки (SDLC). Сертифікат видається на весь термін життя кожного окремої моделі.

3.4 Висновки до розділу 3

В третьому розділі було детально розглянуто та про аналізовано сучасний стан регулювання міжнародних організацій та оновлення нових стандартів кібербезпеки підключеного автомобіля. Згідно останніх стандартів ISAC, ENISA, ISO/SAE, Uptane було досліджено сучасний стан автомобільної кібербезпеки, передбачено ризи з кібератак та їх запобіганню.

4 СИСТЕМА СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

4.1 Документ ООН з кібербезпеки ECE/TRANS/WP.29/GRVA/2022/5.

WP.29 ЄЕК ООН (United Nations Economic Commission for Europe (UNECE) World Forum for the Harmonization of Vehicle Regulations. Originally named the Working Party (WP)) – це Всесвітній форум Європейської економічної комісії ООН (ЄЕК ООН) з гармонізації правил щодо транспортних засобів. Спочатку названий Робочою групою (WP) експертів з технічних вимог до транспортних засобів, форум визначає критерії для затвердження типу колісних транспортних засобів, обладнання та частин і є найбільшою міжнародною системою регулювання транспортних засобів у світі.

Його основний обов’язок полягає в тому, щоб оновлювати та відповідати правилам щодо транспортних засобів, щоб підтримувати міжнародну торгівлю та доступ до ринку. Станом на 2020 рік кількість договірних сторін (ДС) угоди ЄЕК ООН 1958 року зросла до 54, включаючи всі країни ЄС та інші країни ОЕСР, такі як Японія, Туреччина, Росія, Австралія та Південна Африка [23].

У першому документі основна увага приділяється кібербезпеці та системам управління кібербезпекою (CSMS) [20].

Визначення WP.29 CSMS: під CSMS розуміється систематичний підхід на основі оцінки ризиків, який визначає організаційні процеси, зони відповідальності та управління для правильного трактування ризиків, пов'язаних з кіберзагрозами транспортних засобів та із захистом транспортних засобів від кібератак.

У документі CSMS добре розглянуті загрози, пов'язані з кібербезпекою, наведено великий перелік уразливостей та методів атаки. У таблиці 3.2, наведених нижче, узагальнено погрози та вразливості. Існує 6 типів загроз і

безліч типів уразливостей (29) з безліччю прикладів (67), перелічених у документі CSMS.

Таблиця 3.2 – Резюме загроз і вразливостей з кібербезпеки за документом WP.29

Таблиця №	Тип загрози
A1	Сервер бази даних для машин, що знаходяться в дорозі Канали комунікації між машинами Процедури оновлення для автомобілів Сполучність та з'єднання між автомобілями Дані та програмний код для автомобілів Уразливості, пов'язані з недостатньою захищеністю чи міцністю систем

У наступній таблиці 3.3 резюмовано заходи щодо запобігання загрозам з кібербезпеки, описані в документі CSMS. Дані з таблиці B описують загрози, що виникають на борту автомобіля, дані таблиці C – загрози, що виникають поза автомобілем. Другий регулюючий документ норми ООН щодо кібербезпеки, в рамках документа WP.29 стосується процесів оновлення програмного забезпечення та систем управління такими оновленнями (SUMS).

Система управління оновленнями програм – це систематичний підхід, що визначає, які організаційні процеси та процедури повинні відповідати вимогам щодо доставки програмних оновлень згідно з цим регулюючим документом.

Нова регулююча норма ООН про універсальні передумови до оновлень програм та систем управління оновленнями програм застосовується до автомобілів, робота яких залежить від оновлення програмного забезпечення.

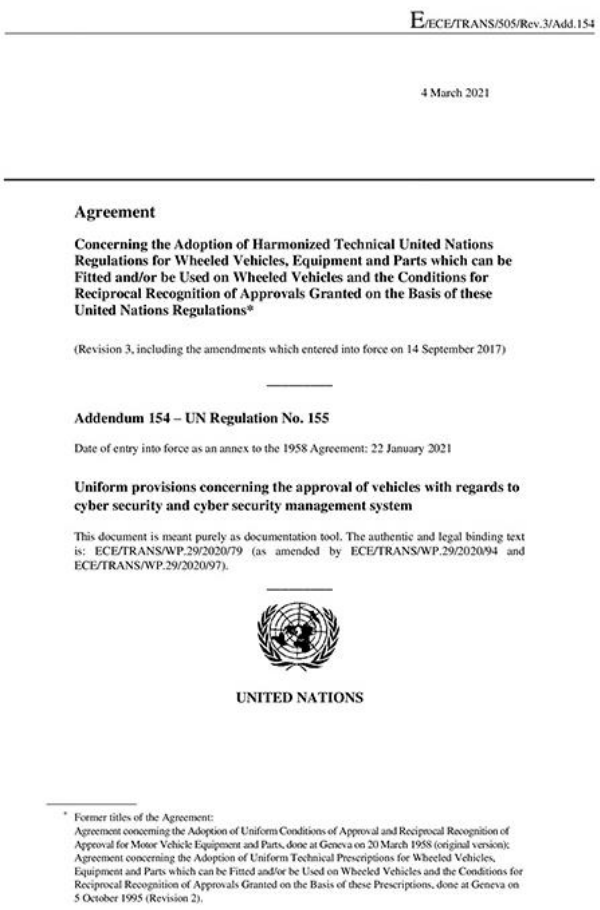
Вимоги наказують отримання сертифікату (Рисунок 3.2) відповідності для компанії та Vehicle Type Approval для кожної моделі автомобіля. Без цих сертифікатів з 2024 року продавати ТЗ у низці країн буде неможливо.

