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

Інститут телекомунікаційних систем

Кафедра інформаційно-комунікаційних технологій та систем

«На правах рукопису»
УДК 004.056

«До захисту допущено»

В.О. завідувача кафедри

_____Аліна МОШІНСЬКА

«___»_____2022 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Розроблення рекомендацій щодо державного регулювання питань кібербезпеки підключеного автомобіля»

Виконала:
студентка ІІ курсу, групи ТС-11мп
Синявіна Євгенія Павлівна _____

Керівник:
професор кафедри ІКТС д.т.н, проф.
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

ВО завідувача кафедри

_____ Аліна МОШИНСЬКА

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Синявіній Євгенії Павлівній

1. Тема дисертації: «Розроблення рекомендацій щодо державного регулювання питань кібербезпеки підключеного автомобіля», науковий керівник дисертації Горицький Віктор Михайлович д.т.н., професор, затверджені наказом по університету від «____» «____» 202_ р. № _____

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження – державне регулювання питань кібербезпеки підключеного автомобіля

4. Предмет дослідження – кібербезпека підключеного автомобіля

5. Перелік завдань, які потрібно розробити

- Визначити актуальність розроблення рекомендацій щодо державного регулювання питань кібербезпеки підключеного автомобіля.
- Проаналізувати нормативно-правовий аспект технічного регулювання

- Проаналізувати технологічні особливості стандартів кібербезпеки, що мають знизити ризик загроз для кібербезпеки підключеного автомобіля
- Проаналізувати моделі існуючих стандартів кібербезпеки для підключених транспортних засобів та обґрунтувати вибір стандартів
- Надати рекомендації щодо державного регулювання питань кібербезпеки підключеного автомобіля

6. Орієнтовний перелік ілюстративного матеріалу

Слайд №1 «Тема, мета, об’єкт та предмет дослідження магістерської роботи»

Слайд №2 «Завдання, що вирішуються у дослідженні»

Слайд №3 «Особливості нормативно-правових аспектів технічного регулювання»

Слайд №4 «Порівняння існуючих стандартів кібербезпеки з встановленими вимогами та знаходження недосконалості їх імплементацій»

Слайд №5 «Пропозиції щодо покращення стандартів та усунення даних невідповідностей»

Слайд №6 «Результати вибору оптимального методу впровадження вибраної реалізації»

Слайд №7 «Висновки по виконаній роботі»

7. Дата видачі завдання ____.10.2021 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Обґрунтування актуальності розроблення рекомендацій державного регулювання щодо кібербезпеки підключеного автомобіля	01.11.2021 - 15.01.2022	
2	Аналіз технологічних особливостей стандартів кібербезпеки підключених автомобілів	15.01.2022 - 15.02.2022	
3	Аналіз моделей існуючих стандартів кібербезпеки підключених автомобілів	15.02.2022 - 15.04.2022	
4	Аналіз вимог до державних органів з акредитації	15.04.2022 - 15.06.2022	
5	Розробка рекомендацій державного регулювання	15.06.2022 - 15.09.2022	
6	Оформлення результатів.	До 06.12.2022	

Студентка _____ Євгенія СИНЯВІНА
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Віктор ГОРИЦЬКИЙ
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Темою магістерської дисертації є розроблення рекомендацій щодо державного регулювання питань кібербезпеки підключеного автомобіля

Робота містить 85 сторінки, зокрема 12 ілюстрацій, 1 таблицю та 41 джерело інформації

Метою роботи є розгляд існуючих міжнародних регламентів щодо регулювання питань кібербезпеки підключених автомобілів, та розробка рекомендацій щодо державного регулювання їх в Україні.

Актуальність даної роботи полягає в тому, що поточні тенденції вказують на поступове збільшення використання саме підключених автомобілів, що в свою чергу збільшує кількість ймовірних ризиків саме в питанні кібербезпеки цих автомобілів.

Об’єктом дослідження є державне регулювання кібербезпеки підключених автомобілів. Кібербезпека для підключених автомобілів є предметом дослідження

В даній роботі вивчаються особливості державного регулювання кібербезпеки підключеного автомобіля, розглядаються існуючі міжнародні органи, що регулюють питання кібербезпеки транспортних засобів, досліджуються вимоги щодо створення подібних органів державного регулювання, а також досліджується питання визнання даного органу поза межами України.

В роботі проводиться дослідження та розробляються рекомендації щодо державного регулювання питань кібербезпеки підключеного автомобіля

Ключові слова: стандарти ISO/SAE 21434, ISO 26262 кібербезпека, підключені автомобілі, оцінка відповідності, технічне регулювання.

ABSTRACT

The topic of the master's thesis is the development of recommendations for state regulation of cyber security issues of the connected car

The work contains 85 pages, including 12 illustrations, 1 table and 41 sources of information

The purpose of the work is to review the existing international regulations regarding the regulation of cyber security issues of connected cars, and to develop recommendations for their state regulation in Ukraine.

The relevance of this work lies in the fact that current trends indicate a gradual increase in the use of connected cars, which in turn increases the number of potential risks in the issue of cyber security of these cars.

The object of the study is the state regulation of cyber security of connected cars. Cyber security for connected cars is a subject of research

This paper studies the peculiarities of the state regulation of the cyber security of the connected car, examines the existing international bodies that regulate the issue of cyber security of vehicles, examines the requirements for the creation of similar state regulatory bodies, and also examines the issue of recognition of this body outside Ukraine.

The work conducts research and develops recommendations for state regulation of cyber security issues of the connected car

Keywords: standards ISO/SAE 21434, ISO 26262 cyber security, connected cars, conformity assessment, technical regulation

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	(Internet of Things) - Інтернет речей
GPS	(Global Positioning System) - глобальна система позиціонування;
ПЗ	програмне забезпечення;
LPWAN	(Low-power Wide-area Network) - енергоефективна мережа далекого радіусу дії;
Li-Fi	Li-Fi (Light Fidelity) - Плазмовий інтернет;
IM	(Instant messaging) - миттєві повідомлення;
WSNS	(Wireless Sensor Networks) - бездротові сенсорні мережі;
VSNS	(Virtual Sensor Networks) - віртуальні сенсорні мережі;
VANETS	(Vehicle Ad hoc NETworks) - мережі зв'язку транспортних засобів;
DoS	(Denial of Service) - відмова в обслуговуванні;
SLA	(Service-level agreement) - угода між постачальником послуг і користувачем про рівень послуг
QOS	(Quality of Service) - якість обслуговування
Pow	(Proof-of-work) - докази роботи
FN	(Fog node) - туманний вузол
P2P	(peer-to-peer) - вузол до вузла
AI	(Artificial intelligence) - штучний інтелект;

ВСТУП

Автомобільна промисловість стикається з радикальною зміною парадигми: із швидкими темпами цифровізації все більше і більше електронних систем керування, інтелектуальних компонентів, вбудованих систем та інтерфейсів API знаходять свій шлях у транспортні засоби, що робить їх потужнішими, безпечнішими та розумнішими, ніж будь-коли раніше. Автомобільна кібербезпека - це виклик сучасності для виробників автомобілів. Кожен додатковий комунікаційний інтерфейс і компонент є потенційною точкою атаки для кіберзлочинців. Потенціал шкоди від маніпуляцій швидко зростає, наприклад, стосовно автономно керованих транспортних засобів або електронно керованих функцій водіння та гальмування. З цієї причини Організація Об’єднаних Націй зараз визначає базові рамки для автомобільної кібербезпеки за допомогою двох нових правил. Це кібербезпека UNECE Cyber Security (UN R 155), яка безпосередньо посилається на новий стандарт ISO/SAE 21434, та оновлення програмного забезпечення UNECE Software Updating (UN R 156). Разом з тим, говорити про наявність дієвої системи сертифікації кібербезпеки в Україні не приходиться.

Про це відверто зазначено у Рішенні Комітету Верховної Ради України з питань цифрової трансформації, який розглянув на своєму засіданні 19 лютого 2020 року (протокол № 13) питання про практику застосування Закону України «Про основні засади забезпечення кібербезпеки України» та відповідності закону прийнятих Кабінетом Міністрів України та відомствами підзаконних нормативно-правових актів, своєчасності прийняття таких нормативно-правових актів, де констатовано, що:

- «Визнати невиконаними в повній мірі (протягом 2017, 2018, 2019 років) Кабінетом Міністрів України, державними органами, службами та відомствами завдання, встановлені пунктом 3 Прикінцевих та перехідних положень Закону

України від 5 жовтня 2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» щодо забезпечення у тримісячний строк з дня набрання чинності цим Законом, прийняття нормативно-правових актів, необхідних для реалізації цього Закону; приведення своїх нормативно-правових актів у відповідність із цим Законом; забезпечення перегляду і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону;

- Комітету Верховної Ради України з питань цифрової трансформації ініціювати створення Тимчасової слідчої комісії з розслідування зазначеного питання».

Серед інших причин такого топтання на місті в стратегічно важливому для України питанні слід визначити і складність та відсутність визначеної в Державі системи сертифікації кібербезпеки підключених автомобілів, що є на сьогодні невирішеною проблемою На даний момент в Україні не існує законодавчих регламентів, що могли б забезпечити подібне регулювання, саме тому було обрано таку тематику.

1 НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ТЕХНІЧНОГО РЕГУЛЮВАННЯ

1.1 Закон України про кібербезпеку

В сучасному світі концепція підключених автомобілів стає все більш поширеною, а отже і з’являється більше ризиків та загроз щодо їх використання.

Саме тому, є необхідність для створення органу, що здійснюватимете діяльність з оцінки відповідності, включаючи випробування, сертифікацію та інспектування кібербезпеки підключеного автомобіля. А для цього в першу чергу необхідно ознайомитись з нормативно-правовими аспекти регулювання кібербезпеки, а також технічним регламентом та оцінкою відповідності.

Згідно Закону України про кібербезпеку, кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Методи й захисні практики комп’ютерної безпеки застосовуються в різних галузях – від бізнес-сфери до мобільних технологій, серед яких можна виокремити кібербезпеку автомобілів і транспортної інфраструктури. У кінці серпня 2021 р. [2] був надрукований міжнародний стандарт інженерії комп’ютерної безпеки дорожніх транспортних засобів ISO/SAE 21434:2021, що призначені допомогти виробникам завжди бути на крок попереду [3]. Мірою того як автомобілі все частіші починають підключатися до глобальної мережі, зростає ризик порушення кібербезпеки. Так, дослідження, проведені в Англії організацією Zenzic, показали, що з 2016 р. кількість зламів програмного забезпечення в автомобільній галузі в річному обчисленні зросло на 94 %, майже удвічі [4]. Незважаючи на те, що галузь, яка займається боротьбою з хакерами, розвивається, ведеться постійна боротьба за те, щоб не відстати від усе більш досконалих технологій. Кібербезпека транспорту

– це безпека особистих даних, якими користувач ділиться з транспортним засобом або агрегатором транспортних даних. Нині «розумні» системи поширені всюди: вони контролюють траси й залізниці за допомогою платформ для моніторингу, як навігатори відслідковують затори та запобігають їм, відповідають за безпеку пасажирів та водія в середині автомобілів [5]. Усі ці системи використовують контролери та датчики, які дозволяють тримати зв’язок із зовнішніми джерелами даних. На практиці виявляється, що чим більше в транспортного засобу є зв’язок із зовнішнім світом, тим уразливіший він стає зовні для кібератак і тим більше йому потрібна особлива система захисту.

Початком цифровізації автомобілів можна вважати електронне запалювання, анти блокувальну систему гальмування або електронну систему керування двигуном, які запропонували Pontiac, Chrysler та GM ще 1963, 1971, 1979 рр. [6]. У подальшому компоненти автомобілів ставали все більш електронними й, нарешті, цифровими (тут складно провести чітку межу), але справжнім початком цифрової революції в автомобільних технологіях можна вважати лютий 1986 р., коли на конгресі автомобільних інженерів (SAE) компанія Robert Bosch GmbH представила світу цифровий мережний протокол комунікації електронних компонент автомобіля (CAN – controller area network). Що цікаво, фахівці цієї теми й авторитетні інтернет джерела засвідчують: цей мережний протокол і сьогодні є найбільш поширеним та присутній практично в кожному серійному автомобілі. Крім різновидів CAN-шин (lowspeed, high-speed CAN, FD-CAN) сьогодні ще використовуються FlexRay (трансмісія), LIN (низько швидкісна шина), оптична MOST (мультимедіа) і, нарешті, бортовий Ethernet (на сьогодні 100 Мбіт/с, у наступних генераціях до 1 Гбіт/с). На сьогодні, з розвитком різних комутаційних протоколів, під час проєктування сучасних автомобілів використовуються так звані технології Drive by Wire (без механічних приводів), що містять електронну педаль газу, гальмову педаль (Toyota, Ford та GM застосовують її з 1998 р. у своїх гібридах і електроавтомобілях), електронні

системи паркування (parking sensors parktronics), електронний перемикач передач, електронне рульове управління (першими були Infinity з моделлю Q50 2014 р.). 2000 р. Honda встановлює на серійну S2000 систему EPS (Electric Power Steering), що за визначених умов може керувати кермом замість людини. Починаючи з 2001 р., коробка передач спілкується з людиною тільки по проводах (раніше цю функцію виконував тросик). Тоді ж масово почали застосовувати електронні кнопки запуску, що дозволяли керувати двигуном усупереч бажанню водія. З 2010 р. поширюється попит на повністю графічні приладні панелі, які можуть виводити будь що. Електроніка кузова (двері, замки, вікна тощо) з 2015 р. практично в усіх виробників зав'язана на спеціальний комп'ютер і має свою автономію прийняття рішень. Кількість підключених автомобілів (connected car, з'єднаних із «хмарою» автовиробника) постійно зростає та стрімко наближається до 100 %. Необхідно зазначити, що в деяких країнах існують обмеження на такі автомобілі, але вони мають застарілий законодавчий характер і з часом будуть обов'язково переглянуті. Перший у сучасному сенсі підключений автомобіль з'явився 1996 р. і був результатом співробітництва GM та Motorola Automotive, що привело до появи телематичної (сфери інформатики, що охоплює напрям комунікацій) системи OnStar – системи, що спроможна була самостійно з'єднуватись з оператором служби порятунку у випадку аварії. Віддалена діагностика автомобіля була представлена 2001 р., а 2003 р. підключений автомобіль навчили відправляти виробнику звіти про стан бортових систем. Телематичні блоки data-only були запропоновані індустрією 2007 р. Улітку 2014 р. кампанія Audi першою запропонувала опцію встановлення хотспотів (точок доступу) 4G-LTE-Wi-Fi на свої авто. 2015 р. в GM серійно впроваджували хотспоти до всіх своїх машин і отримали понад мільярд телематичних звітів від клієнтів. Нині автовиробники не тільки збирають телеметрію, але починають її монетизацію: провідну роль тут відіграє BMW із конвергенцією смартфонів та автомобілів [7].

1.2 Закон України про технічні регламенти та оцінку відповідності

Згідно до Закону України про технічні регламенти та оцінку відповідності, 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;

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;

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

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

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

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

Технічними регламентами та процедурами оцінки відповідності, застосування яких передбачене технічними регламентами, можуть бути встановлені особливості регулювання відносин, на які поширюється дія цього Закону.

Рисунок 1.1 – Структура технічного регулювання

Технічне регулювання є правовою основою регулювання відносин, що виникають при формуванні обов'язкових та добровільних вимог до продукції, процесів її проектування (включаючи вишукування), виробництва, будівництва, монтажу, налагодження, експлуатації, зберігання, перевезення, реалізації та утилізації, виконання робіт або надання послуг, а також при проведенні оцінки відповідності об'єктів регулювання встановленим вимогам. Цілі, засоби і методи їх досягнення, завдання, які вирішуються в рамках технічного регулювання відносин між сферами виробництва і споживання, представлені на рисунку 1.2.

Рисунок 1.2 – Цілі, засоби, методи і завдання технічного регулювання

Технічне регулювання має забезпечити основу для вирішення двох комплексів завдань. По-перше, їх реалізація повинна забезпечувати регулювання внутрішнього ринку, по-друге, вони повинні бути спрямовані на створення сприятливих умов для розвитку зовнішньої торгівлі.

Перше завдання викликана необхідністю виробити механізм формування вимог до продукції і до оцінки її відповідності в процесі створення і руху товару, який відповідав би вимогам реформування нашої економічної системи, надання їй соціальної орієнтації, підвищення конкурентоспроможності продукції та економіки в цілому. Держава при цьому встановлює якість вимоги безпеки на базі оцінки ризику застосування продукції з урахуванням реальних соціально-економічних можливостей. Споживчі властивості формуються ринком. Завдання ж держави в цій галузі полягає в тому, щоб створити рівні і сприятливі умови для всіх учасників ринку і засобами технічного регулювання, та іншими заходами – такими, наприклад, як усунення монополізму, створення саморегулюючих організацій та ін.