Таблиця 3.3 – Резюме способів запобігання кіберзагрозам, пов'язаним з документом WP.29

Таблиця №	Запобігання загрозам, пов'язаним з	Усередині або поза машиною	Способів запобігання
B1	Канали комунікації між автомобілями	Усередині	20
B2	Процес оновлення ПЗ	Усередині	5
B3	Ненавмисні дії людини, що сприяють кібератаці	Усередині	2
B4	З'єднання із зовнішніми пристроями	Усередині	7
B5	Потенційна мета атаки та її мотивація	Усередині	14
B6	Вразливість, яка використовується у разі недостатнього захисту автомобіля	Усередині	8
B7	Втрата даних або крадіжка даних із автомобіля	Усередині	1

Продовження таблиці 3.3

B8	Фізичні маніпуляції із системою з метою створення умов для атаки	Усередині	1
C1	Сервери бази даних	Зовні	6
C2	Ненавмисні людські дії	Зовні	2
C3	Фізична втрата чи втрата даних	Зовні	3



E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

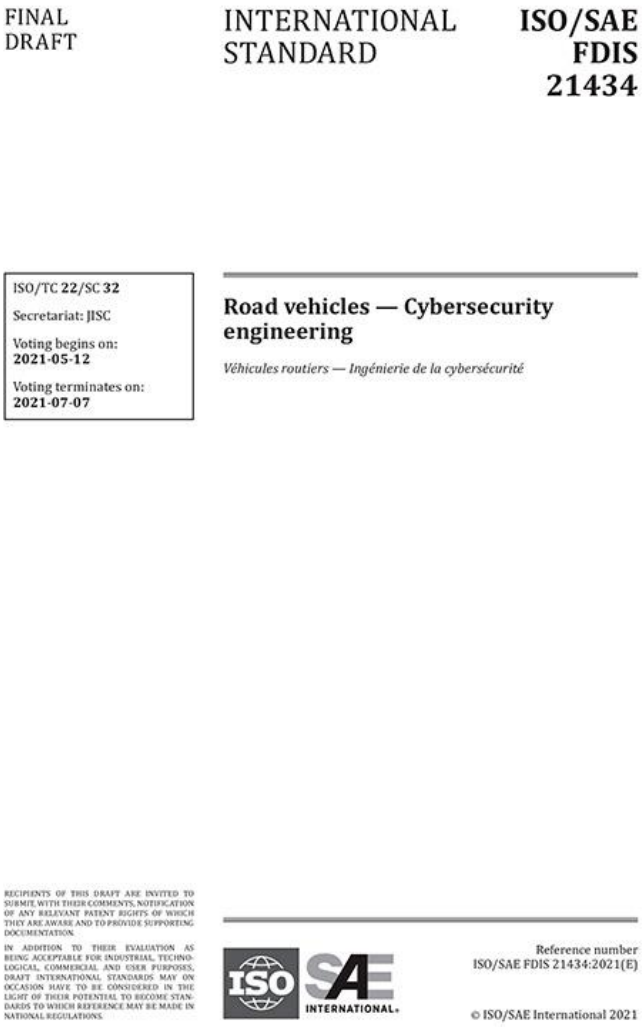
UNITED NATIONS

* Former titles of the Agreement:
Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).

Рисунок 3.2 – UN regulations WP29, ECE155, ECE156 — правила ООН про однакові положення щодо офіційного затвердження транспортних засобів щодо кібербезпеки та їх систем управління кібербезпекою

Стандарт багато в чому є основою для UN ECE 155 (Рисунок 3.3). Без впровадження процесів стандартів, що передбачаються, неможливо отримати сертифікати відповідності.

Впровадження вимог стандарту є обов'язковим для сертифікації


FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/SAE
FDIS
21434

ISO/TC 22/SC 32
Secretariat: JISC
Voting begins on:
2021-05-12
Voting terminates on:
2021-07-07

Road vehicles — Cybersecurity engineering

Véhicules routiers — Ingénierie de la cybersécurité

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/SAE FDIS 21434:2021(E)

© ISO/SAE International 2021

Рисунок 3.3 – ISO 21434 ISO/SAE 21434 «Дорожні транспортні засоби – Інженерія кібербезпеки», передбачає комплекс заходів автовиробникам.

4.2 Глобальна структура сертифікації продуктів. Послуг та процесів.

Кібербезпека сьогодні є серйозною проблемою для належного функціонування та безпеки цифрової економіки та державного управління в найближчому майбутньому.

Оцінка відповідності кібербезпеки (сертифікація) підключених автомобілів відіграє важливу роль у сфері автомобільних технологій. Наприклад кібербезпека програмного забезпечення, обладнання, ECU, хмарних сервісів, кібербезпека технологічних процесів та власна компетентність у питаннях кібербезпеки. Також важлива кібербезпека механізму використання підключеного автомобіля і самого підключеного автомобіля.

Система сертифікації встановлюється процедурами, правилами та управлінням сертифікації кібербезпеки, а система сертифікації складається з набору правил і процедур для управління подібними або тісно пов’язаними системами оцінки відповідності.

Сьогодні перед Україною стоїть важливе та актуальне завдання: розробка схем і систем сертифікації кібербезпеки підключених транспортних засобів на основі існуючої в країні системи технічного регулювання, а також досягнень у сфері оцінки відповідності та сертифікації. Вимоги законодавства України з кібербезпеки, ставить завдання застосування найвищих міжнародних та європейських принципів оцінки відповідності кібербезпеки.

Оцінка відповідності доводить, що «зазначені вимоги» до продукту, процесу, послуги, системи, особи чи органу були реалізовані (оцінка відповідності включає випробування, перевірку, верифікацію, перевірку, сертифікацію та діяльність із сертифікації). Визначені вимоги представляють потреби або визначені очікування та можуть бути отримані з директивних документів, таких як правила, стандарти та технічні специфікації. Об’єкт підлягає оцінці відповідності, якщо застосовуються «визначені вимоги».

Структура оцінки відповідності – це перелік правил і процедур, які описують, що підлягає оцінці на відповідність, визначають ці вимоги та забезпечують метод проведення оцінки відповідності. Структурою оцінки відповідності можна керувати в рамках системи оцінки відповідності. Система оцінки відповідності - перелік правил і процедур для управління подібними або тісно пов'язаними системами оцінки відповідності. Оцінка відповідності певним вимогам незацікавленою третьою стороною, органом з оцінки відповідності (CAB), називається сертифікацією.

Тільки за останнє десятиліття було створено багато систем і стандартів оцінки, які використовуються в усьому світі для сертифікації інформації та кібербезпеки. Найвідомішими з них є сімейство стандартів ISO/IEC 27000. Framework v1.1 Національного інституту стандартів і технологій США (NIST); стандарт сімейства ISO/SAE 21434; ООН WP.29.

Чітке використання встановлених систем сертифікації та стандартів можна знайти в основному в промислових системах сертифікації. Ця різноманітність створює значні технічні перешкоди для широкого або транскордонного визнання відповідних сертифікатів. Крім того, у секторі, який функціонує як глобальна та складна система, сама наявність або застосування різних вимог і процедур може становити значні ризики.

З метою усунення технічних бар’єрів для оцінки відповідності та акредитації сертифікатів створено Глобальну систему оцінки відповідності – перелік умов комплексної акредитації оцінок відповідності та сертифікатів.

Описана вище система є акредитацією органів з оцінки відповідності (ООВ), яка також включає органи сертифікації.

Організації, відповідальні за акредитацію в організаціях технічного регулювання, повинні оцінювати компетентність установи щодо сертифікації продукції, послуг і процесів, перевірок і персоналу, систем управління, а також випробувальних і калібрувальних лабораторій. Акредитація — це офіційне визнання, яке гарантує клієнтам і користувачам послуг компетентне функціонування певної організації. Акредитація надає транскордонну

акредитацію послуг в рамках Міжнародного форуму з акредитації (IAF) і Міжнародного комітету з акредитації випробувальних лабораторій (ILAC).

IAF та ILAC сприяють і регулюють визнання Двосторонніх або Багатосторонніх угод або домовленостей (MPA/MLA), в яких держави-учасниці зобов'язуються взаємно визнавати результати випробувань, перевірок, сертифікації чи акредитації. Угоди MRA/MLA тепер є важливим фактором оптимізації або скорочення кількості сертифікацій продуктів, послуг, систем, процесів і матеріалів, які особливо необхідні для міжнародної діяльності.

На рисунку 4.1 показано рівні та сфери, за якими національні органи з акредитації України акредитовані в глобальній системі IAF.