Друге завдання викликана проблемами глобалізації. Питання тут полягає в тому, що необхідно створити такий механізм технічного регулювання, який, з

одного боку, дозволяв би вести економічно вигідну для держави політику у зовнішній торгівлі, а з іншого - був би гармонізований з правилами, встановленими міжнародним співтовариством.

У відповідності з цими двома завданнями можна умовно сформулювати дві групи принципів.

Перша група – це основні принципи технічного регулювання для внутрішнього ринку. Вони передбачають наступне:

- Відповідність системи технічного регулювання рівню розвитку національної економіки, матеріально-технічної бази і науково-технічного розвитку. Встановлювані в технічних регламентах вимоги повинні бути мінімально необхідними для досягнення цілей регулювання;
- Застосування єдиних правил встановлення вимог до продукції і процесам її проектування (включаючи вишукування), виробництва, будівництва, монтажу, налагодження, експлуатації, зберігання, перевезення, реалізації та утилізації, а також до виконання робіт або надання послуг;
- Єдність і обов'язковість для виконання на всій території Росії вимог технічних регламентів;
- Доказовою базою виконання вимог технічних регламентів можуть бути національні стандарти;
- - Формування механізму технічного регулювання на основі оцінки ризику застосування продукції;
- Незалежність органів з акредитації та органів з сертифікації від виробників, продавців, виконавців і споживачів;
- Наявність єдиної системи і правил акредитації, неприпустимість суміщення діяльності з акредитації та сертифікації та обмеження конкуренції при виконанні цих робіт;
- Неприпустимість суміщення повноважень органу державного контролю (нагляду) та органу з сертифікації;

- Встановлення в технічних регламентах експлуатаційних, а не конструкційних характеристик.

Суть другої групи принципів зводиться до того, щоб надані до виробників і продавцям різних країн обов'язкові вимоги до продукції і процесам її проектування, виробництва, будівництва і т.д. не переростає в торгові бар'єри. Країни повинні прагнути створювати такі механізми, які дозволили б уникнути перешкоди у торгівлі при введенні в дію технічних регламентів, стандартів і процедур оцінки відповідності. Міжнародна практика в цій області базується на таких основних положеннях.

Усунення надлишкових бар'єрів у торгівлі. Технічні бар'єри є результатом прийняття країнами технічних регламентів, стандартів і процедур оцінки відповідності. При цьому через відмінності в соціально-економічному розвитку, кліматі, національних традиціях, смаках різних країн ці регламенти, стандарти і процедури можуть відрізнятися один від одного. Держави мають можливість брати до уваги ці фактори в законодавстві на тому рівні, який вважають за необхідне. Разом з тим необхідно прагнути розробляти гнучкі технічні регламенти, які в мінімальному ступені були б обмежувальними для торгівлі. Тому технічні регламенти повинні встановлювати експлуатаційні, а не конструкційні вимоги.

Якщо обставин, які змусили прийняти підвищені вимоги, більше не існує або цілі регулювання можуть бути досягнуті іншими, менш обмежувальними заходами, такі заходи повинні бути застосовані. Подібні дії необхідно зробити і у випадку, якщо прийняті умови регулювання не відповідають ризику недосягнення цілей.

Зобов'язання щодо усунення технічних бар'єрів у торгівлі відносяться також до процедур оцінки відповідності та стандартам.

Недискримінаційній основі**.** Цей принцип встановлює, що вимоги технічних регламентів для допуску в країну імпортованої продукції повинні встановлювати

не менш сприятливий режим, ніж для допуску власної продукції на свій ринок. Такий же режим поширюється і на процедури оцінки відповідності. Це, зокрема, означає, що умови сертифікації для імпортованої продукції повинні застосовуватися на недискримінаційній основі, у тому числі за строками її проведення та вартості.

Гармонізація припускає використання міжнародних стандартів у якості основи для національних технічних регламентів в тому випадку, якщо вони забезпечують досягнення цілей технічного регулювання. Міжнародні стандарти повинні застосовуватися також в якості основи для процедур оцінки відповідності, якщо вони не суперечать цілям регулювання.

Еквівалентність**.** Розробка міжнародних стандартів може виявитися тривалою через необхідність досягнення консенсусу по технічно складних питань. Тому поряд з принципом гармонізації пропонується принцип еквівалентності, зміст якого зводиться до того, що країни повинні позитивно сприймати технічні регламенти інших країн як еквівалентні їх власним за умови досягнення тих же цілей технічного регулювання. Характер конструктивних рішень при цьому не повинен мати значення.

Взаємне визнання результатів оцінки відповідності. Країнам пропонується вести на постійній основі переговори про взаємне визнання результатів оцінки відповідності та досягати при цьому позитивних результатів. Дана необхідність викликана тим, що процедури оцінки відповідності можуть створювати технічні бар'єри в торгівлі, якщо продукція, що поставляється в інші країни, повинна бути вдруге піддана оцінки відповідності внаслідок відмінностей у вимогах як до самої продукції, так і до процедур оцінки. Такий підхід може бути обумовлений чисто технічними причинами, але часто в його основі лежить зацікавленість бізнесу або чиновників.

Єдиних моделей взаємного визнання не існує, але є типові підходи й елементи, які можуть розглядатися на переговорах. Насамперед - визнання

сертифікатів і знаків відповідності, виданих акредитованими органами за кордоном, як еквівалентних. Крім того, це перелік продукції, що підпадає під угоду про взаємне визнання, і способи її ідентифікації. У перелік можуть бути включені критерії визнання компетентності органів з сертифікації та випробувальних лабораторій в кожній країні і їх опублікований список. І нарешті, угоди про взаємне визнання можуть передбачати вирішення протиріч на основі обміну інформацією та спільного моніторингу.

Фундаментом створення та функціонування єдиного світового ринку є вільне переміщення товарів. Наявність в міжнародній торгівлі технічних бар'єрів створює перешкоди як для виходу української продукції на європейські та міжнародні ринки, так і для доступу вітчизняних споживачів до якісних закордонних продуктів. Механізми ліквідації технічних бар'єрів в торгівлі базуються на взаємному визнанні результатів оцінки відповідності, що може бути забезпечено тільки в результаті технічної гармонізації.

Така гармонізація досягається наявністю в країні сучасної системи технічного регулювання, яка б відповідала загальновизнаним міжнародним нормам та правилам, насамперед, Світової організації торгівлі та міжнародних організацій з стандартизації – ISO, IEC, ITU. Основними складовими системи технічного регулювання є стандартизація; оцінка відповідності (сертифікація товарів, робіт, послуг), метрологія , акредитація органів з оцінки відповідності та випробувальних і калібрувальних лабораторій.

Встановлюючи правила та порядок застосування елементів регулювання у їхньому взаємозв'язку, законодавець формує відповідну модель технічного регулювання.

В Євросоюзі створена система технічного регулювання, яка на сьогодні у світі розглядається, як найбільш ефективна модель для міжнародного співробітництва, оскільки визначально створювалась для формування єдиного

економічного простору. Цей факт відмічено у звіті Європейської економічної комісії ООН за 2003 р.

Ефективність європейського підходу у сфері технічного регулювання підтверджується наявністю угод про взаємне визнання результатів оцінки відповідності з такими країнами, як Японія, США, Канада, Австралія, Нова Зеландія, Швейцарія, Ізраїль. В країнах ЄС вільне переміщення товарів базується на основі «Нового підходу» до технічної гармонізації і стандартизації (прийнятий Радою Європи 7 травня 1985 р.) та «Глобального підходу» у сфері оцінювання відповідності (прийнятий Радою Європи 21 грудня 1989 р.). Такі підходи реалізуються через відповідні інструменти - директиви ЄС, які також затверджуються Радою Європи.

Основні принципи «Нового підходу» зводяться до наступного:

- в директивах на продукцію задають обов'язкові для виконання загальні (суттєві) вимоги безпеки;

- задачі встановлення конкретних характеристик покладається на європейські стандарти, які є добровільними для застосування;

- продукція, яка виготовлена згідно з вимогами гармонізованих з директивою ЄС європейських стандартів розглядається як відповідна суттєвим вимогам директиви (принцип презумпції відповідності);

- продукція може бути розміщена на ринку ЄС тільки після процедури оцінки відповідності;

- нагляд за ринком забезпечують державні органи.

«Глобальний підхід» передбачає застосування модулів для різних стадій процедур оцінювання відповідності, встановлення єдиних критеріїв їх використання та призначення спеціальних органів, що виконують ці процедури. Модульний підхід дозволяє формувати безліч сполучень модулів і, таким чином, збільшити кількість схем підтвердження відповідності, з яких можливо вибрати схему, адекватну рівню можливого ризику заподіяння шкоди конкретною

продукцією. Що стосується малого бізнесу, то в ЄС в цей час розробляються методичні документи з відбору та впровадження модулів оцінки відповідності продукції дрібносерійного та несерійного виробництва з урахуванням специфіки підприємств малого та середнього бізнесу.

За суттю, перераховані основні принципи і визначають модель технічного регулювання в країнах ЄС. Виключно важливо, що ці принципи представляють собою цілісну систему. Іншими словами, виключення із цього набору хоч одного принципу порушує системність підходу. В цілому, застосування такої моделі технічного регулювання створює сприятливі умови для вільного обігу безпечних товарів та суттєво обмежує адміністративне втручання в розміщення виробів на ринку та господарську діяльність виробників.[40]

1.3 Технічне регулювання як основа державного регулювання

Зі вступом у 2008 р. до Світової організації торгівлі (СОТ), Україна прийняла правила гри, які діють на світовому ринку і, з метою подолання технічних бар'єрів в торгівлі з країнами-членами СОТ, взяла на себе зобов'язання до 2012 р. реформувати національну систему технічного регулювання. Відомо, що Україна приводить національну систему технічного регулювання до визнаної у світі, європейської моделі, тобто до норм та правил, які прийняті в країнах – членах ЄС.

З прийняттям Верховною Радою законів «Про стандартизацію», «Про підтвердження відповідності», «Про метрологію та метрологічну діяльність», «Про акредитацію органів з оцінки відповідності», «Про стандарти, технічні регламенти та процедури оцінки відповідності», національна система технічного регулювання почала адаптуватися до міжнародних, в першу чергу, європейських вимог. Основну увагу сконцентровано на впровадженні європейських директив «Нового підходу», гармонізації національних стандартів з міжнародними та

європейськими. Установлено, що європейські директиви впроваджуються в Україні в якості технічних регламентів.

Технічний регламент, як нормативно-правовий акт, прийнятий органом державної влади, встановлює обов'язкові вимоги щодо усунення загрози для національної безпеки; захисту життя, здоров'я та майна людини; захисту тварин, рослин та довкілля та ін. Під кожний затверджений регламент слід оприлюднювати перелік національних стандартів, що забезпечують відповідність до вимог регламентів.

Принципи «Глобального підходу» запроваджені в Україні «Технічним регламентом модулів оцінки відповідності та вимог щодо маркування національним знаком відповідності, які застосовуються в технічних регламентах» та застосовані в усіх інших технічних регламентах. На даний час в Україні протягом 2003-2010 рр. прийнято 30 технічних регламентів, які розмішені на сайті gssu.gov.ua у розділі «Регуляторні акти та технічні регламенти».

Відповідно до Угоди про партнерство і співробітництво між Україною та ЄС, в лютому 2008 р. було розпочато переговорний процес щодо Угоди про асоціацію між Україною та ЄС, інтегральною складовою якої є положення Угоди про зону вільної торгівлі (ЗВТ). Виходячи з європейської практики укладання подібних угод, невід'ємним додатком до положень Угоди про ЗВТ має бути Протокол щодо оцінки відповідності та прийнятністі промислової продукції АСАА (угода про взаємне визнання Україною та ЄС сертифікатів відповідності на промислову продукцію).

Такі угоди укладались ЄС з країнами, які були кандидатами на членство в ЄС, та країнами Середземномор'я, і дали змогу продукції, що охоплювалась цими угодами, вільно просуватись на внутрішньому ринку ЄС без додаткових процедур оцінки відповідності.

У рамках плану дій АСАА було визначено і погоджено з європейською стороною чотири пріоритетні сектори української промисловості (низьковольтне

обладнання, машини і механізми, прості посудини високого тиску, електромагнітна сумісність), у яких буде здійснюватись доступ продукції на ринки сторін на основі дії Угоди АСАА.

1.4 Висновки до розділу 1

Розділ присвячений дослідженню нормативно-правових аспектів технічного регулювання та оцінки відповідності забезпечення кібербезпеки підключеного автомобіля та дослідженню технічного регламенту як основи державного регулювання. Зазначено коректну термінологію, та роз’яснено важливість аспекту технічного регулювання в контексті державного регулювання кібербезпеки транспортних засобів.

2 ПІДКЛЮЧЕНИЙ АВТОМОБІЛЬ ТА ПОВ’ЯЗАНІ З НИМ РИЗИКИ

2.1 Поняття про підключений автомобіль

Автомобільна промисловість є свідком радикальних змін, оскільки виробники автомобілів запроваджують нові технології, які, здається, взяті прямо з майбутнього. Сучасні виробники автомобілів інвестують значні кошти в розробку власних операційних систем і програм, які вони пропонують майже в усіх своїх продуктах. Підключені автомобілі стали новою нормою в автомобільній промисловості, і ми можемо лише очікувати, що вони стануть безпечнішими та зручнішими. Дизайн підключених автомобілів постійно вдосконалюється, роблячи їх більш ергономічними та футуристичними. Сьогодні підключений автомобіль має багато зручних і розумних функцій. Ці функції допомагають покращити загальні враження від водіння, зробити поїздку безпечнішою, зменшити затори та надати інформацію в реальному часі, а також додати систему безпеки з розширеними функціями безпеки.[1]

Підключені транспортні засоби – це інноваційні допоміжні системи, (частково) автономне водіння, мережеве виробництво за участю постачальників, підключені автомобілі з підключеними сервісами — цифровізація чітко проявляється майже в кожній галузі автомобільної промисловості, і вона швидко прогресує.

Підключений автомобіль — 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 всередині, так і зовні автомобіля. Очікується, що для критичних для безпеки додатків автомобілі також будуть підключатися за допомогою спеціального зв'язку ближнього радіусу дії (DSRC) або стільникових радіостанцій, які працюють у діапазоні 5.9 ГГц, наданій FCC з дуже низькою затримкою.

Обидва варіанти США та ЄС зосереджені на зв'язку 5,9 ГГц, однак 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 і масштабованим. Разом з іншими новими 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. [2]

Підключений автомобіль має підключення до Інтернету через вбудований чіп або SIM-карту за умови стабільного покриття бездротової мережі. Connected Vehicles також може завантажувати бездротові оновлення, видані виробником, і надає доступ до інших онлайн-додатків і послуг.

Hyundai розробила вбудовану eSIM-карту Vodafone-Idea для свого компактного SUV Venue. Позашляховик не потребує підключення смартфона користувача до безлічі опцій, таких як розваги, навігація та екстрене реагування тощо.

Вбудовані eSIM ідентифікують окремі транспортні засоби, шифрують зв’язок і забезпечують безпечне глобальне підключення до інтелектуальних транспортних систем, включаючи рішення для екстрених викликів eCall, транспортну телематику, навігацію тощо.

Європейська комісія вже вибрала eSIM як частину системи екстреного виклику в автомобілі.

Відповідно до GSMA, eSIM допоможе виробникам автомобілів пропонувати будь-який тип послуги, підключеної до автомобіля через SIM-карту, яка може бути забезпечена профілем мобільного оператора після доставки автомобіля, а також після закінчення контракту, без SIM потрібно змінити.

Вбудований SIM-модуль в автомобілі / підключення через смартфон /

Підключені транспортні засоби оснащені спеціальними додатками для смартфонів, які підключаються до автомобіля через бездротову мережу. Ці програми дозволяють користувачам віддалено керувати такими функціями автомобіля, як замикання/відмикання дверей, відкривання люка, запуск/зупинка двигуна, клімат-контроль, увімкнення/вимкнення фар і звуковий сигнал. Додаток також допоможе визначити місцезнаходження автомобіля за допомогою бортового GPS.

Нещодавно компанія Cerence Inc. співпрацювала з HARMAN для голосової підтримки програм сторонніх розробників, доступних у HARMAN Ignite Store. Завдяки системі розпізнавання голосу Cerence на базі штучного інтелекту автовиробники, які розгортають магазин HARMAN Ignite Store, можуть запропонувати безпечний доступ до широких можливостей платформи без використання рук, забезпечуючи безперебійний і потужний досвід своїм водіям. Cerence надає технологію розпізнавання мовлення та розуміння природної мови, яка буде інтегрована з програмами в магазині Ignite, щоб водії могли вибрати будь-яку програму, яка їх цікавить, не відриваючи рук від керма.

Геозонування визначає географічну зону для відстеження транспортних засобів, якщо вони в'їжджають або виїжджають із цієї зони. У геозоні система використовує технологію GPS, а також використовує інші сигнали даних, включаючи стільниковий зв’язок і WiFi.

Технології Vehicle to Vehicle (V2V) або Vehicle to Everything (V2X) дозволяють транспортним засобам спілкуватися один з одним. V2V дозволяє обмінюватися важливою інформацією, такою як рух транспорту, стан доріг, обмеження швидкості та багато іншого. Згідно з новим дослідницьким звітом аналітичної фірми IoT Berg Insight, наприкінці 2020 року на дорогах було близько 0,7 мільйона автомобілів із можливостями V2X. Очікується, що до 2025 року це число зросте до 35,1 мільйона. Обговорювалося питання зв’язку між

транспортними засобами. протягом більше двох десятиліть, але з невеликою кількістю реалізацій.

Підключені транспортні засоби мають кілька важливих функцій безпеки, як-от обмін інформацією про місцезнаходження/відстеження в реальному часі, екстрені виклики SOS у разі аварії, допомога на дорозі у разі поломки автомобіля та багато іншого. Окрім вбудованих інструментів безпеки, ці інтелектуальні функції безпеки стають у пригоді у складних ситуаціях.

Рішення SDL базуються на безпечній хмарній інфраструктурі, яка дозволяє клієнтам збирати, обробляти, аналізувати та передавати дані про сотні тисяч «підключених» автомобілів. SDL розробила власний телематичний модуль, рішення для запобігання крадіжкам, картографічний сервіс, системи скорингу, готові до використання базові рішення для створення фінтех-продуктів, професійний портал для управління автопарком і кастомні мобільні додатки для власників автомобілів і водіїв.

Хоча робота над мережею 5G для операторів мобільного зв’язку все ще триває, темпи розгортання та запуску прискорюються. Станом на кінець лютого 2022 року, за даними GSA (Global Mobile Suppliers Association), 489 операторів у 146 країнах інвестували в мережі 5G у формі тестування, пілотних проектів, придбання ліцензій, запланованого та фактичного розгортання. З них 209 операторів у 83 країнах запустили комерційні послуги 5G, сумісні з 3GPP. Крім того, GSA повідомила, що 99 операторів інвестують у автономні 5G для публічних мереж.

Відповідно до звіту VIAVI Solutions, опублікованого в червні 2021 року, кількість міст з мережами 5G у всьому світі зросла до 1662.

Величезний попит на більш високі швидкості та кращий зв’язок серед азіатських клієнтів стимулює розгортання мереж 5G. Проте з точки зору розширення пропускної здатності та впровадження 5G Китай і США значно випереджають інші країни.

Відповідно до звіту IANS (Індо-Азіатська служба новин), до 2025 року кожен четвертий автомобіль матиме підключення до 5G, що, серед інших удосконалень, дозволить краще використовувати передачу даних у реальному часі та швидкий зв’язок із хмарою автомобіля. Дослідження показало, що автомобілі з підтримкою 4G досягають зрілості в таких розвинених країнах, як США, Китай, Німеччина та Великобританія, разом із появою телематичних блоків керування (TCU) 5G.

Безперебійне підключення транспортних засобів і можливість двостороннього зв’язку для перекладу великої кількості даних і обміну ними через безперебійну мережу. Такі транспортні засоби не лише збирають інформацію про себе, але й про оточення, інші транспортні засоби та обмінюються нею через єдину мережу. Якщо ви поєднаєте рівень зберігання даних підключених транспортних засобів із хмарною інфраструктурою, це призведе до належного зберігання та використання. Використовуючи цю комбінацію, водії автомобілів отримають реальне уявлення про транспортний засіб, географічне розташування, моделі використання споживачами та зміни навколишнього середовища.

Хоча розширене підключення до транспортного засобу, безумовно, покращило враження від водіння, підключені автомобілі збирають, обробляють і генерують величезні обсяги даних. Деякі коментатори прогнозують, що автономні автомобілі створюватимуть 4000 гігабайт (ГБ) даних на день, що становить понад 1400 терабайт (ТБ) даних на рік.

Європейська рада із захисту даних (EDPB) прийняла та опублікувала остаточну версію Рекомендацій 01/2020 щодо обробки персональних даних у контексті програм, пов’язаних із підключеними транспортними засобами та мобільністю.

Ці рекомендації щодо підключених автомобілів адресовані традиційним зацікавленим сторонам в автомобільній промисловості та новим гравцям у

цифровій індустрії. Рекомендації включають додатковий розділ із прикладами для надання практичних рекомендацій, таких як:

- визначення договірних зобов’язань як правової основи для обробки даних послуг страхування за принципом «оплата за кермом» і «оплата за кермом»;
- для страхових послуг на основі використання страхові компанії повинні отримувати лише згенеровані числові оцінки, а не необроблені дані автомобільної телематики;
- визначення договірного зобов'язання як правової основи для обробки даних послуг оренди-паркування;
- лише передача даних автомобільних систем службам екстреної допомоги та сервісним партнерам у разі серйозної аварії, що викликає екстрений дзвінок eCall на номер 112, який є обов’язковим з 2018 року;
- лише збереження даних, отриманих у eCall на номер 112, доки вони не знадобляться для обробки екстреної ситуації;
- використання згоди як правової основи для досліджень або досліджень, для яких суб’єкти даних добровільно надають дані;
- використання згоди як правової основи для обробки даних про місцезнаходження транспортного засобу у випадку викрадення автомобіля, коли суб’єкти даних хочуть знайти транспортний засіб.

Підключені автомобілі мають дані та можливості відстеження, які можуть допомогти страховикам розробити точні стратегії ціноутворення на основі поведінки споживачів за кермом. Дані, зібрані підключеними автомобілями, також можуть допомогти страховикам спростити процес розгляду претензій і заощадити кошти.

Але збільшення зв’язку в підсумку означає все значне збільшення коду, і цей код може бути скомпрометований різними способами. Зрештою, сучасні автомобілі містять до 150 електронних блоків управління і близько 100 мільйонів рядків коду, який, як очікується, збільшиться втричі до 2030 року. Кількість

програмного забезпечення в сучасних автомобілях вже в чотири рази більше, ніж у літака-винищувача. Особливу увагу слід приділяти IT-безпеці чи автомобільній кібербезпеці не лише після пандемії COVID-19 та пов'язаного з нею зростання кібератак. Транспортний засіб повинен мати можливість гарантувати його функціональну безпеку в будь-який час. Потенціал шкоди від кібератак на розумні автомобілі величезний. Треба розглянути можливі сценарії загроз, пов'язаних із великими обсягами атак («Всі електронні гальма в автомобілях виробника одночасно паралізовані хакерською атакою»). Тут потрібні точні, ефективні концепції безпеки.

Управління технологічними вузлами «розумного» автомобіля здійснюється через електронні блоки управління (ЕБУ). ЕБУ — це комп'ютер, який збирає дані з підключених до нього датчиків, кнопок, перемикачів, кнопок, обробляє їх та подає команди на виконавчі механізми. Найважливіша частина кожного ЕБУ — його програмне забезпечення, від якого залежить надійність функціонування транспортного засобу. У деяких автомобілях налічується понад 100 ЕБУ. Взаємодія між ЕБУ відбувається за допомогою протоколів CAN/CAN FD, LIN, MOST, Ethernet і FlexRay. Їхня загальна риса — підвищена надійність. Вони стійкі до збоїв в жорстких умовах експлуатації автомобіля, проте в жодному з них не передбачено вбудованих функцій безпеки у вигляді шифрування даних або автентифікації пристроїв. У найближчому майбутньому очікується поява масових моделей, оснащених вдосконаленими системами допомоги водієві (ADAS), автопілотами, а також системами взаємодії між автомобілями (V2V) і з дорожньою інфраструктурою (V2I). Такі системи допоможуть запобігати ДТП або пом'якшувати їхні наслідки, проте також і створюватимуться нові можливості для зловмисників. Популярність каршерингa зробила затребуваною функції централізованого контролю автопарку, наприклад, можливість відстежувати кожен автомобіль в реальному часі, збирати телеметричні дані і керувати режимами роботи двигуна. Затребуваність нових технологій змушує

автовиробників скорочувати цикли розробки і виробництва, щоб продовжувати нарощувати темпи впровадження нових технологій. Гонка технологічної оснащеності призводить до того, що питання кібербезпеки залишаються невирішеними. Результат закономірний: нові автомобілі містять безліч потенційних вразливостей

Приблизно шість років тому всерйоз взялися за кібербезпеку, почали інвестувати в проєктування та розвиток кіберзахисних рішень [8]. На сьогодні в автомобільній індустрії кібербезпека забезпечується як апаратними, так і програмними рішеннями, але потрібно пройти довгий шлях, перш ніж усі ЕБУ (електронні блоки керування) в машині будуть захищені від активності кібератак. Кібербезпека в автомобільному будівництві значно складніша, ніж на смартфонах і персональних комп'ютерах, з двох основних причин:

а) десятки ЕБУ у кожній машині з'єднані множиною електронних шин і відповідають за різні функції та характеристики;

б) множина потенційних точок доступу як розташованих всередині автомобіля, так і віддалених, зокрема: OBDII, USB та SD порти, безключовий доступ, Bluetooth і WiFi, вбудований модем, датчики, інфотейнмент або застосунок для смартфонів, а також множина підключень із використанням телеметричних та інших хмарних систем, що мають доступ до систем автомобіля.

Що зазвичай відбувається під час традиційної IT-атаки на підключений автомобіль? Фірма Trend Micro Incorporated проаналізували чотири тематичні дослідження віддаленого злому автомобілів (Jeep Hack 2015, Tesla Hack 2016 та 2017 та BMW Hack 2018) та виявили закономірність, за якою слідували ці атаки (рис. 1) [9].

Рисунок 2.1 – Узагальнений ланцюг віддалених атак хакерів на основі тематичних досліджень віддалених атак

2.2 Ризики пов’язані з кібербезпекою підключеного автомобіля

Нагода для оптимізму полягає в тому, що в галузі автомобільної кібербезпеки все більше робиться для оснащення автомобіля власним апаратним і програмним забезпеченням, а також для розвитку хмарових платформ, що забезпечують кібербезпеку. Формується декілька стандартів і регламентів, які регулюють кібербезпеку, що додатково сприяють розгортанню кіберзахисних рішень у всіх автомобілях, які підключаються. Кібербезпека автомобіля: поточний стан Компанія Upstream Security надрукувала декілька різних звітів з аналізом кібератак на автомобілі. Новітній із цих звітів, виданий на початку 2021 р. містить інформацію за період з 2010 до 2020 рр. і розглядає понад 200 кіберінцидентів з автомобілями по всьому світу. Звіт містить інформацію про глибокі мережі та

даркнет (DarkNet – прихована мережа), де кіберзлочинці, які спеціалізуються на автомобілях, мають можливість спілкуватися, зберігаючи значну анонімність. Існують форуми, де детально обговорюють атаки на підключені транспортні засоби, доступ до конфіденційних даних, перехват управління автомобілем та способи угону машини. Навіть у «поверхневому» інтернеті кіберзлочинці часто знаходять інтернет магазини, що торгують інструментами для зламу, сервісами, які відключають імобілайзери, кодграббери, а також довідками щодо угону машини.

Таблиця 2.1 – Напрямок атак на автомобільному транспорті за 2010–2020 рр. від Upstream Security

Апаратні або програмні компоненти	Доля від цього
Хмарні сервери	32,9%
Безключовий доступ/ брелок для ключів	25,3%
Мобільний застосунок	9,9%
Порт комп’ютерної діагностики автомобіля	32,9%
Система інфотейнменту (мультимедійний інтерфейс)	8,4%
IT-система	7%
Датчики	4,8%
Шлюз між блоками управління електронікою та телематикою	4,3%
Бортова мережа	3,8%

Із таблиці 2.1 чітко видно, що найбільш популярні дві цілі: хмарні сервери (бо вони є воротами для 33 % усіх кібератак, оскільки хакери намагаються отримати доступ до цінних паперів, що можуть бути використані для зламу кіберзахисту автомобіля) та незахищений безключовий доступ (електронні

брелоки також часто застосовуються для проникнення в машину та угону). Замикають трійку мобільні застосунки: через них здійснюється близько 10 % кібератак. Цікаво, що сумарна доля віддалених атак становить приблизно 80 %, а доля фізичних атак – близько 20 %. У лютому 2021 р. Агентство з мережної та інформаційної безпеки Євросоюзу (ENISA) надрукувала документ «Виклики кібербезпеки, які зв'язані з упровадженням штучного інтелекту в автономному водінні». Звіт дозволяє скласти враження про виклики кібербезпеки, пов'язані з використанням ШІ-технологій (технологій штучного інтелекту) в автомобілях. Проблема описана в контексті політики, що реалізується як на європейському, так і більш широкому, міжнародному рівні. У листопаді 2019 р. ENISA надрукувала документ «Рекомендації про забезпечення інформаційної безпеки розумних автомобілів», в якому визначені практики, що рекомендуються для забезпечення безпеки підключених автомобілів та напівавтономних транспортних засобів. А 2017 р. ENISA надрукувала документ «Кібербезпека та надійність розумних автомобілів», в якому основна увага приділена практикам, що рекомендуються для виробників автомобільних комплектуючих та для їхніх постачальників із метою захисту автомобільних систем, що встановлюються, від кібератак. Основна вимога до стандартів та регламентів у галузі кібербезпеки – захистити автомобіль протягом усього його життєвого циклу – від проєктування до виробництва й далі до використання клієнтом. Після дворічної підготовки та редагування ООН 24 червня 2020 р. прийняла документ WP/29 ЕЄК, який регулює питання кібербезпеки. WP.29 діє у 54 країнах, зокрема ЄС, Великої Британії, Японії та Південної Кореї. На ці 54 країни доводиться близько 35 % світового виробництва автомобілів. У багатьох інших країнах приймаються автомобілі, що відповідають нормам ООН. США не входять до складу цих 54 країн. Усі виробничники, зокрема автовиробники із США, які продають автомобілі на світових ринках, мають дотримуватися вимог кібербезпеки, що викладені в WP.29 щодо всієї їхньої продукції та процесів. Регламенти ООН є юридично забезпеченими. Якщо країна

або регіон приймає регламент WP.29, то від усіх діючих у ній виробників комплектуючих вимагається доказ відповідності для проходження обов'язкової сертифікації та подальшого права працювати на ринку. У Європі проходження обов'язкової сертифікації вимагає взаємного визнання відповідно до нормам на рівні всього автомобіля. Якщо виробник отримує сертифікат на автомобіль визначеного типу в одній країні ЄС, то може продавати таку модель у всіх країнах ЄС без подальших перевірок. У червні 2020 р. були прийняті дві нові регламентні норми ООН щодо кібербезпеки в межах документа WP.29. Дві норми, що застосовуються до транспортних засобів усіх типів, були оновлені в березні 2021 р. Упровадження цих норм у деяких країнах починається 2021 р. і 2022 р., а найбільш широке впровадження відбудеться 2023 р. і 2024 р. У першому документі основна увага приділяється кібербезпеці й системам управління кібербезпекою (CSMS). Під CSMS розуміється системний підхід на основі оцінки ризиків, що визначають організаційні процеси, зони відповідальності та управління для правильного тлумачення ризиків, пов'язаних із кіберзагрозами транспортним засобам та їхнім захистом від кібератак. У документі CSMS детально розглянуті загрози, пов'язані з кібербезпекою, та наведена значна кількість прикладів нападів і методів кібератаки. У додатку 5 міститься 10 аркушів з описом вразливостей, розподілених за множинними категоріями. У першій із таблиць документа CSMS, який наводиться за вищевказаною адресою, узагальнені загрози й вразливості. Існують шість типів загроз та множина типів вразливостей (29) з великою кількістю прикладів (67), що перелічені в документі CSMS. Другий документ стосується процесів оновлення програмного забезпечення та систем управління актуальними оновленнями (SUMS). У ньому наводиться система управління оновленнями програм як системний підхід, що визначає, які організаційні процеси й процедури мають відповідати вимогам за доставку програмних оновлень згідно із цим регламентним документом. Нова норма ООН про універсальні передумови до оновлень програм і систем управління

оновленнями програм стосується автомобілів, робота яких залежить від оновлення програмного забезпечення. Ця норма стосується трейлерів і сільської господарчої техніки, а також пасажирського транспорту, фургонів, грузовиків і автобусів.

Підключений до інтернету автомобіль має значну кількість відкритих портів, які потенційно можуть використовувати кіберзлочинці. А враховуючи поверхове ставлення до питань безпеки з боку розробників автомобілів, проникнення в будь-який доступний ЕБУ — відносно проста задача. Перехопивши контроль над одним модулем, атакуючий може переміщатися від одного керуючого блоку до іншого і виробляти найрізноманітніші види атак, наприклад:

• DoS-атаки на ЕБУ рульового керування або гальмівної системи, які можуть призвести до аварії зі смертельним наслідком;

• блокування інформаційно-розважальної системи, або відключення запуску двигуна з вимогою викупу;

• впровадження недійсних даних у потік обміну між модулями або модифікацію переданих даних з метою, наприклад, порушити режим роботи двигуна і вивести його з ладу;

• відключення ЕБУ з використанням протоколів виявлення помилок;

• перехоплення керування автомобілем, в результаті якого може статися аварія, причому встановити справжнього винуватця в цьому випадку практично неможливо.