Рисунок 4.1 - Угода MRA та сфера в IAF

Система IAF/ILAC, описана вище, керується регіональними органами акредитації (які також є частиною цієї системи). на рисунках 4.2 і 4.3 показано географічне розташування цих організацій. Регіональним органом з акредитації в Україні є Європейська організація з акредитації (EA) [43].

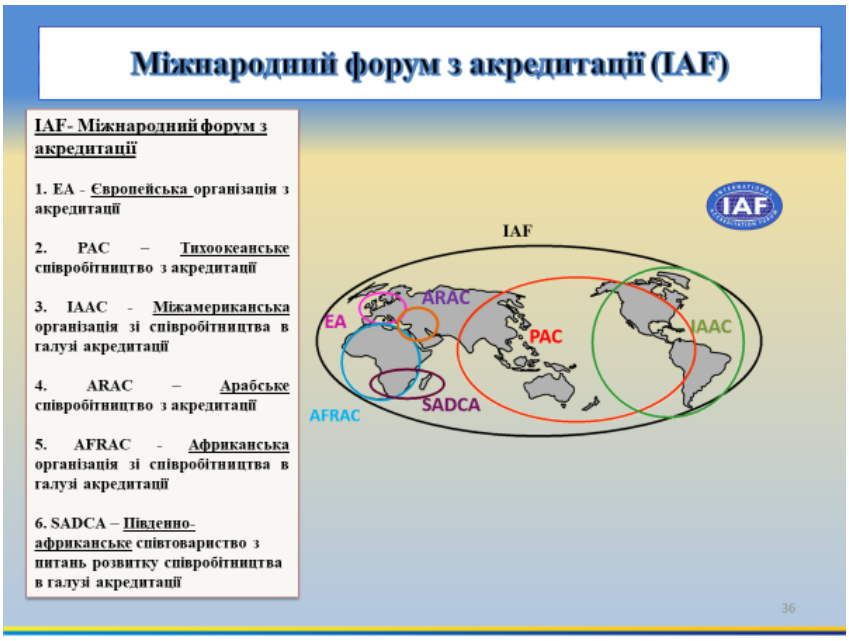


Рисунок 4.2 – Регіональні організації IAF

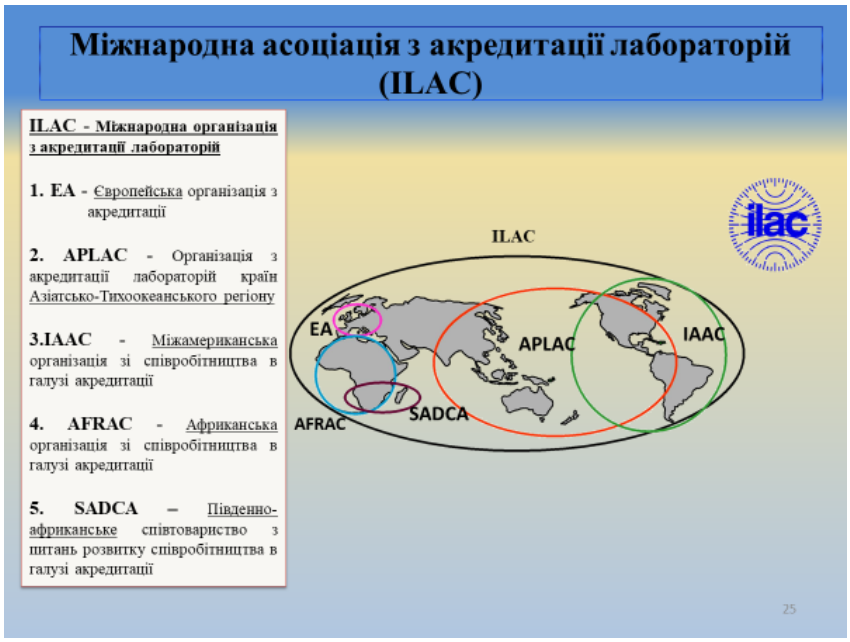


Рисунок 4.3 – Регіональні організації ILAC

4.3 Розробка схеми сертифікації кібербезпеки підключеного автомобіля для України

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, основнізасади 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.

Ієрархічна модель оціночних стандартів для схеми сертифікації кібербезпеки в автомобільній галузі дозволяє упорядити визначення та застосування стандартів чи інших нормативних документів, стандартів та схем з можливими комбінаціями для розробки схем сертифікації.

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 ЕА та в документах IAF та/або ILAC (затверджених ЕА як обов'язкові для ЄС) [44].

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 сертифікаціїкібербезпеки 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. Рівень 4 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 (30) 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», стаття 1 [44].