Вразливі діагностичні сканери

Додатковим джерелом загроз часто стають самі власники автомобілів з числа ентузіастів чіп-тюнінгу. Вони набувають Wi-Fi – або Bluetooth-сканери, які підключаються до шини CAN через діагностичний роз’єм OBD-II. Як правило, прошивка таких сканерів не містить засобів захисту від атак, тому будь-який бажаючий може розміститися по сусідству з ноутбуком, перехопити контроль над донглом і додати трохи «чіп-тюнінгу» на свій розсуд.

Головні мультимедійні пристрої

Ще один уразливий елемент, який рідко беруть до уваги, — головні мультимедійні пристрої з GPS-навігацією та іншими функціями. Автовласники часто заміняють штатні мультимедійні системи на альтернативні, щоб отримати додаткові можливості. Велика частина таких пристроїв працює на застарілих версіях Android, які практично не оновлюються. Популярна серед водіїв функція автоматичної адаптації гучності звуку до швидкості руху вимагає, щоб головний пристрій підключено до шини CAN. В результаті віддалений зловмисник може скористатися відомими уразливими місцями Android, щоб провести атаку на CAN-шину.

Найнеприємніше: вразливі версії Android використовуються навіть у штатних мультимедійних пристроях деяких автомобілів.

Небезпечні прошивки

Практично кожен власник «розумного» автомобіля хоче, щоб його цей автомобіль став швидше і потужніше, ніж передбачено виробником. А краще всього, якщо вийде додати функції старшої моделі в більш дешеву молодшу. Гаражні майстерні, що спеціалізуються на таких модифікаціях, замінюють прошивки ЕБУ, які являють собою ОС разом з завантажувачем. Цим умільцям не заважає навіть те, що файли прошивок повинні бути підписані цифровим підписом виробника: модифікуючи код в ЕБУ, вони відключають перевірку підпису, в результаті чого блок працює з будь прошивкою, в тому числі і з шкідливою.

Уразливості в шині CAN

Розроблена компанією Bosch в 1983 році шина CAN була офіційно представлена в 1986-му, а вперше використано в серійних автомобілях у 1989-му, Через чотири роки ISO прийняла CAN в якості стандарту для автомобілів, і з тих пір ця шина і відповідний протокол для обміну даними використовуються практично в кожному транспортному засобі.

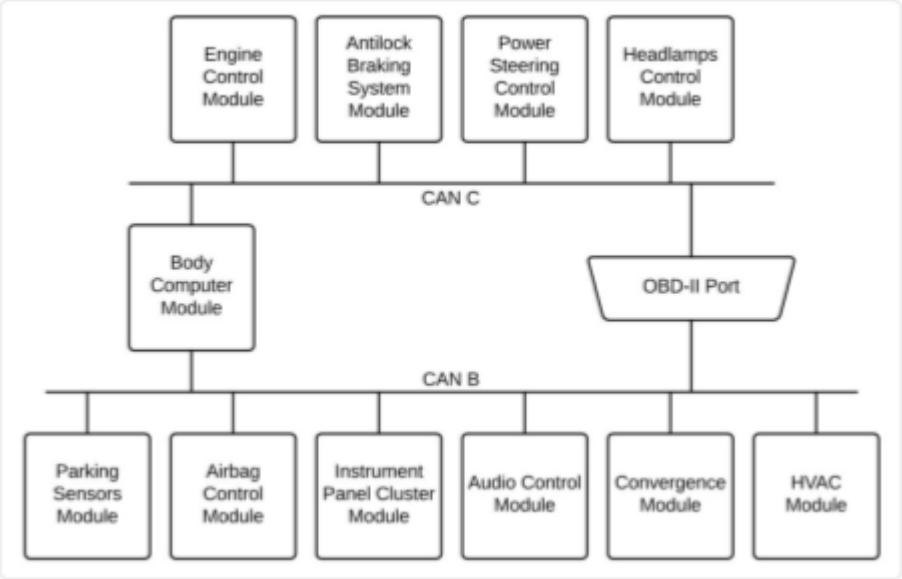

Рисунок 2.2 – Системи автомобіля, підключені до CAN

Всі пристрої автомобіля взаємодіють через шину CAN. Завдяки цьому головний мультимедійний пристрій дізнається, отримавши інформацію про спрацювали подушки безпеки, що потрібно подзвонити в екстрену службу і повідомити про аварію.

Підключення до CAN пристрою взаємодію між собою, передаючи особливі повідомлення — фрейми. Ці повідомлення можуть містити різну інформацію, включаючи повідомлення про помилки. Об’єднана команда дослідників розробила атаку на шину CAN, яка експлуатує наявні в цьому випадку особливості обробки помилок:

1) помилки виникають, коли пристрій зчитує значення, які не відповідають вихідного очікуваного значення на кадрі;

2) коли пристрій виявляє таку подію, воно записує повідомлення про помилку на шину CAN, щоб «відкликати» помилковий кадр і повідомити інші пристрої, щоб вони проігнорували його;

3) якщо пристрій посилає занадто багато помилок, то, як наказують стандарти CAN, воно переходить у стан Bus Off, тобто відключається від CAN і не

може 10 прочитати або записати дані в CAN, — ця функція допомагає ізолювати явно несправні пристрої, щоб вони не заважали роботі інших систем;

4) передаючи досить велика кількість помилок, можна домогтися того, щоб цільове пристрій перейшло в стан Bus Off, тобто відключилася.

Це може стати небезпечним і навіть фатальним, особливо якщо вдасться так вимкнути подушки безпеки або ABS.

Щоб провести атаку, досить підключити до CAN пристрій, яке буде повторно надсилати в CAN кадри з помилками. А для підключених автомобілів не потрібно ніякого пристрою — достатньо скористатися уразливими в ЕБУ і запустити атаку дистанційно.

2.3 Стандарти кібербезпеки підключених автомобілів

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. Ось чому був розроблений стандарт ISO 21434 – для сприяння кібербезпеці в системах дорожніх транспортних засобів.

Стандарт ISO/SAE 21434 встановлює межі кібербезпеки для автомобільних компаній і містить єдину термінологію для спілкування та управління ризиками, що пов’язані з кібербезпекою. Незважаючи на те, що зазначене не належить безпосередньо до технологій як таких і не сприяє їхньому впровадженню, надані межі розширюють співробітництво у сфері кібербезпеки в галузі автотранспорту й таким чином приведуть до появи технологій і рішень, що краще відповідатимуть проблемам кібербезпеки сьогодні й у майбутньому. Це допоможе розглядати проблеми кібербезпеки на кожному етапі процесу розроблення та в польових умовах, створювати контрольний лист для інженерів, що передбачають сканування на наявність помилок, збільшення кількості власних засобів

кіберзахисту й проведення аналізу ризиків потенційних вразливостей за кожним компонентом.

Стандарт ISO/SAE 21434 вже задіяний для підтримки чинних правил. З метою подальшого покращення взаємозв'язку між регулюванням та стандартизацією в Організації Об'єднаних Націй нещодавно почалась робота над загальнодоступною специфікацією ISO/PAS 5112, в якій містяться вказівки керівництву організацій з організаційних аудитів щодо інженерних аспектів кібербезпеки. Вона буде основана на стандарті ISO/SAE 21434 і призначена для проведення аудиту систем управління кібербезпекою, як це визначено в постанові ООН. Даний стандарт призначений покращити кібербезпеку автомобілів і знизити ризики за всією довжиною ланцюга постачання – від розроблення й проєктування автомобілів до їхнього введення в експлуатацію. Багато представників галузі вже будують плани щодо забезпечення його інтеграції. Кінцевою метою є широке впровадження цього стандарту в повсякденну інженерну практику галузі поряд із підвищенням інформованості, яка досягається за рахунок включення вищезгаданого стандарту в навчальну програму підготовки інженерів.

ISO 21434 — це стандарт, розроблений Міжнародною організацією зі стандартизації (ISO). Його розроблено, щоб створити основу для кібербезпеки в системах дорожніх транспортних засобів. Стандарт охоплює все: від оцінки та управління ризиками до засобів контролю безпеки та стратегій пом'якшення. Тобто, ISO 21434 стосується захисту транспортних засобів від кібератак.

ISO 21434 базується на стандарті ISO/SAE 21434, розробленому Товариством автомобільних інженерів (SAE). Стандарт ISO/SAE 21434 — це набір інструкцій щодо кібербезпеки в транспортних засобах. Його створили у відповідь на зростання кількості кібератак на легкові та вантажівки. Стандарт ISO/SAE 21434 є добровільним, але ISO 21434 є обов'язковим для всіх членів ISO.

ISO 21434 включає чотири основні частини:

- оцінка та управління ризиками,

- засоби контролю безпеки,
- зв’язок та обмін інформацією,
- стратегії пом’якшення.

Оцінка та управління ризиками: ISO 21434 вимагає від організацій оцінювати та керувати ризиками для систем автомобіля. Це включає виявлення, оцінку та управління ризиками кібербезпеки. Організації також повинні мати план боротьби з кіберінцидентами.

Контроль безпеки: ISO 21434 вимагає від організацій впровадження заходів безпеки для захисту транспортних засобів від кібератак. Ці елементи керування включають такі речі, як автентифікація, авторизація та шифрування.

Комунікація та обмін інформацією: ISO 21434 вимагає від організацій обмінюватися інформацією про ризики та інциденти кібербезпеки. Це включає в себе обмін інформацією з постачальниками, клієнтами та іншими зацікавленими сторонами.

Стратегії пом'якшення: ISO 21434 вимагає від організацій мати стратегії пом’якшення наслідків кіберінцидентів. Ці стратегії мають бути розроблені таким чином, щоб мінімізувати вплив інциденту на системи автомобіля.

Сьогодні кожен транспортний засіб оснащено потужністю штучного інтелекту. Від Wi-Fi і Bluetooth до підключення USB і LTE, автомобіль надзвичайно завантажений високотехнологічними речами, що робить його більш привабливим і сучасним. Все це разом робить транспортний засіб не тільки більш потужним, але й дуже схильним до кібератак.

Метою ISO 21434 є захист транспортних засобів від усіх видів кібератак. Цей стандарт надає організаціям основу для оцінки, управління та пом’якшення ризиків для систем автомобіля. ISO 21434 розроблено, щоб гарантувати, що кібербезпека враховується на кожному етапі розробки продукту, від початку до виходу з експлуатації.

ISO/IEC 27001 є провідним міжнародним стандартом для впровадження цілісної системи управління інформаційною безпекою. Більшість організацій мають ряд засобів контролю інформаційної безпеки . Однак без системи управління інформаційною безпекою (СУІБ) засоби контролю, як правило, дещо неорганізовані та роз'єднані, часто реалізуються як точкові рішення для конкретних ситуацій або просто як умовність. Засоби безпеки, що діють, зазвичай стосуються певних аспектів інформаційних технологій (IT) або безпеки даних спеціально; в цілому залишаючи інформаційні активи, не пов'язані з IT (такі як документообіг і власні знання), менш захищеними. Крім того, плануванням безперервності бізнесу та фізичною безпекою можна керувати абсолютно незалежно від IT або інформаційної безпеки, тоді як практика відділу людських ресурсів може мало згадувати про необхідність визначення та розподілу ролей та обов'язків у сфері інформаційної безпеки в усій організації. ISO/IEC 27001 вимагає, щоб менеджмент:

- Систематично досліджувати ризики інформаційної безпеки організації, враховуючи загрози, вразливі місця та вплив;
- Розробити та запровадити послідовний і комплексний набір засобів контролю інформаційної безпеки та/або інших форм обробки ризиків (таких як уникнення ризиків або передача ризиків) для усунення тих ризиків, які вважаються неприйнятними; і
- Прийміть загальний процес управління, щоб гарантувати, що засоби контролю інформаційної безпеки продовжують постійно задовольняти потреби організації в інформаційній безпеці.

Які засоби контролю будуть перевірені в рамках сертифікації за ISO/IEC 27001, залежить від аудитора сертифікації. Це може включати будь-які засоби контролю, які організація вважає такими, що входять до сфери застосування СУІБ, і це тестування може здійснюватися на будь-якій глибині чи обсязі, оціненому

аудитором, якщо це необхідно для перевірки того, що засоби контролю запроваджено та діє ефективно.

Керівництво визначає сферу застосування СУІБ для цілей сертифікації та може обмежити її, скажімо, одним бізнес-підрозділом або місцезнаходженням. Сертифікат ISO/IEC 27001 не обов'язково означає, що решта організації, за межами сфери дії, має адекватний підхід до управління інформаційною безпекою.

Інші стандарти сімейства стандартів ISO/IEC 27000 надають додаткові вказівки щодо певних аспектів проектування, впровадження та експлуатації СУІБ, наприклад щодо управління ризиками інформаційної безпеки (ISO/IEC 27005).

ISO 26262 під назвою «Дорожні транспортні засоби – Функціональна безпека» — це міжнародний стандарт функціональної безпеки електричних та/або електронних систем, які встановлюються в дорожні транспортні засоби серійного виробництва (за винятком мопедів), визначений Міжнародною організацією стандартизації (ISO).

Функціональні функції безпеки є невід'ємною частиною кожного етапу розробки автомобільного продукту, починаючи від специфікації і закінчуючи проектуванням, впровадженням, інтеграцією, перевіркою, перевіркою та випуском у виробництво. Стандарт ISO 26262 є адаптацією стандарту функціональної безпеки IEC 61508 для автомобільних електричних/електронних систем. ISO 26262 визначає функціональну безпеку для автомобільного обладнання, що застосовується протягом життєвого циклу всіх автомобільних електронних та електричних систем безпеки.

Перше видання (ISO 26262:2011), опубліковане 11 листопада 2011 року, було обмежено електричними та/або електронними системами, встановленими в «легкових автомобілях серійного виробництва » з максимальною повною масою 3500 кг. Друге видання (ISO 26262:2018), опубліковане в грудні 2018 року, розширило сферу застосування з легкових автомобілів на всі дорожні транспортні засоби, крім мопедів . [1]

Стандарт спрямований на вирішення можливих небезпек, спричинених несправністю електронних та електричних систем транспортних засобів. Незважаючи на назву «Дорожні транспортні засоби – функціональна безпека», стандарт стосується функціональної безпеки електричних і електронних систем, а також систем в цілому або їх механічних підсистем.

Як і його вихідний стандарт, IEC 61508 , ISO 26262 є стандартом безпеки, заснованим на оцінці ризику, де якісно оцінюється ризик небезпечних робочих ситуацій і визначаються заходи безпеки, щоб уникнути або контролювати систематичні збої, а також виявити або контролювати випадкові збої апаратного забезпечення або пом’якшити їхні ефекти.

Цілі ISO 26262:

●Забезпечує життєвий цикл автомобільної безпеки (управління, розробка, виробництво, експлуатація, обслуговування, виведення з експлуатації) і підтримує адаптацію необхідних дій на цих етапах життєвого циклу.

●Охоплює аспекти функціональної безпеки всього процесу розробки (включно з такими видами діяльності, як специфікація вимог, проектування, впровадження, інтеграція, верифікація, валідація та конфігурація).

●Забезпечує специфічний для автомобільного транспорту підхід, заснований на ризиках, для визначення класів ризику (автомобільних рівнів безпеки , ASIL).

●Використовує ASIL для визначення необхідних вимог безпеки для досягнення прийнятного залишкового ризику .

●Містить вимоги до заходів валідації та підтвердження для забезпечення досягнення достатнього та прийнятного рівня безпеки.

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

кіберзагрозами для транспортних засобів, та захисту транспортних засобів від кібератак.

Основними характеристиками CSMS є:

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

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

●Моніторинг нових вразливостей і відомих атак для відповіді новими оновленнями.

●Дозволяє незалежну оцінку акредитованим інститутом тестування.

●Важливий плюс на практиці: систематизація кібербезпеки, яка супроводжується запровадженням CSMS, робить обов’язковим для компаній вирішувати питання інформаційної безпеки у ризик-орієнтований спосіб.

Це включає повне визначення та оцінку ризиків, а також продумування ймовірності їх виникнення. Ця оцінка ризику забезпечує надійну відправну точку для зниження конкретної потенційної шкоди до прийнятного рівня–перевірений і прагматичний підхід. Подібні системи допомагають відслідковувати відповідність визначеним регламентам, таким як наприклад: Дві нові норми ООН щодо кібербезпеки та оновлень програмного забезпечення допоможуть упоратися з цими ризиками, встановивши чіткі вимоги щодо ефективності та аудиту для виробників автомобілів. Це перші міжнародно гармонізовані та обов'язкові норми в цій сфері.