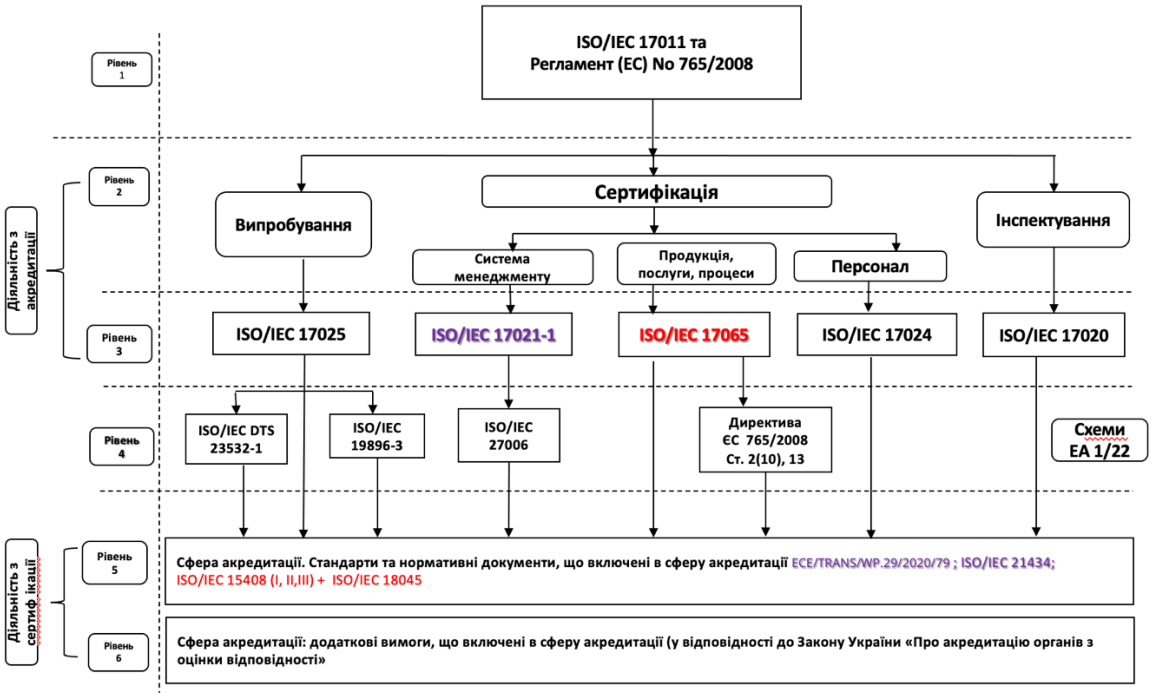


Рисунок 4.4 - Ієрархічна модель оціночних стандартів для схеми сертифікації кібербезпеки в автомобільній галузі

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.

На рис. 4.4 зображена 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.

-MLA (Mutual Recognition Arrangement) - Угода про взаємне визнання;

-MRA (Multilateral Recognition Arrangement) – Багатостороння угода про визнання

-BLA (Bilateral Recognition Arrangement) – Двостороння угода про визнання

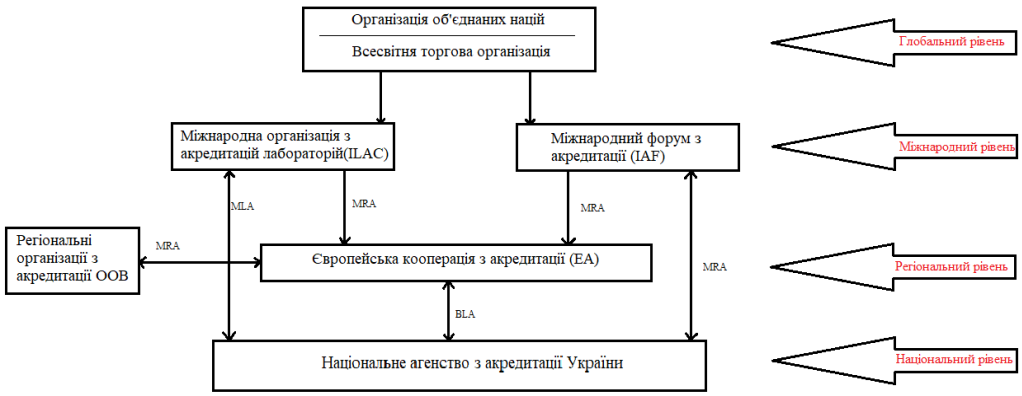


Рисунок 4.5 – Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки

Для створення ефективної Системи Оцінки Відповідності Кібербезпеки CSMS України доцільним є аналіз Угод, які є чинними для НААУ у системі EA 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.

Угоди, які визначають статус Національного органу України з акредитації ООВ щодо транскордонного визнання діяльності, показані на рисунках 4.6 та 4.7. 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.

Рисунок 4.6 – Угода MRA та сфера в ILAC

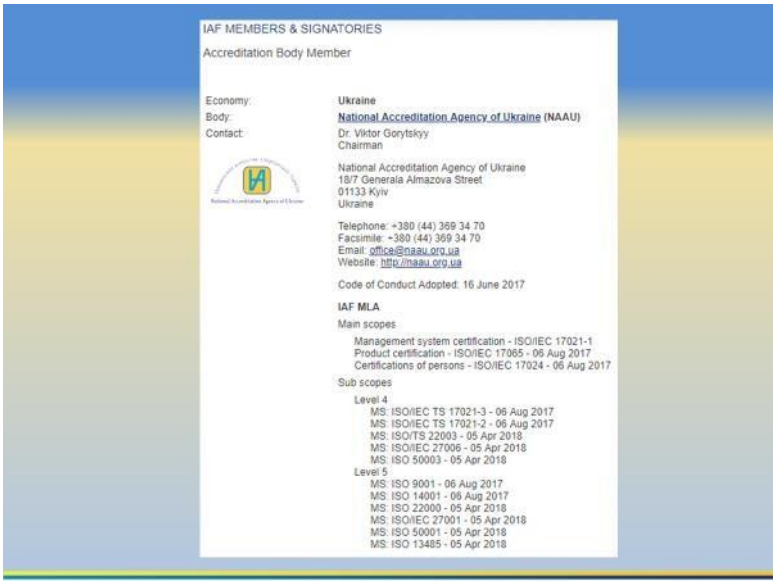


Рисунок 4.7 – Угода MRA та сфера в IAF

Цей проект Системи сертифікації кібербезпеки CSMS для України побудований на попередньому аналізі та баченні ЄС з цього питання, яке викладено в Акті з кібербезпеки ЄС [14]. Як зазначено вище, Система сертифікації формується з 7 основних елементів

1. Вимоги для оцінювання (стандарти чи інші нормативні документи). Сертифікат кібербезпеки CSMS 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 підключеного автомобіля.

2. Акредитація органів з оцінки відповідності (сертифікації). Після того, як буде прийнята схема сертифікації кібербезпеки, виробники або постачальники продуктів кібербезпеки пдіключеного автомобіля повинні мати можливість подавати заявки на сертифікацію своїх продуктів кібербезпеки транспортних засобів 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 кібербезпеки пдіключеного автомобіля 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 [39].

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 [14]. 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 [7]. Вимоги до призначених органів з сертифікації кібербезпеки повинні бути відповідними вимогам закону України «Про технічні регламенти та оцінку відповідності», який, у свою чергу, гармонізовані 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 [40]. Наприклад, мають власні акредитовані випробувальні лабораторії для проведення принаймні деяких видів випробувань продукції підключеного автомобія в межах сфери призначення.

Робочі версії схем 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 [10]. Повна версія схеми сертифікації, згідно зі стандартом, повинна мати у своєму складі 17 елементів. У роботі досліджено та визначені найбільш важливі та системоутворюючі елементи деяких схем сертифікації кібербезпеки. Такі версії схем будемо називати робочими. Дослідження спрямовано на гармонізацію національних схем сертифікації кібербезпеки з імовірними схемами сертифікації кібербезпеки ЄС [41].

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 піжключеного автомобіля 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.

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 із сертифікації має бути акредитований відповідно до стандарту ISO/IEC 17065. Крім того, він має право бути призначеним своїм НОСК видавати сертифікати на рівні гарантій „високий” CSA.

Випробувальна лабораторія (ВЛ), включаючи її персонал, що проводить оцінки для органу з сертифікації, будь то внутрішня лабораторія випробувань органу з оцінки відповідності або зовнішня лабораторія випробувань у випадку, коли випробування виконує субпідрядник, повинна бути технічно компетентною для відповідних завдання.

Для рівня гарантій „суттєвий” ця технічна компетентність повинна оцінюватися шляхом акредитації випробувальної лабораторії відповідно до ISO/IEC 17025.

НОСК може надати за підтримки органу з акредитації (НААУ) вказівки щодо гармонізованого тлумачення ISO/IEC 17025 для Схеми з урахуванням відповідних стандартів, таких як 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.

Крім того, Схема передбачає наступні конкретні вимоги, до яких підлягають органи з оцінки відповідності, щоб гарантувати їх технічну компетентність для оцінки вимог щодо кібербезпеки:

• конкретні вимоги стосуються технічної компетенції, пов'язаної з конкретною випробувальною діяльністю, і застосовуються лише щодо сертифікатів, виданих на рівні гарантій «високий»;

• вимоги застосовуються як до внутрішніх випробувальних лабораторій органів з оцінки відповідності, так і до зовнішніх у випадках, коли випробування виконує субпідрядник.