Два нових правила ООН, ухвалені Всесвітнім форумом ЄЕК ООН з гармонізації правил щодо транспортних засобів, вимагають, щоб заходи впроваджувалися в 4 різних дисциплінах: Управління кіберризиками транспортних засобів; Захист транспортних засобів за проектом для зменшення ризиків уздовж ланцюжка створення вартості; Виявлення та реагування на інциденти безпеки в автопарку; Забезпечення безпечних і захищених оновлень

програмного забезпечення та гарантування безпеки транспортного засобу без шкоди, запроваджуючи правову основу для так званих «повітряних» (OTA) оновлень бортового програмного забезпечення автомобіля.

Правила стосуватимуться легкових автомобілів, мікроавтобусів, вантажівок та автобусів. Вони набули чинності в січні 2021 року. Згідно з правилами ЄС, виробники повинні завжди забезпечувати функціональність своїх систем управління та детально документувати статус всього свого програмного забезпечення.

Щоб забезпечити сертифікований стандарт функціональності CSMS, Міжнародна організація зі стандартизації (ISO)разом із Товариством автомобільних інженерів (SAE) опублікували ISO/SAE 21434 у серпні 2021 року. У професійних колах очікується, що ISO/SAE 21434 стане основою, визнаною органами сертифікації для впровадження системи управління кібербезпекою у виробника транспортних засобів.

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

Для сертифікації системи керування оновленням програмного забезпечення стандартом має стати ISO 24089. Однак на даний момент дизайн цього стандарту все ще відкритий. Україна також згідно чинного законодавства починає використовувати встановлені стандарти через 30 календарних днів з моменту його прийняття.

2.4 Висновки до розділу 2

Сьогодні вибіркових заходів уже недостатньо для цілісного захисту транспортних засобів. Натомість потрібні системні та стратегічні підходи, які визначають чіткі вимоги до обсягу, продуктивності та аудиту системи безпеки. Стратегічний підхід повинен охоплювати весь життєвий цикл продукту. Тут, наприклад, потрібно зосередитися на довгостроковій доступності оновлень програмного забезпечення або на інтеграції всього ланцюжка поставок. Щоб створити належну основу для автомобільної кібербезпеки, Всесвітній форум з гармонізації транспортних правил (World Forum for Harmonization of Vehicle Regulations) Європейської економічної комісії ООН (UNECE) влітку 2020 року вперше прийняв два обов'язкових правила. Опубліковано під абревіатурами UNECE R 155 та UNECE R 156, правила стосуються IT-безпеки та оновлення програмного забезпечення в транспортних засобах, і, таким чином, тісно пов'язані між собою.

Положення набули чинності на початку 2021 року. З липня 2022 року їх дотримання стане обов'язковим для нових типів транспортних засобів. Виробники, які не відповідають вимогам, зіткнуться з не реєстрацією відповідних типів транспортних засобів. Нарешті, з липня 2024 року правила будуть застосовуватися до всіх нових транспортних засобів. Регламенти, вимагають впровадження заходів у чотирьох сферах:

- Управління кіберризиками для транспортних засобів
- Захист транспортних засобів відповідно до підходу безпеки за проектом для зменшення ризиків у ланцюжку створення вартості
- Виявлення та захист від атак у всьому автопарку
- Надання оновлень програмного забезпечення з точки зору безпеки та запровадження правової основи для ефірних оновлень (O.T.A. over-the-air updates) програмного забезпечення транспортних засобів.

3 СИСТЕМИ ВИЗНАННЯ ТЕХНІЧНОГО РЕГУЛЮВАННЯ УКРАЇНИ В МЕЖАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

3.1 Складові системи сертифікації

Сертифікація кібербезпеки має досить вагоме значення для підвищення довіри до продуктів, сервісів та процесів. Цифровий єдиний ринок, економіка даних і IoT, можуть процвітати тільки в тому випадку, якщо існує загальна суспільна довіра, що такі продукти, послуги і процеси забезпечують певний рівень кібербезпеки. Під'єднані та автоматизовані автомобілі, електронні медичні прилади, системи управління промисловою автоматикою та смарт-сітки є лише деякими прикладами секторів, в яких сертифікація вже широко використовується або, ймовірно, буде використовуватися найближчим часом. Сектори, які регулюються Директивою (ЄС) 2016/1148, також є секторами, в яких сертифікація кібербезпеки є критично важливою.

В даний час сертифікація кібербезпеки продуктів, сервісів і процесів використовується тільки в обмеженій мірі. Здебільшого вона функціонує на рівні держав-членів або в рамках промислових схем, що керуються галуззю. У цьому контексті, сертифікат, що видається національним органом з сертифікації кібербезпеки, не може бути визнаним в інших державах-членах. Таким чином, компанії можуть сертифікувати свої продукти, послуги та процеси в декількох державах-членах, де вони реалізуються, наприклад, з метою участі в національних процедурах закупівель, що тим самим збільшує їх витрати. Більше того, з появою нових схем, стає все більш помітною відсутність ,узгодженого і цілісного підходу до питань кібербезпеки, наприклад, в області IOT. Існуючі схеми представляють значні недоліки і відмінності в плані покриття варіації продукції, рівнях надійності, предметних критеріях і актуальному використанні, перешкоджаючи механізмам взаємного визнання всередині Союзу.

В результаті було докладено певних зусиль для забезпечення взаємного признання сертифікатів всередині ЄС. Проте ці зусилля були не повністю успішними. Найбільш важливим прикладом у зв'язку з цим є «Угода про взаємне визнання» (MRA) Групи вищих посадових осіб з безпеки інформаційних систем (SOG-IS). Хоча документ і представляє найважливішу модель співпраці і взаємне визнання в області сертифікації безпеки, SOG-Є визнається тільки деякими державами-членами. Цей факт обмежив ефективність SOG-IS MRA з точки зору внутрішнього ринку.

Тому необхідно прийняти спільний підхід і встановити європейську систему сертифікації кібербезпеки, яка закладає основні горизонтальні вимоги до європейських схем сертифікації кібербезпеки, які повинні бути розроблені і дозволяють європейським сертифікатам кібербезпеки та заявам ЄС про відповідність продукції ІСТ, Послуги або процеси кібербезпеки підключених автомобілів, які повинні бути визнані і використані в усіх державах-членах. При цьому необхідно будувати на існуючих національних і міжнародних схемах, а також на системах взаємного розпізнавання, зокрема SOG-IS, і зробити можливим поступовий перехід до схем за новою європейською системою сертифікації кібербезпеки. Європейська система сертифікації кібербезпеки повинна мати подвійне призначення. По-перше, це має допомогти підвищити довіру до продуктів, послуг та процесів кібербезпеки підключених автомобілів, які були сертифіковані за європейськими схемами сертифікації кібербезпеки. По-друге, це повинно допомогти уникнути множення суперечливих або перекритих національних схем сертифікації кібербезпеки і, таким чином, зменшити витрати на заходи, що працюють на цифровому єдиному ринку. Європейські схеми сертифікації кібербезпеки мають бути недискримінаційними і базуватися на європейських або міжнародних стандартах, в тому випадку якщо вони не являються неефективними або невідповідними для досягнення цілей Союзу в цьому відношенні.

Європейська система сертифікації з галузі кібербезпеки повинна бути створена на однаковій основі у всіх державах-членах, щоб не допустити такого явища як «торгівля сертифікатів» у різних державах-членах на різних рівнях суворості.

Європейські системи сертифікації кібербезпеки повинні ґрунтуватися на тому, що на вже на даний момент функціонує на міжнародному та національному рівнях, (і в окремих випадках на технічних специфікаціях форумів та консорціумів), перейняти на себе приклади з використання сильних сторін та виправляючи недоліки.

Необхідні гнучкі рішення в галузі кібербезпеки, щоб промисловість могла дати відсіч кіберзагрозам, і тому будь-яка система сертифікації повинна розроблятися таким чином, щоб уникнути ризик швидкого старіння та втраті її актуальності.

Комісія має бути наділена уповноваженнями приймати європейські схеми сертифікації кібербезпеки щодо відповідних угрупувань послуг, продуктів та процесів кібербезпеки підключених транспортних засобів. Ці системи повинні впроваджуватися та контролюватись національними сертифікаційними органами з питань кібербезпеки, а сертифікати, що видаються відповідно до цих схеми, мають бути дійсними та визнаватись на всій території Союзу. Якщо вже є схеми сертифікації, які використовуються галуззю або приватними організаціями, то вони не повинні підпадати під дію цих Правил. Однак органи, які здійснюють такі схеми, повинні мати можливість пропонувати Комісії розглядати такі схеми як основу для їх затвердження як європейської схеми сертифікації кібербезпеки.

Мета європейських схем сертифікації кібербезпеки повинна полягати у забезпеченні того, щоб продукти, послуги та процеси кібербезпеки підключених транспортних засобів, сертифіковані відповідно до вище описаних схем, підходили конкретним вимогам, спрямованих на захист їхньої автентичність, доступності, цілісності і конфіденційність переданих, збережених або оброблених

даних або відповідних функцій та послуг, які пропонуються або доступні через ці продукти, послуг та процеси пов’язані з кібербезпекою транспортних засобів упродовж усього їх життєвого циклу.

Відповідно до цього регламенту неможливо повністю окреслити вимоги кібербезпеки, що стосуються всіх продуктів, послуг та процесів пов’язані з кібербезпекою транспортних засобів. Продукти, послуги та процеси пов’язані з кібербезпекою транспортних засобів, а також потреби в галузі кібербезпеки, пов'язані з цими продуктами, послугами та процесами, мають дуже широкий спектр застосування, через що доволі важко підготувати загальні вимоги в галузі кібербезпеки, які були б дійсними за різних обставин. Виходячи з цього потрібно прийняти загальне поняття кібербезпеки для цілей сертифікації, яке має доповнюватися рядом конкретних цілей у галузі кібербезпеки, які повинні враховуватися під час розробки європейських систем сертифікації кібербезпеки. Механізми досягнення таких цілей у конкретних продуктах, послугах та процесах пов’язані з кібербезпекою транспортних засобів повинні бути більш детально визначені на рівні індивідуальної системи сертифікації, прийнятої Комісією; наприклад, шляхом посилання на стандарти або технічні специфікації, у випадку відсутності відповідних стандартів.

Технічні специфікації, що підлягають використанню в європейських схемах сертифікації кібербезпеки, мають відповідати вимогам, про які йдеться у II додатку до Регламенту № 1025/2012 Європейського Парламенту та Ради [31]. Разом з тим, деякі відхилення від цих вимог можуть вважатися необхідними в належним чином обґрунтованих випадках, коли ці технічні характеристики повинні використовуватися в європейській системі сертифікації кібербезпеки з посиланням на «високий» рівень надійності. Причини таких відхилень повинні оприлюднюватися.

Вибір відповідної сертифікації та відповідних вимог безпеки користувачами європейських сертифікатів кібербезпеки має ґрунтуватися на вивченні ризиків, що

пов'язані з експлуатацією продуктів, послуг чи процесів пов’язані з кібербезпекою транспортних засобів. Виходячи з цього, рівень гарантії повинен бути порівнянний з рівнем ризику, пов'язаного з передбачуваним використанням продукту, послуг або процесу пов’язані з кібербезпекою транспортних засобів.

Кібербезпека підключених автомобілів на сьогоднішній день є вагомою проблемою для належної діяльності та безпеки і державного управління в найближчий час [32, 33].

Вагоме значення у сфері кібербезпеки підключених автомобілів відіграє оцінка відповідності (сертифікація)[34].

Схему сертифікації встановлюють процедури, правила та менеджмент проведення сертифікації кібербезпеки, в той час як система сертифікації складається із набору правил та процедур для керування схожими або близькими схемами оцінки відповідності [35].

На сьогоднішній день перед Україною постає важлива та актуальна задача в вигляді розробки схем та системи сертифікації для інтернету речей базуючись на існуючій в країні системі технічного регулювання та здобутків у сфері оцінки відповідності, акредитації [36], та вимог чинного законодавства України з питань кібербезпеки, яке ставить перед собою завдання застосувати найкращі міжнародні та європейські принципи оцінки відповідності кібербезпеки [32].

Оцінка відповідності – це докази того, що «зазначені вимоги» , які відносяться до продукції, процесу, послуги, системи, особи чи органу, були реалізовані (оцінка відповідності охоплює наступні види діяльності: випробування, інспектування, валідація, верифікація, сертифікація та акредитація). Під зазначеною вимогою мають на увазі необхідність або зазначене сподівання та їх можна взяти з нормативних документів, наприклад, регламентів, стандартів та технічних специфікацій. Об'єкт є об'єктом оцінки відповідності, якщо до нього застосовуються «зазначені вимоги». Схема оцінки відповідності – це перелік правил та процедур, які описують об’єкти оцінки відповідності,

визначають ці вимоги та забезпечують методики проведення оцінки відповідності. В рамках системи оцінки відповідності можна керувати схемою з оцінки відповідності.

Система оцінки відповідності – перелік правил та процедур для управління схожими або близькими схемами оцінки відповідності. Оцінка відповідності визначеним вимогам незацікавленою третьою стороною, що є органом з оцінки відповідності (ООВ), називається сертифікацією [35].

Тільки за останні десять років по всьому світу було створено купу систем та оціночних стандартів, що використовуються для сертифікації інформаційної та кібербезпеки. Найвідоміші з них: стандарти сімейства ISO/IEC 17000; стандарт ISO/SAE 21434 та інші.

Прикладне використання зазначених систем та стандартів сертифікації зустрічається переважно в промислових схемах сертифікації. Така багатогранність утворює вагомі технічні перешкоди у широкому чи транскордонному визнанні відповідних оцінок (сертифікатів). Більше того, значний ризик може становити й сама наявність або експлуатація різних вимог і процедур у таких секторах, які функціонують як глобальні та складні системи.

Для того щоб усунути технічні бар’єри на шляху визнання оцінки відповідності та сертифікатів, створено глобальну систему оцінки відповідності, яка формує перелік умов для всебічного визнання оцінок відповідності та сертифікатів.

Описана вище система є акредитацією органів з оцінки відповідності (ООВ), у склад яких входять й органи з сертифікації [37].

3.2 Європейська асоціація з питань кібербезпеки (ЕА)

Система сертифікації кібербезпеки ЄС для продуктів кібербезпеки підключених транспортних засобів дозволяє створювати індивідуальні та засновані на ризиках схеми сертифікації ЄС.

Сертифікація відіграє вирішальну роль у підвищенні довіри та безпеки важливих продуктів і послуг для цифрового світу. На даний момент в ЄС існує низка різних схем сертифікації безпеки для продуктів кібербезпеки підключених транспортних засобів. Але без загальної основи для дійсних сертифікатів кібербезпеки в ЄС зростає ризик фрагментації та бар'єрів між державами-членами.

Система сертифікації забезпечить загальноєвропейські схеми сертифікації як повний набір правил, технічних вимог, стандартів і процедур. Структура базуватиметься на домовленості на рівні ЄС щодо оцінки властивостей безпеки конкретного продукту або послуги на основі кібербезпеки підключених транспортних засобів. Він засвідчуватиме, що продукти та послуги кібербезпеки підключених транспортних засобів, які були сертифіковані відповідно до такої схеми, відповідають визначеним вимогам.

Зокрема, кожна європейська схема повинна визначати:

- категорії продуктів і послуг, що охоплюються;
- вимоги кібербезпеки, такі як стандарти або технічні характеристики;
- тип оцінювання, наприклад, самооцінка або оцінка третьою стороною;
- передбачуваний рівень гарантії.

Рівні надійності використовуються для інформування користувачів про ризики кібербезпеки продукту та можуть бути базовими, значними та/або високими. Вони співрозмірні з рівнем ризику, пов'язаного з передбачуваним використанням продукту, послуги або процесу, з точки зору ймовірності та впливу

аварії. Високий рівень гарантії означатиме, що сертифікований продукт пройшов найвищі тести безпеки.

Отриманий сертифікат буде визнано в усіх державах-членах ЄС, що полегшить бізнесам транскордонну торгівлю, а покупцям – зрозуміти функції безпеки продукту чи послуги.

Що стосується впровадження системи сертифікації, органи держав-членів, об'єднані в Європейську групу сертифікації кібербезпеки (ECCG), вже кілька разів зустрічалися.

Після набуття чинності Закону про кібербезпеку в 2019 році Європейська комісія оголосила конкурс для відбору членів Групи сертифікації кібербезпеки зацікавлених сторін (SCCG).

SCCG відповідатиме за консультування Комісії та ENISA щодо стратегічних питань щодо сертифікації кібербезпеки та допомогу Комісії в підготовці поточної робочої програми Союзу. Це перша експертна група зацікавлених сторін із сертифікації кібербезпеки, започаткована Європейською Комісією.

У організації технічного регулювання організація, що несе відповідальність за акредитацію, має оцінювати компетенцію органів з сертифікації продукції, послуг та процесів, інспектування й персоналу, систем менеджменту, випробувальних й калібрувальних лабораторій. Акредитація носить в собі офіційне визнання, що завіряє клієнтів і користувачів послуг про компетентну функціональність зазначених організацій. Акредитація забезпечує транскордонне визнання її послуг в контексті Міжнародного форуму з акредитації (IAF) і Міжнародного комітету з акредитації лабораторій (ILAC) [38,39].

IAF і ILAC допомагають та керують визнанням Двосторонніх або Багатосторонніх Угод або Домовленостей (MRA/MLA), відповідно до яких члени, які беруть участь в них, зобов'язуються взаємно признавати результати тестування, інспекцій, сертифікації або акредитації. Угоди MRA/MLA на сьогодні є вагомим чинником до оптимізації чи зменшення числа сертифікацій продуктів,

послуг, систем, процесів і матеріалів, потрібних зокрема в міжнародній діяльності [38,39]. На рисунку 3.1 представлено рівні та сфери, за якими в глобальній системі IAF визнано національний орган акредитації України.

Рисунок 3.1 - Угода MRA та сфера в IAF

Описані вище системи IAF/ILAC здійснюють свою діяльність через регіональні організації з акредитації (вони в свою чергу також є частинами цих систем). На рисунки 3.2 та 3.3 зображена географічна локація цих організацій.

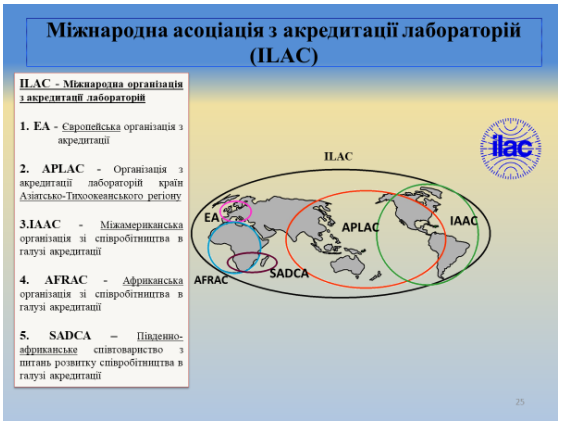

Рисунок 3.2 – Регіональні організації ILAC

Рисунок 3.3 – Регіональні організації IAF

Регіональною організацією з акредитації для України є ЕА - Європейська організація з акредитації [40].

На сьогоднішній день дуже актуальним та пріоритетним завданням є розробка схем сертифікації кібербезпеки. Глобальною проблемою є те, що існуючі системи та стандарти оцінки, що можна застосувати до сертифікації кібербезпеки, не передбачають обопільного визнання результатів випробувань, процедур (включаючи оцінки випробувальними лабораторіями), а також готовності до погоджених і порівнянних процедур оцінки і впровадження заходів для досягнення кібербезпеки. Задля досягнення цієї мети чинне законодавство України у сфері кібербезпеки поставило перед собою завдання у використанні найуспішніших європейських та міжнародних принципів ОВ інформації та кібербезпеці, для чого є необхідним відповідне науково-методичне забезпечення.

Для регуляції питань кібербезпеки України застосовується ряд правових актів[35, 41]. В цих питаннях найбільше приділяється увага на реалізацію Національної системи кібербезпеки України та відтворення в ній принципів ОВ інших держав, а також відповідно до міжнародних стандартів НАТО та ЄС гармонізувати нормативні документи у сфері кібербезпеки та запровадити найкращі світові практики та стандарти. Нажаль, повною мірою це питання є

невирішеним не тільки в Україні, а й на більш глобальному рівні (про це йдеться в доповіді ООН [42]).

ENISA виконує завдання, покладені на неї цим Регламентом, з метою досягнення високого загального рівня кібербезпеки в усьому Союзі, в тому числі шляхом активної підтримки держав-членів, установ, органів, офісів та установ Союзу в покращенні кібербезпеки. ENISA діятиме як орієнтир для консультацій та досвіду з питань кібербезпеки для установ, органів, офісів та установ Союзу, а також для інших відповідних зацікавлених сторін Союзу.

ENISA повинна сприяти зменшенню фрагментації внутрішнього ринку, виконуючи завдання, покладені на неї цим Регламентом.

2. ENISA виконуватиме завдання, покладені на неї правовими актами Союзу, які встановлюють заходи щодо наближення законів, підзаконних та адміністративних положень держав-членів, що стосуються кібербезпеки.

3. Виконуючи свої завдання, ENISA діятиме незалежно, уникаючи дублювання діяльності держав-членів та беручи до уваги наявний досвід держав-членів.

4. ENISA повинна розвивати власні ресурси, включаючи технічні та людські можливості та навички, необхідні для виконання завдань, покладених на неї цим Регламентом.

5. ENISA є центром експертизи з питань кібербезпеки завдяки своїй незалежності, науковій та технічній якості наданих порад та допомоги, інформації, яку вона надає, прозорості своїх операційних процедур, методів роботи та старанності у виконанні своїх завдань.

6. ENISA допомагає установам, органам, установам та установам Союзу, а також державам-членам у розробці та реалізації політики Союзу, пов'язаної з кібербезпекою, включаючи галузеву політику щодо кібербезпеки.

7. ENISA підтримуватиме розбудову потенціалу та готовність по всьому Союзу, допомагаючи установам, органам, офісам та установам Союзу, а також

державам-членам та державним та приватним зацікавленим сторонам підвищити захист своєї мережі та інформаційних систем, розвивати покращити стійкість та здатність реагувати на кіберпрограму та розвивати навички та компетенції у галузі кібербезпеки.

8. ENISA повинна сприяти співпраці, включаючи обмін інформацією та координацію на рівні Союзу, між державами-членами, установами, органами, установами та агенціями Союзу та відповідними приватними та державними зацікавленими сторонами з питань, пов'язаних з кібербезпекою.

9. ENISA сприятиме збільшенню можливостей кібербезпеки на рівні Союзу з метою підтримки дій держав-членів щодо запобігання та реагування на кіберзагрози, зокрема у випадку транскордонних інцидентів.

10. ENISA сприятиме використанню європейської сертифікації з кібербезпеки з метою уникнення фрагментації внутрішнього ринку. ENISA сприятиме створенню та підтримці європейської системи сертифікації кібербезпеки відповідно до Розділу III цього Регламенту з метою підвищення прозорості кібербезпеки продуктів, послуг та процесів кібербезпеки підключених транспортних засобів, тим самим зміцнюючи довіру до цифрового внутрішнього ринок та його конкурентоспроможність.

11. ENISA повинна сприяти високому рівню обізнаності в галузі кібербезпеки, включаючи кібергігієну та кіберграмотність серед громадян, організацій та бізнесу.

ENISA повинна мати можливість відповідати на спеціальні запити держав членів та установ, органів, управлінь та установ Союзу щодо питань, що належать до повноважень ENISA. Розумно та рекомендується впроваджувати певні принципи щодо управління ENISA з метою дотримання Спільної заяви та Спільного підходу, узгоджених у липні 2012 року Міжвідомчою робочою групою з питань децентралізованих установ ЄС, метою якої є впорядкування діяльність децентралізованих агентств та покращення їх роботи. Рекомендації у Спільній

заяві та Спільному підході також повинні бути відображені, у відповідних випадках, у робочих програмах ENISA, оцінках ENISA та звітній та адміністративній практиці ENISA. Для ефективної діяльності ENISA чималу роль відіграє те, наскільки грамотно організована її структура – чи немає непотрібних елементів або, навпаки, можливо якійсь частині агентству не вистачає? Тому, в цій роботі аналізується структура ENISA, яка показана на рисунку 3.4.

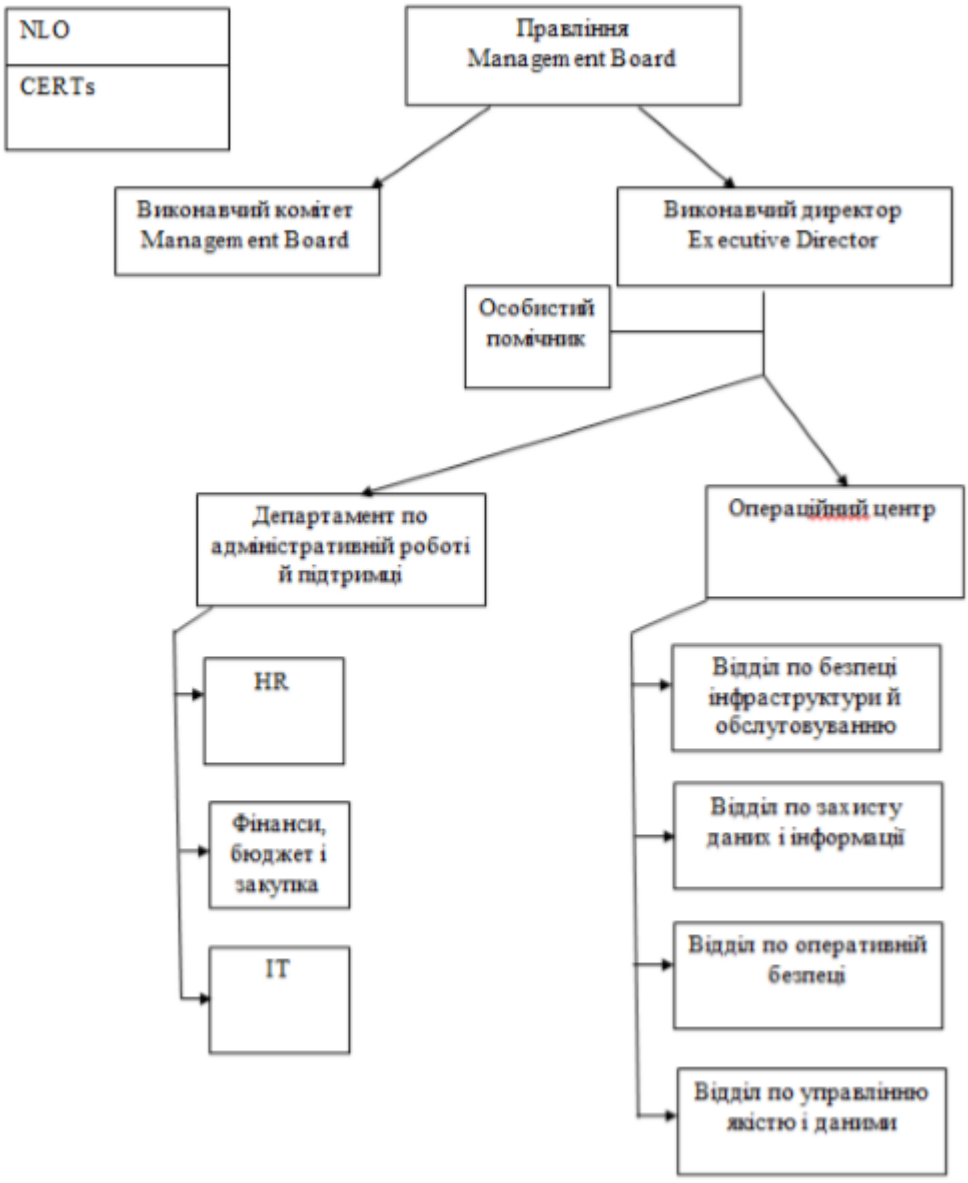

Рисунок 3.4 – Структура ENISA

Правління, до складу якого входять представники держав-членів та Комісії, повинно встановити загальний напрямок діяльності ENISA та забезпечити виконання своїх завдань відповідно до Регламенту (ЄС) 2019/881

Виходячи з описаного вище, можна зробити висновок про те, шо сертифікація зі кібербезпеки підключеного автомобіля має вміщувати набір правил і процедур для опису об’єктів сертифікації, визначати ці вимоги та забезпечувати методологію проведення сертифікації.

Система сертифікації кібербезпеки інформаційно-комунікаційних технологій включає в себе:

1. Міжнародні стандарти та системи, що використовуються для сертифікації кібербезпеки підключених автомобілів. За останні роки по всьому світу було створено купу оціночних стандартів та систем, що використовуються для сертифікації інформаційної та кібербезпеки. Найвідоміші з них: стандарти сімейства ISO/IEC 17000; та інші. Практичне застосування – названі системи та стандарти сертифікації знаходять здебільшого в галузевих схемах сертифікації, рідше в національних схемах. Така різноманітність утворює потужні технічні бар’єри у підтвердженні відповідних сертифікатів. У більшості випадків існування або використання різних вимог і процедур у тих секторах, які функціонують як глобальні і комплексні сфери, може являти собою підвищений ризик.

Описані вище стандарти та сертифікації можуть знайти прикладне застосування в промислових, а іноді і в національних схемах сертифікації. Виходячи з такої різноманітності стандартів, створюється потужний технічний бар'єр для того, щоб визнати відповідні оцінки (сертифікати). Більше того, можуть бути значні ризики при існуванні або використанні процедур та вимог в секторах, що функціонують як глобальні і інтегровані області.

2. Акредитація органів з оцінки відповідності. В наслідок такого процесу як акредитація, авторитетним органом надається формальне визнання компетентності організації або приватної у виконанні відповідних завдань.

У організації технічного регулювання організація, що несе відповідальність за акредитацію, має оцінювати компетенцію органів з сертифікації продукції, послуг та процесів, інспектування й персоналу, систем менеджменту, випробувальних й калібрувальних лабораторій. Акредитація носить в собі офіційне визнання, що завіряє клієнтів і користувачів послуг про компетентну функціональність зазначених організацій.

3. Система сертифікації кібербезпеки підключених автомобілів в Україні. Перш за все для сертифікації кібербезпеки підключеного автомобіля для національної системи кібербезпеки України, необхідно створити систему оцінки відповідності кібербезпеки підключеного автомобіля.

В залежності від ризику для громадян та суспільства, умов сертифікації у кіберпросторі та відношення до різних інформаційно-комунікаційних технологій, системи ОВ для сертифікації кібербезпеки України можуть застосовуватися різними методами.

Схему сертифікації необхідно реалізувати зі зважанням до всіх належних умов та факторів. Для сертифікації кібербезпеки України, необхідно виділити наступні фактори:

- Підписання Договору про визнання акредитації органів сертифікації;
- Необхідність дотримання вимог Угоди ЄС-Україна та статті 56 цієї Угоди;
- Наявність в ЄС Регламенту 2019/881 про сертифікацію кібербезпеки, головні принципи якого будуть впроваджені в Національну систему кібербезпеки України.

Для реалізації ефективної та гнучкої системи сертифікації кібербезпеки України, яка в майбутньому буде складатись з серії схем сертифікації кібербезпеки для дієвої відповіді на виклики кібербезпеки, необхідно провести систематизацію двох основних елементів системи:

– Вимог до оцінки (наприклад посилання нормативні інструменти або

стандарти);

– Механізми взаємного визнання сертифікатів (Угода про визнання).

Це можна реалізувати шляхом впровадження уніфікованих моделей на основі глобальних механізмів з усуненням технічних бар'єрів у сфері торгівлі та поточному стану технічної регуляторної системи України:

– Ієрархічна модель оцінки стандартів системи сертифікації кібербезпеки;

– Ієрархічна модель Угод взаємного визнання сертифікатів кібербезпеки.

Ієрархічна модель оцінки стандартів системи сертифікації кібербезпеки зображена на рисунку 3.5.

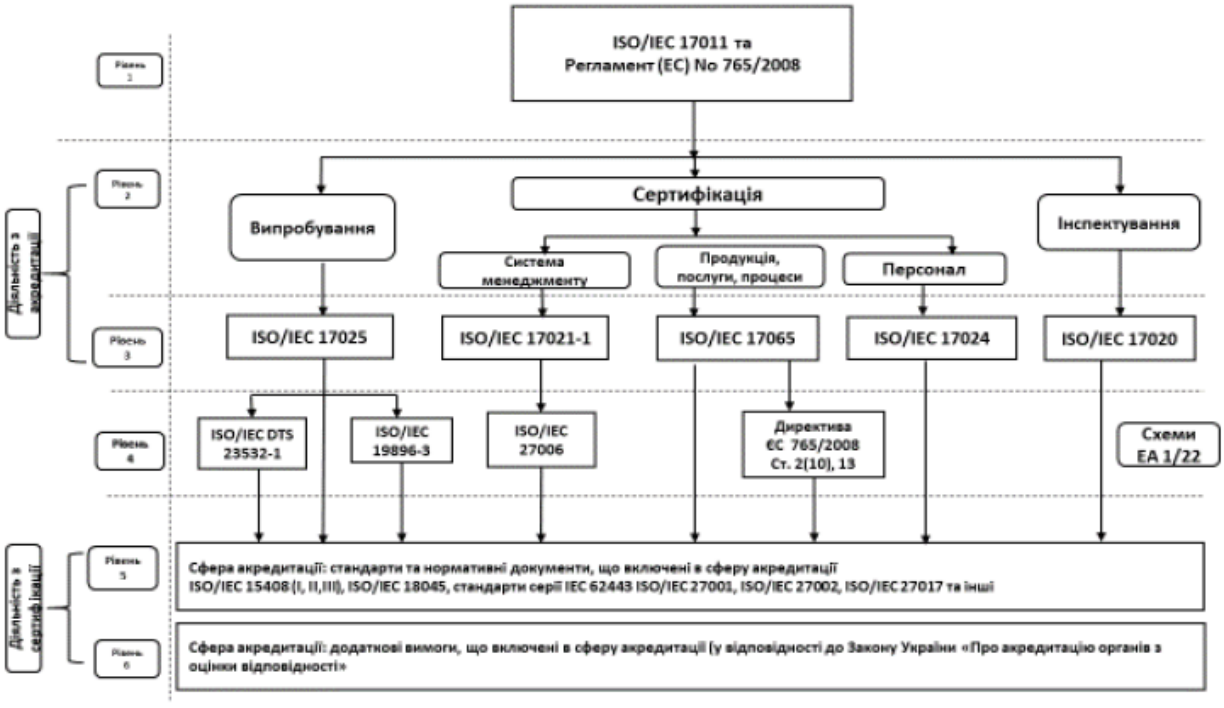

Рисунок 3.5 – Ієрархічна модель оціночних стандартів Системи сертифікації кібербезпеки

Дана модель дає дозвіл на регулювання визначень і застосувань стандартів або інших нормативних інструментів, схем і стандартів, з різними можливими поєднаннями для розробки схем сертифікації.