Ці ВЛ та відповідний персонал повинні відповідати наступним вимогам:

(a) мати необхідні знання та досвід у виконанні конкретних тестових дій для визначення стійкості продукту до конкретних атак;

(b) Для технічних областей мати необхідний досвід та досвід у виконанні специфічних випробувальних заходів, необхідних для методичного визначення стійкості виробу до атак, що здійснюються в робочому середовищі виробу, припускаючи відповідний потенціал атаки як „помірний”, так і „високий”, як описано в CC (AVA_VAN.4 - Методичний аналіз вразливості, AVA_VAN.5 - Розширений методичний аналіз вразливості).

Однак може знадобитися взаємозатверджене тлумачення стандартів акредитації для діяльності лабораторій сертифікації та випробувань і їх слід визначити як керівництво схемою (за підтримки НААУ чи Європейської кооперації з акредитації). НОСК може керувати цією діяльністю, використовуючи досвід різних членів SOG-IS MRA, які розробляли такі інтерпретації зі своїм Національним органом з акредитації (NAB), та використовуючи такі потенційно відповідні стандарти:

• ISO/IEC 19896, Вимоги до компетенції для тестувальників та оцінювачів інформаційної безпеки, особливо:

Частина 1: Вступ, поняття та загальні вимоги

Частина 3: Вимоги до знань, навичок та ефективності для оцінювачів СС

- 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;

4.4 Висновки до розділу 4

У цьому розділі наведено огляд основних вимог до роботи органів кібербезпеки Європейського Союзу та описано сертифікацію кібербезпеки та вимоги до підключених транспортних засобів відповідно до регламенту ЄС 2019/881 і документу WP.29 ЄЕК ООН. Було зроблено висновок, що сертифікація кібербезпеки підключених автомобілв необхідна для транскордонного визнання результатів сертифікації в рамках відповідних схем сертифікації та розробок схем.

Система сертифікації кібербезпеки України для підключених транспортних засобів може бути побудована на основі механізмів національної системи технічного регулювання згідно з Міжнародною угодою Національної організації України з акредитації органів з оцінки.

ВИСНОВКИ

Система сертифікації встановлюється процедурами, правилами та управлінням сертифікації кібербезпеки, а схема сертифікації складається з набору правил і процедур для управління подібними або тісно пов’язаними системами оцінки відповідності.

Сьогодні перед Україною стоїть важливе та актуальне завдання: розробка схем і систем сертифікації кібербезпеки підключених транспортних засобів на основі існуючої в країні системи технічного регулювання, а також досягнень у сфері оцінки відповідності та сертифікації. Вимоги законодавства України з кібербезпеки ставить завдання застосування міжнародних та європейських принципів оцінки відповідності кібербезпеки.

Сертифікація кібербезпеки підключених транспортних засобів в Україні відсутня і потребує створення національної системи сертифікації кібербезпеки підключених транспортних засобів на основі міжнародних стандартів, кращих практик та глобальної системи технічного регулювання.

Для створення національної системи кібербезпеки підключених транспортних засобів на основі стандартів та систем, які застосовуються для сертифікації продукції у системі ILAC/IAF розроблена Ієрархічна модель оціночних стандартів для схеми сертифікації кібербезпеки в автомобільній галузі.

Для створення національної системи кібербезпеки на основі Угод про визнання, які існують у системі ILAC/IAF/EA розроблена Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки підключених транспортних засобів. Досліджено стан та міжнародний статус Національного органу України з акредитації ООВ щодо транскордонного визнання сертифікації інформаційної та кібербезпеки підключених транспортних засобів.

На основі ієрархічної моделі оціночних стандартів, ієрархічної моделі Угод про взаємне визнання та аналізу міжнародного статусу Національного

органу України з акредитації запропонована версія схеми сертифікації кібербезпеки в автомобільній галузі, яка встановлює процедуру створення систем сертифікації кібербезпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про технічні регламенти та оцінку відповідності Закон України від 15.01.2015 № 124-VIII // Відомості Верховної Ради України. – 2015. – № 14.
2. Про основні засади забезпечення кібербезпеки України Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45.
3. Про технічні регламенти та оцінку відповідності Закон України від 15.01.2015 № 124-VIII // Відомості Верховної Ради України. – 2015. – № 14.
4. Про акредитацію органів з оцінки відповідності Закон України від 17.05.2001 № 2407-III // Відомості Верховної Ради України. – 2001. – № 32
5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : Указ Президента України від 15.03.2016 № 96/2016. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016
6. Conformity assessment - Vocabulary and general principles : ISO/IEC 17000:2020. – [Чинний від 2020-01-06]. – International Organization for Standardization/International Electrotechnical Commission, 2020. – 30 P.
7. International Accreditation Forum [Електронний ресурс]. – Режим доступу: https://www.iaf.nu/.
8. International Laboratory Accreditation Cooperation [Електронний ресурс]. – Режим доступу: https://ilac.org/.
9. Сучасне та майбутнє безпеки транспортних засобів завдяки сертифікації CSMS (ISO/SAE 21434). [Електронний ресурс] https://www.igloo.co.kr/security-information/csmsiso-sae-21434