Для опису моделі можна використати 6 рівнів:

- 1 рівень демонструє умови органів з акредитації, за якими можна акредитувати органи, що відносяться до сертифікації кібербезпеки. Прописані у стандарті ISO/IEC 17011, в Регламенті (ЄС) 765/2008 і в окремих випадках вимоги, що визначаються в обов'язкових документах ЕА та в документах IAF та/або ILAC
- 2 рівень базується на діяльності з оцінки відповідності ООВ, якою органи з акредитації акредитують у відповідності зі стандартами, які відносяться до 3 рівня.
- 3 рівень включає в себе гармонізовані стандарти та деякі нормативні документи, в яких містяться загальні вимоги до ООВ, які мають виконувати діяльність з оцінки відповідності кібербезпеки, віднесених до другого рівня. Це наступні оціночні стандарти: ISO/IEC 17025; ISO/IEC 17020; ISO/IEC 17065; ISO/IEC 17021-1; ISO/IEC 17024.
- На 4 рівні містяться документи, в яких описуються додаткові критерії та умови до 3-го рівня. Цей рівень застосовується в тому випадку, коли існують доповняльні документи до 3-го рівня стандартів (тому 5 рівень часто пов’язаний зі стандартами 3-го рівня). Прикладами таких документів для ЄС можуть бути галузеві стандарти та нормативні документи; галузеві схеми, як зазначено у Регламенті (ЄС) 765/2008 Статті 2 [43] та 13; схеми оцінки відповідності згідно з ЕА-1/22 (далі – схеми).
- 5 рівень є сферою акредитації органу з сертифікації: стандарти та інші нормативні документи, які використовують акредитованими ООВ для конкретної акредитованої сфери оцінки відповідності. Можуть включатися відповідні способи випробувань та відповідні ультиматуми до системи управління (такі як:

ISO/IEC 27001), критерії кібербезпеки (ISO/IEC 15408), методику оцінки кібербезпеки (ISO/IEC 18045) тощо.

6 рівень представляє собою сферу акредитації органу з сертифікації: додаткові вимоги до сфери акредитації, що можуть бути утвердженими в державі. Визначені в законі України «Про акредитацію органів з оцінки відповідності», стаття 1 [37].

3.3 Висновки до розділу 3

Метою системи сертифікації кібербезпеки ЄС відповідно до Регламенту (ЄС) 2019/881 є встановлення та підтримка довіри та безпеки до продуктів, послуг та процесів кібербезпеки. Складання схем сертифікації кібербезпеки на рівні ЄС має на меті надати критерії для проведення оцінки відповідності, щоб встановити ступінь відповідності продукції, послуг та процесів конкретним вимогам. Користувачі та постачальники послуг повинні мати можливість визначати рівень забезпечення безпеки продуктів, послуг та процесів, які вони закуповують, роблять доступними чи використовують. Було розглянуто існуючі системи сертифікації Європейського союзу та їх складові, а також визначено ряд вимог для можливості розробки подальших рекомендацій.

4 РОЗРОБЛЕННЯ ПРОПОЗИЦІЙ РЕГУЛЮВАННЯ ЩОДО НАГАЛЬНИХ ПИТАНЬ КІБЕРБЕЗПЕКИ ПІДКЛЮЧЕНОГО АВТОМОБІЛЯ

Для формування системи сертифікації необхідно включити 7 компонентів:

1.Критерії для оцінювання (прикладом може бути стандарт або нормативний документ).

Якщо оцінка була проведена з застосуванням необхідних схем сертифікації та була успішною, то можна надавати сертифікат з кібербезпеки. Сертифікація може бути проводена акредитованим відповідно до стандарту ISO/IEC 17065 органом при умові залучення акредитованої відповідно до стандарту ISO/IEC 17025 лабораторії. Далі може бути виданий сертифікат державним чи приватним органом, якщо рівень гарантії це дозволяє.

2. Акредитація органів з оцінки відповідності .

Після прийняття схеми сертифікації кібербезпеки продуценти або дилери продуктів, послуг та процесів пов’язаних з кібербезпекою підключеного авто матимуть змогу подавати заявки для сертифікації своєї продукції щодо кібербезпеки підключеного автомобіля до органу з оцінки відповідності, який в свою чергу має бути акредитованим національним органом з акредитації. Відповідно до виконання органом з оцінки відповідності умов, національний орган з акредитації має право обмежувати, призупиняти або відкликати акредитацію.

3.Механізм угоди про визнання.

Відповідно до Регламенту ЄС №2019/881, система сертифікації кібербезпеки України може укласти Угоду про взаємне визнання результатів ОВ. Це необхідно насамперед для визнання ланцюжка постачання глобальним. В такому випадку для системи сертифікації кожна схема буде передбачати певні критерії для угод взаємного визнання з країнами третього світу

4. Керування системою сертифікації кібербезпеки.

Керування системою сертифікації бере до уваги залучення зацікавлених сторін та визначає роль органу управління при плануванні та пропонуванні та іншої роботи зі схемами сертифікації кібербезпеки. Регулятор (національний орган влади) створює орган управління системою сертифікації, який має створити Робочу програму задля створення і в деяких випадках адаптацію можливих схем сертифікації.

5. Рівень гарантії сертифікатів кібербезпеки.

Для схеми сертифікації кібербезпеки має бути можливість визначати рівень гарантії сертифікату (наприклад *базовий*, *суттєвий* або *високий*) та декларацій (тільки базовий рівень) про відповідність, що видаються відповідно схеми. Це необхідно для забезпечення узгодженості системи сертифікації кібербезпеки.

6. Національні органи з сертифікації.

Національний орган є доцільним для гармонізації з Регламентом ЄС. Він потрібен для контролю дотримання взятих на себе зобов’язань, що описуються у системі сертифікації та для сприянням з моніторингу національним органам з акредитації. Але ця складова не є обов’язковим елементом для системи сертифікації.

7. Призначення органів з сертифікації кібербезпеки.

Вимоги до призначених органів з сертифікації кібербезпеки мають бути належними до закону України «Про технічні регламенти та оцінку відповідності».

4.1 Створення органів сертифікації кібербезпеки підключеного автомобіля чи розширення сфери в існуючих органах сертифікації

Національні органи з сертифікації кібербезпеки

- повинні, зокрема, контролювати та виконувати зобов'язання виробників або постачальників продуктів, послуг чи процесів кібербезпеки

підлюченого автомобіля, створених на його відповідній території, щодо декларації про відповідність ЄС,

- повинні допомагати національним органам з акредитації у моніторингу та нагляді діяльності органів з оцінки відповідності, надаючи їм досвід та відповідну інформацію,
- повинен уповноважувати органи з оцінки відповідності виконувати свої завдання, якщо такі органи відповідають додатковим вимогам, встановленим європейською схемою сертифікації кібербезпеки,
- та слідкувати за відповідним розвитком у галузі сертифікація кібербезпеки.

Національні органи з сертифікації кібербезпеки

- повинні також розглядати скарги, подані фізичними або юридичними особами стосовно європейських сертифікатів кібербезпеки, виданих цими органами влади, або стосовно європейських сертифікатів кібербезпеки, виданих органами з оцінки відповідності, якщо такі сертифікати свідчать про рівень впевненості `` високий ",
- слід проводити розслідування, наскільки це можливо, предмет скарги
- і повинен інформувати скаржника про хід та результати розслідування протягом розумного періоду.

Більше того, національні органи з сертифікації кібербезпеки

- повинні співпрацювати з іншими національними органами з сертифікації кібербезпеки або іншими державними органами, в тому числі шляхом обміну інформацією про можливу невідповідність продуктів кіберпезпеки підключеного автомобіля, послуг та процесів вимогам цього Регламенту або конкретним європейським схеми сертифікації кібербезпеки.

Комісія повинна сприяти такому обміну інформацією, надаючи загальну електронну систему інформаційної підтримки, наприклад, Інформаційно-

комунікаційну систему з нагляду за ринком (ICSMS) та систему швидкого оповіщення про небезпечні непродовольчі товари (RAPEX), яка вже використовується ринком органи нагляду відповідно до Регламенту (ЄС) No 765/2008.

4.2 Акредитація органів сертифікації на сферу кібербезпеки підключеного автомобіля

Акредитація - це процедура, у ході якої національний орган з акредитації засвідчує компетентність юридичної особи чи відповідного органу з оцінки відповідності (ООВ) виконувати певні види робіт (випробування, калібрування, сертифікацію, контроль).

Акредитація надає:

- забезпечення єдиної технічної політики у сфері оцінки відповідності в країні;
- забезпечення довіри споживачів до результатів діяльності з оцінки відповідності;
- створення умов для взаємного визнання результатів діяльності акредитованих органів на міжнародному рівні;
- усунення технічних бар’єрів для бізнесу.

НААУ проводить акредитацію відповідно до Закону України “Про акредитацію органів з оцінки відповідності” з урахуванням вимог міжнародних та європейських стандартів з акредитації за основними напрямками

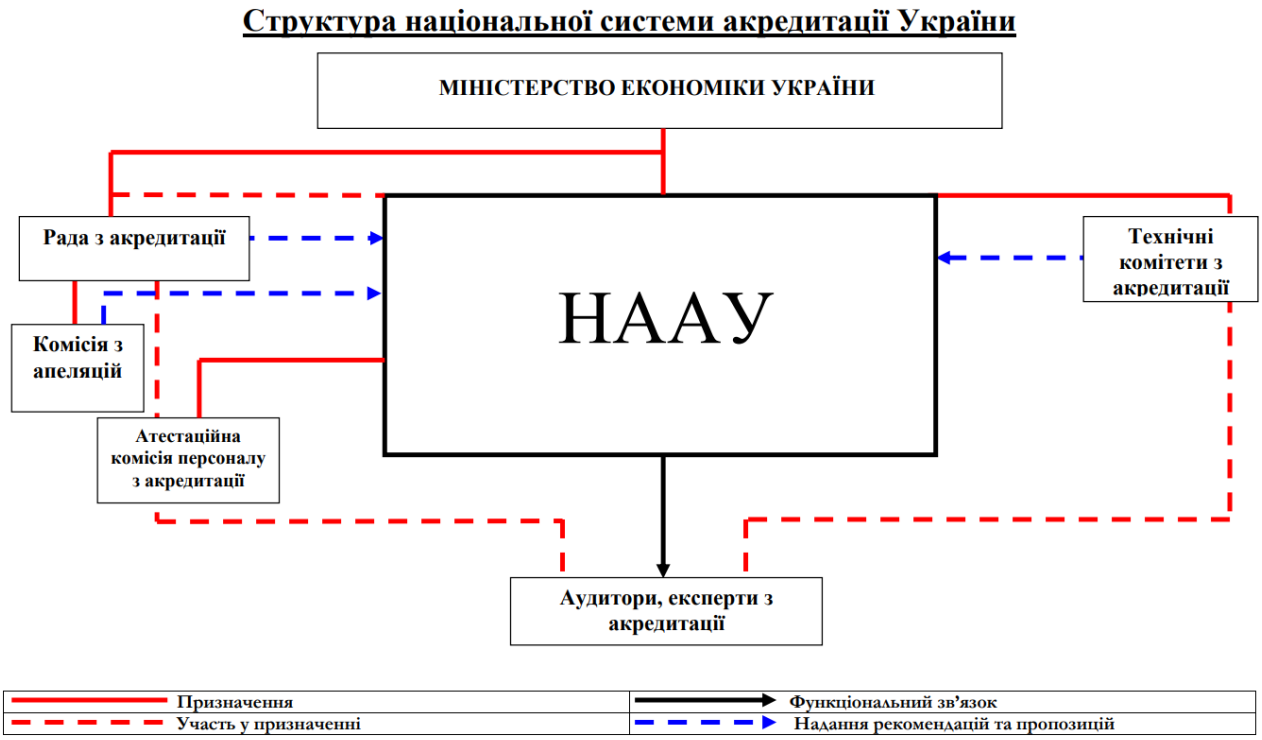

Рисунок 4.1 – Структура національної системи акредитації України

4.2.1 Призначення органів сертифікації кібербезпеки підключеного автомобіля

Призначення - урядовий дозвіл органу з оцінки відповідності на здійснення визначених заходів з оцінки відповідності.

Орган влади, що призначає - організація, створена в рамках уряду або уповноважена урядом, для призначення органів з оцінки відповідності та припинки чи скасування їх призначення.

Держава повинна призначити (designate) один або кілька національних органів з сертифікації кібербезпеки *для нагляду за дотриманням зобов'язань*, що містяться в Системі сертифікації кібербезпеки (from this Regulation).

Національним органом з сертифікації кібербезпеки може бути існуючий або новий орган.

Держава-учасник також повинна мати можливість призначити, після узгодження з іншою державою-учасником, одного або декількох національних органів з сертифікації кібербезпеки на території цієї іншої держави-учасника

4.3 Впровадження в діяльність НААУ (на всіх рівнях) можливості виконання робіт з акредитації органів сертифікації кібербезпеки підключеного автомобіля (експерти, технічний комітет, аудитори, тощо)

Орган з сертифікації кібербезпеки може застосовувати одну або більшу кількість схем сертифікації, що охоплюють його сертифікаційну діяльність. Елементи таких схем можуть бути поєднані з нагляданням за продукцією, або з оцінюванням та нагляданням за системою управління клієнта, або з обома. Загальне керівництво щодо розробки схем надається в стандарті ДСТУ EN ISO/IEC 17067:2014 Оцінка відповідності. Основні положення сертифікації продукції та керівні вказівки щодо схем сертифікації продукції (EN ISO/IEC 17067:2013, IDT) з врахуванням вимог стандартів ДСТУ ISO/IEC Guide 28:2007. Оцінювання відповідності. Настанови щодо системи сертифікації продукції третьою стороною (ISO/IEC Guide 28:2004, IDT) та ДСТУ ISO/IEC Guide 53:2008. Порядок виконання системи управління якістю організації у сертифікації продукції (ISO/IEC Guide 53:2005, IDT). [13]

Вимоги, на відповідність до яких оцінюються продукція, послуги та процеси пов’язані з кібербезпекою підключеного автомобіля клієнта, повинні бути встановлені в конкретних стандартах та інших нормативних документах. Керівництво для розробки відповідних нормативних документів міститься в стандарті ДСТУ ISO/IEC 17007:2009 Оцінювання відповідності. Настанови щодо складання нормативних документів, придатних до використання для оцінювання відповідності (ISO/IEC 17007:2009, IDT). [13]

Якщо необхідні пояснення щодо застосування документів для певної схеми сертифікації, вони мають бути сформульовані відповідними неупередженими особами або комітетами, що мають необхідну технічну компетентність, і орган з сертифікації кібербезпеки повинен надавати їх на вимогу. [13]

4.4 Отримання визнання НААУ на рівні ЄА (IAF) в сфері стандарту ISO 17065 щодо кібербезпеки підключеного автомобіля

Зазначена вище 6-рівнева Ієрархічна Модель оціночних стандартів Системи Сертифікації кібербезпеки є інструментом, що надає можливість створити гнучку схему сертифікації кібербезпеки з транскордонним визнанням результатів оцінки відповідності у сфері кібербезпеки.

Ієрархічна модель Угод про взаємне визнання сертифікатів кібербезпеки (рисунок 4.5) має описувати:

1) рівень;

2)обсяг визнання серед міжнародних акредитаційних організацій.