10. [Електронний ресурс] https://www.tuvsud.com/ko-kr/resource-centre/stories/cyber-security-threats-of-connected-vehicles
11. [Електронний ресурс] https://learn.ztu.edu.ua/pluginfile.php/78550/mod_folder/content
12. [Електронний ресурс] https://uk.wikipedia.org/wiki
13. [Електронний ресурс] https://habr.com/ru/post/373457/
14. [Електронний ресурс] https://securelist.ru/a-study-of-car-sharing-apps/90804/
15. ISO 26262-10 Second edition 2018-12 Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262
16. [Електронний ресурс] https://www.iso.org/ru/standard/70918.html
17. E/ECE/TRANS/505/Rev.3/Add.151 (unece.org)
18. Регламент Європейського Парламенту і Ради (ЄС) № 526/2013 від 21 травня 2013 року про Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) та про скасування Регламенту (ЄС) № 460/2004 (OB L 165, 18.06.2013, с. 41).
19. "Interinstitutional agreements"[Електронне джерело] – Режим доступу до ресурсу:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC%3A2018%3A012%3ATOC
20. Про основні засади забезпечення кібербезпеки України Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45.
21. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації Розпорядження Кабінету Міністрів України; від 17.01.2018 № 67-р. – Режим доступу : https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi
22. https://argus-sec.com/unece-wp29-approved/

23. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) – [Чинний від 2019-04-17]. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2019/881/oj.
24. Conformity assessment - Vocabulary and general principles : ISO/IEC 17000:2020. – [Чинний від 2020-01-06]. – International Organization for Standardization/International Electrotechnical Commission, 2020. – 30 P.
25. Про технічні регламенти та оцінку відповідності Закон України від 15.01.2015 № 124-VIII // Відомості Верховної Ради України. – 2015. – № 14.
26. Про акредитацію органів з оцінки відповідності Закон України від 17.05.2001 № 2407-III // Відомості Верховної Ради України. – 2001. – № 32.
27. International Accreditation Forum [Електронний ресурс]. – Режим доступу: https://www.iaf.nu/.
28. International Laboratory Accreditation Cooperation [Електронний ресурс]. – Режим доступу: https://ilac.org/.
29. European co-operation for Accreditation [Електронний ресурс]. – Режим доступу: https://european-accreditation.org/
30. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : Указ Президента України від 15.03.2016 № 96/2016. – Режим доступу : https://zakon.rada.gov.ua/laws/show/96/2016
31. Economic and Social Council Report. On the sectoral initiative on cyber security. – United Nations: Geneva, 20–22 November 2019. – Режим доступу:https://unece.org/DAM/trade/wp6/documents/2019/ECE_CTCS_WP.6_2019_9E.pdf

32. Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes : ISO/IEC 17067:2013. – [Чинний від 2013-08-07]. – International Organization for Standardization/International Electrotechnical Commission, 2013. – 13 P.
33. Цвілій О.О. «Система сертифікації кібербезпеки інформаційних та комунікаційних технологій» – Режим доступу до ресурсу: https://ojs.onat.edu.ua/index.php/sbornik_onat/article/view/1224
34. France.The European cooperation for Accreditation. EA-1/06 A-AB: 2017 EA Multilateral Agreement. Criteria for signing. Paris, 2017.
35. https://mtu.gov.ua/content/zasidannya-komisii-mininfrastrukturi-z-pitan-zabezpechennya-vikonannya-zhenevskoi-ugodi-1958-roku.html
36. https://www.iso.org/ru/home/standards/popular-standards/isoiec-17025--testing-and-calibr.html
37. https://www.igloo.co.kr/security-information/csmsiso-sae-21434%EC%9D%B8%EC%A6%9D%EC%9C%BC%EB%A1%9C-%EC%82%B4%ED%8E%B4%EB%B3%B4%EB%8A%94-%EC%B0%A8%EB%9F%89-%EB%B3%B4%EC%95%88%EC%9D%98-%ED%98%84%EC%9E%AC%EC%99%80-%EB%AF%B8%EB%9E%98/
38. https://m.kmib.co.kr/view.asp?arcid=0924236895
39. https://habr.com/ru/company/bright-box/blog/336078/
40. https://visuresolutions.com/uk/%D0%B1%D0%BB%D0%BE%D0%B3/%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%BE%D0%B1%D1%96%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9/ISO-21434/
41. https://www.dqsglobal.com/uk-ua/blog/avtomobil%27na-kiberbezpeka-novi-obov%E2%80%99yazkovi-pravila#automotive-cyber-security-neue-verbindliche-vorschriften-chapter10
42. https://ela.kpi.ua/bitstream/123456789/51207/1/Pikhota_magistr.pdf