Ця модель складається з чотирьох рівнів: глобального, міжнародного, регіонального та національного. Між рівнями діють наступні угоди про взаємне визнання:

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

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

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

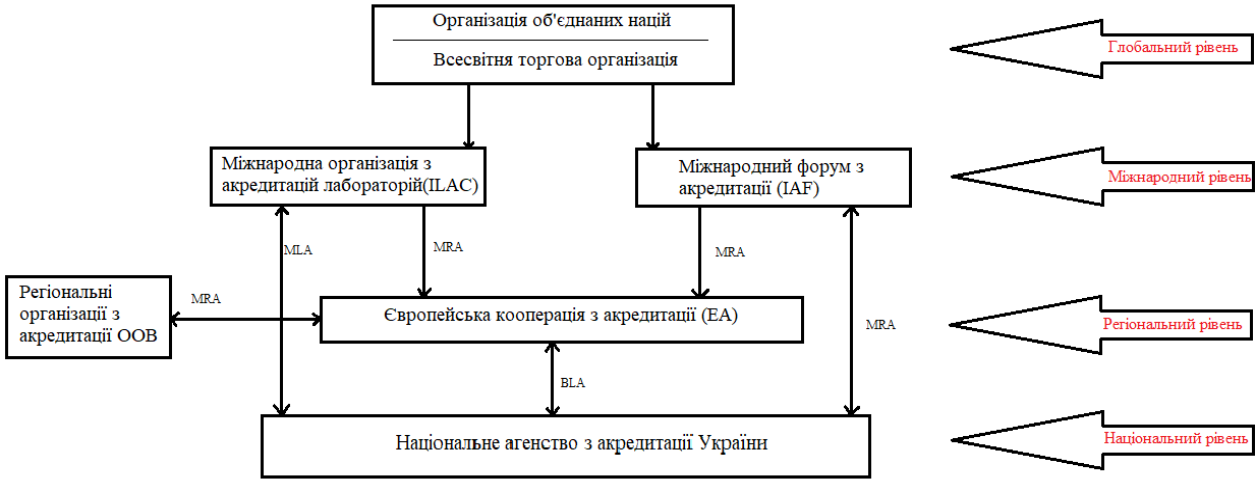

Рисунок. 4.2 – Ієрархічна модель угод щодо взаємного визнання сертифікатів кібербезпеки

Під час розробки систем та схем кібербезпеки зазначена модель допоможе сформувати зміст відповідних розділів відносно рівня гарантії сертифікатів з кібербезпеки, оціночних стандартів, акредитації ООВ, а також взаємного визнання сертифікатів.

Забезпечення мережевих та інформаційних систем в Європейському Союзі вважається ключовою метою в спробах зберегти функціонування та безпеку Інтернет-економіки ЄС; очевидно, що якщо цього не зробити, це може мати далекосяжні наслідки для європейських громадян і загрожуватиме вплинути на довіру громадян, як галузі, так і державного управління.

Оскільки роль ENISA була додатково посилена за допомогою Регламенту (ЄС) 2019/881 (Закон про кібербезпеку), важливе завдання сертифікації кібербезпеки вимагає залучення та підтримки відповідних зацікавлених сторін.

Метою системи сертифікації кібербезпеки ЄС відповідно до Регламенту (ЄС) 2019/881 є встановлення та підтримка довіри та безпеки до продуктів, послуг та процесів кібербезпеки. Складання схем сертифікації кібербезпеки на рівні ЄС має на меті надати критерії для проведення оцінки відповідності, щоб встановити ступінь відповідності продукції, послуг та процесів конкретним

вимогам. Користувачі та постачальники послуг повинні мати можливість визначати рівень забезпечення безпеки продуктів, послуг та процесів, які вони закуповують, роблять доступними чи використовують.

Сертифікація кібербезпеки вимагає офіційної оцінки продуктів, послуг та процесів незалежним та акредитованим органом на основі визначеного набору критеріїв, стандартів та видачі сертифіката, що свідчить про відповідність; оскільки така сертифікація кібербезпеки відіграє ключову роль у підвищенні довіри та безпеки до продуктів, послуг та процесів. Сертифікація кібербезпеки в ЄС служить для того, щоб надати користувачам повідомлення та запевнити у рівні відповідності заявленим вимогам. Схеми сертифікації кібербезпеки ЄС служать засобом передачі таких вимог від рівня політики ЄС до рівня надання галузевих послуг, а також до користувачів та органів оцінки відповідності.

Як встановлено в Регламенті (ЄС) 2019/881, система сертифікації кібербезпеки ЄС встановлює процедуру створення схем сертифікації кібербезпеки ЄС, що охоплює продукти, послуги та процеси кібербезпеки підключених транспортних засобів.

Кожна схема визначатиме один або кілька рівнів забезпечення (базовий, суттєвий або високий) на основі рівня ризику, пов'язаного із передбачуваним використанням продукту, послуги чи процесу.

Місія ENISA у сфері системи сертифікації кібербезпеки ЄС викладена наступним чином: «Проактивний внесок у формуються основи ЄС для кібербезпеки підключених транспортних засобів -сертифікації продуктів та послуг та проведення розробки схем сертифікації відповідно до Закон про кібербезпеку та додаткові послуги та завдання ”.

Протягом усього свого життя ENISA отримувала належне визнання за свої результати. Переходячи до ролі, яка додає більше значення політиці ЄС щодо мережевої та інформаційної безпеки, ENISA була виділена як відповідна

організація, яка виконає обіцянку скласти схеми сертифікації кандидатів у рамках сертифікації кібербезпеки ЄС. ENISA, зі своєю ключовою роллю як агентства, що займається державними службами, а також галузевими та стандартизаційними організаціями, забезпечує надійний орієнтир для розробки схем сертифікації кібербезпеки. Очікуваний результат ENISA включає проекти та доопрацьовані схеми кандидатів для сертифікації продуктів та послуг кібербезпеки підключених транспортних засобів у значенні Закону про кібербезпеку.

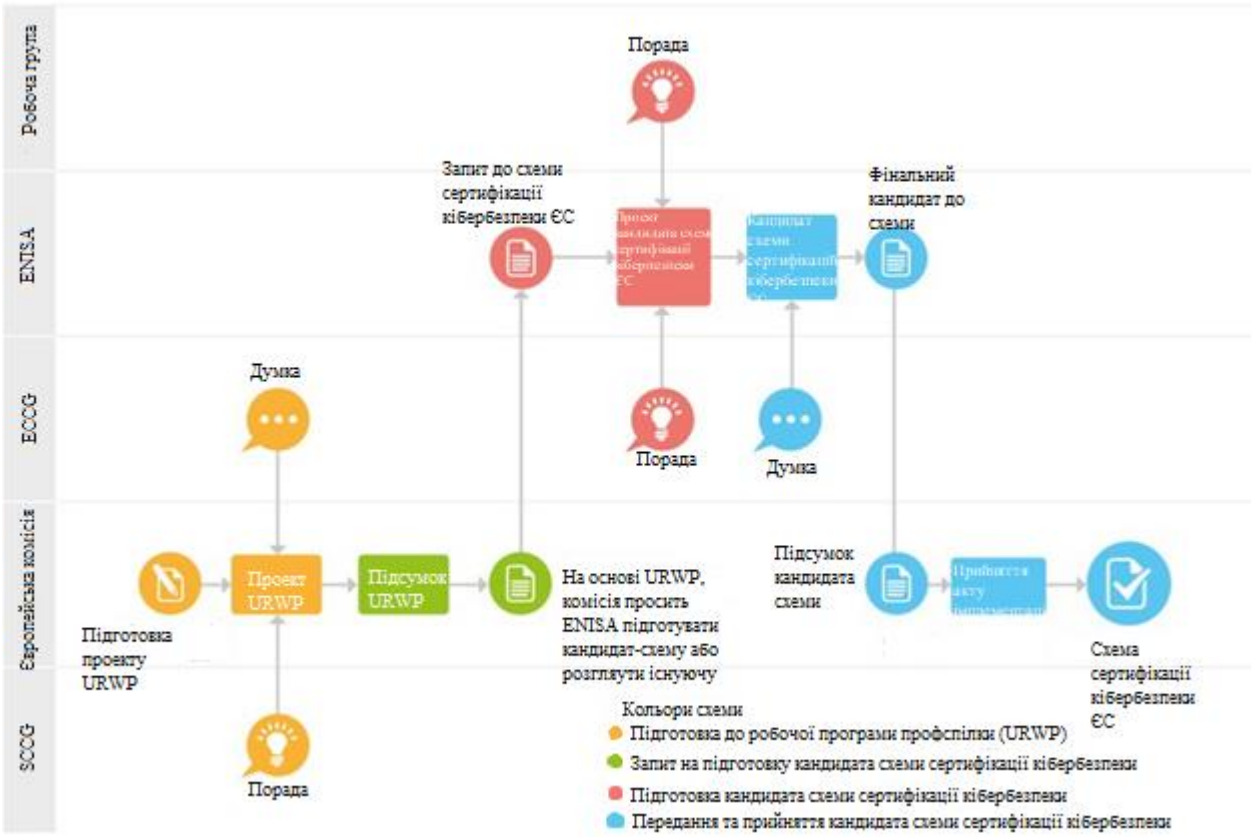

Рисунок 4.3 – Взаємодія сторін

4.5 Висновки до розділу 4

Після синтезу існуючої системи органів сертифікації було розроблено рекомендації щодо врегулювання кібербезпеки підключених транспортних засобів. А саме складено план з чотирьох основних пунктів:

1. Створення органів сертифікації кібербезпеки підключеного автомобіля чи розширення сфери в існуючих органах сертифікації.
2. Акредитація органів сертифікації на сферу кібербезпеки підключеного автомобіля. Призначення органів сертифікації кібербезпеки підключеного автомобіля.
3. Впровадження в діяльність НААУ (на всіх рівнях) можливості виконання робіт з акредитації органів сертифікації кібербезпеки підключеного автомобіля (експерти, технічний комітет, аудитори, тощо).
4. Отримання визнання НААУ на рівні ЄА (IAF) в сфері стандарту ISO 17065 щодо кібербезпеки підключеного автомобіля.

ВИСНОВКИ

У магістерській роботі наведено аналіз нормативно-правових аспектів і нове вирішення наукового завдання, що полягає у розробленні рекомендацій щодо державного регулювання питань кібербезпеки підключеного автомобіля. В роботі вирішені наступні задачі, що мають важливий практичний аспект:

1. Проаналізовано законодавство з питань кібербезпеки та його застосовність до кібербезпеки підключеного автомобіля.

2. На основі закону про технічне регулювання та оцінку відповідності розроблено пропозиції щодо технічного регулювання, як основи кібербезпеки підключеного автомобіля на державному рівні.

3. Досліджено механізми технічного регулювання такі як (оцінка відповідності та акредитація), які можуть бути застосовані для регулювання кібербезпеки підключеного автомобіля на державному рівні.

4. Досліджено шляхи отримання взаємного визнання результатів оцінки відповідності (сертифікації) на міжнародному рівні.

5. Розроблено пропозиції регулювання з регуляторних дій держави щодо нагальних питань кібербезпеки підключеного автомобіля:

5.1. Створення органів сертифікації кібербезпеки підключеного автомобіля чи розширення сфери в існуючих органах сертифікації.

5.2. Акредитація органів сертифікації на сферу кібербезпеки підключеного автомобіля

5.2.1. Призначення органів сертифікації кібербезпеки підключеного автомобіля.

5.3. Впровадження в діяльність НААУ (на всіх рівнях) можливості виконання робіт з акредитації органів сертифікації кібербезпеки підключеного автомобіля (експерти, технічний комітет, аудитори, тощо).

5.4. Отримання визнання НААУ на рівні ЄА (IAF) в сфері стандарту ISO 17065 щодо кібербезпеки підключеного автомобіля.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основні принципи технічного регулювання - Економіка фірми - Підручники для студентів онлайн (stud.com.ua)
2. Модель технічного регулювання, запроваджена в ЄС, є найбільш ефективною для міжнародного співробітництва, - фахівці. (rbc.ua)
3. https://blog.1gb.ua/umn%D1%8Be-y-nebezopasn%D1%8Be-chto-ugrozhaet-vladelc zam-v%D1%8Bsokotehnologychn%D1%8Bh-avtomobylej/
4. https://www.dqsglobal.com/uk-ua/blog/avtomobil%27na-kiberbezpeka-novi-obov%E 2%80%99yazkovi-pravila
5. https://zakon.rada.gov.ua/laws/show/z0788-22#Text
6. https://zakon.rada.gov.ua/laws/show/2163-19
https://uk.m.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%8E_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%BE%D1%8E
7. https://www.sae.org/standards/content/j3061_201601/
8. https://argus-sec.com/sae-j3061-cyber-security-guidebook-for-cyber-physical-vehicle-systems/
9. https://hss-opus.ub.ruhr-uni bochum.de/opus4/frontdoor/index/index/year/2021/docId/8356
https://ukraine-eu.mfa.gov.ua/centr-pidtrimki-eksporteriv/netarifne-regulyuvannya/tehnichne-regulyuvannya-v-yes
10. https://mtu.gov.ua/content/mizhnarodna-tehnichna-dopomoga-es-u-sferi-transportu.html

11. http://dspace.puet.edu.ua/bitstream/123456789/10374/1/%D0%9C%D0%A2%D0%A0-%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf

12. https://www.minregion.gov.ua/napryamki-diyalnosti/energoefektivnist-ta-energozberezhennya/vprovadzhennya-strategiyi-rozvitku-sistemi-tehnichnogo-regulyuvannya/informatsiya-shhodo-tehnichnogo-regulyuvannya/

13. 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/

14. https://www.dqsglobal.com/uk-ua/blog/avtomobil%27na-kiberbezpeka-novi-obov%E2%80%99yazkovi-pravila

15. https://legalitgroup.com/gdpr-ta-avtopilot/

16. https://www.sciencedirect.com/science/article/abs/pii/S2543000920300020

17. https://www.microcontrollertips.com/safety-and-cyber-security-for-the-connected-car-faq/

18. https://www.trustonic.com/opinion/top-10-security-challenges-for-connected-cars/

19. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjkpPTq5sH7AhUFiYsKHXVcDPMQFnoECBUQAw&url=https%3A%2F%2Fwww.bbva.ch%2Fen%2Fnews%2Fadvantages-and-disadvantages-of-autonomous-vehicles%2F&usg=AOvVaw322A3j0dcaC1WkLr53VkPk

20. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjkpPTq5sH7AhUFiYsKHXVcDPMQFnoECAoQAQ&url=https%3A%2F%2Fwww.trendmicro.com%2Fvinfo%2Fus%2Fsecurity%2Fnews%2Finternet-of-things%2Fin-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars&usg=AOvVaw1r72aQmzpClzMDtXWemE2h

21. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjG0NqT58H7AhUMuIsKHQSbCqAQFnoECBYQAQ&url=https%3A%2F%2Fwww.iso.org%2Fru%2Fstandard%2F70918.html&usg=AOvVaw1OAu_wMCmCqcdaUyHxEbb9

22. https://visuresolutions.com/ru/blog/automotive/iso-21434/

23. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiJzvCy58H7AhXErIsKHWKKBa8QFnoECAwQAQ&url=https%3A%2F%2Fwww.riscure.com%2Fnew-iso-sae-21434-security-standard-and-its-effect-on-the-industry%2F&usg=AOvVaw36BE7M_duGMbgv4ckOjz0Z

24. 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).

25. “Interinstitutional agreements”[Електронне джерело] – Режим доступу до ресурсу:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC%3A2018%3A012%3ATOC

26. Регламент Європейського Парламенту і Ради (ЄС) № 1025/2012 від 25 жовтня 2012 року про європейську стандартизацію та про внесення змін до директив Ради 89/686/ЄЕС та 93/15/ЄЕС та директив Європейського Парламенту і Ради 94/9/ЄС, 94/25/ЄС, 95/16/ЄС, 97/23/ЄС, 98/34/ЄС, 2004/22/ЄС, 2007/23/ЄС, 2009/23/ЄС та 2009/105/ЄС, а також про скасування Рішення Ради 87/95/ ЄЕС та Рішення Європейського Парламенту і Ради № 1673/2006/ЄС (OB L 316, 14.11.2012, с. 12).

27. Про основні засади забезпечення кібербезпеки України Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45.

28. 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

29. 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.

30. 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.

31. Про технічні регламенти та оцінку відповідності Закон України від 15.01.2015 № 124-VIII // Відомості Верховної Ради України. – 2015. – № 14.

32. Про акредитацію органів з оцінки відповідності Закон України від 17.05.2001 № 2407-III // Відомості Верховної Ради України. – 2001. – № 32.

33. International Accreditation Forum [Електронний ресурс]. – Режим доступу: https://www.iaf.nu/.

34. International Laboratory Accreditation Cooperation [Електронний ресурс]. – Режим доступу: https://ilac.org/.

35. European co-operation for Accreditation [Електронний ресурс]. – Режим доступу: https://european-accreditation.org/

36. 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

37. 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

38. 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.

39. 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

40. http://bulletin.khadi.kharkov.ua/article/view/257378/254253

41. https://www.rbc.ua/ukr/news/model_tehnicheskogo_regulirovaniya_vvedennaya_v_es_yavlyaetsya_naibolee_effektivnoy_dlya_mezhdunarodnogo_sotrudnichestva_spetsialisty_06042010