Доля К. В.

Основи кібербезпеки та надійності автомобільного транспорту в інтелектуальних транспортних системах

монографія

2026

Основи кібербезпеки та надійності автомобільного транспорту

в інтелектуальних транспортних системах

монографія

Доля К. В.

2026

УДК 656.13:004.056:656.025

Відомості про автора

Доля Костянтин Вікторович — професор, доктор технічних наук, кафедра автомобілів та транспортної інфраструктури, Національний аерокосмічний університет “Харківський авіаційний інститут”, Харків, Україна https://orcid.org/0000-0002-4693-9158

ISBN — 979-8-90553-923-7
DOI — 10.46299/979-8-90553-923-7

Опубліковано Primedia eLaunch

https://primediaelaunch.com

Монографія узагальнює теоретичні засади та прикладні підходи до забезпечення кібербезпеки й надійності автомобільного транспорту в інтелектуальних транспортних системах. Автомобільний транспорт розглядається як кіберфізична система, що охоплює транспортні засоби, дорожню інфраструктуру, V2X-комунікації, цифрові платформи, дані, програмне забезпечення, центри керування та організаційні процеси. Особливу увагу приділено кіберзагрозам, вразливостям, сценаріям атак, функціональній безпеці, експлуатаційній надійності, захисту даних, керуванню оновленнями та формуванню стійких архітектур транспортних сервісів.

Видання рекомендовано як навчальне та наукове джерело для здобувачів освіти спеціальності J8 “Автомобільний транспорт”, студентів, аспірантів, науково-педагогічних працівників і фахівців у сфері автомобільного транспорту, кібербезпеки, інтелектуальних транспортних систем, транспортного планування, організації дорожнього руху та цифрової мобільності. Матеріали можуть використовуватися під час виконання курсових робіт, кваліфікаційних і магістерських робіт, розроблення навчальних курсів, прикладних розрахунків та обґрунтування управлінських рішень щодо безпечної й надійної експлуатації цифровізованих транспортних систем.

Рекомендоване бібліографічне посилання на видання:

Доля, К. В. (2026). *Основи кібербезпеки та надійності автомобільного транспорту в інтелектуальних транспортних системах*. Primedia eLaunch. https://doi.org/10.46299/979-8-90553-923-7

УДК 656.13:004.056:656.025

Перелік скорочень

ITS Інтелектуальні транспортні системи.
CPS Кіберфізична система.
ECU Електронний блок керування.
SW Програмне забезпечення.
DB База даних.
GPS Глобальна система позиціонування.
GNSS Глобальна навігаційна супутникова система.
V2X Взаємодія транспортного засобу з усіма об'єктами транспортного середовища.
V2V Взаємодія між транспортними засобами.
V2I Взаємодія транспортного засобу з дорожньою інфраструктурою.
V2N Взаємодія транспортного засобу з мережею.
V2P Взаємодія транспортного засобу з пішоходами або персональними пристроями.
CAN Контролерна мережа бортових електронних блоків.
OBD Бортова діагностика.
OTA Дистанційне оновлення програмного забезпечення через мережу.
DoS Відмова в обслуговуванні.
DDoS Розподілена відмова в обслуговуванні.
IDS Система виявлення вторгнень.
PKI Інфраструктура відкритих ключів.
QoS Якість обслуговування.

Анотація

Монографію присвячено теоретичним і прикладним засадам забезпечення кібербезпеки та надійності автомобільного транспорту в інтелектуальних транспортних системах. Актуальність теми визначається швидкою трансформацією автомобільного транспорту в складну кіберфізичну систему, у якій технічні, програмні, телекомунікаційні, інформаційні та організаційні компоненти функціонують як взаємопов'язане середовище. Сучасні транспортні засоби, дорожня інфраструктура, центри керування рухом, хмарні сервіси, мобільні застосунки, телематичні платформи, системи моніторингу та V2X-комунікації формують нову реальність експлуатації транспорту, у якій безпека дорожнього руху дедалі більше залежить від якості даних, захищеності каналів зв'язку, надійності програмного забезпечення та стійкості цифрових сервісів.

У дослідженні автомобільний транспорт розглянуто не лише як сукупність транспортних засобів і дорожньої інфраструктури, а як багаторівневу систему, у якій фізичні процеси руху інтегровані з цифровими потоками даних, алгоритмами прийняття рішень, засобами автоматизованого керування, процедурами оновлення програмного забезпечення та організаційними механізмами реагування на інциденти. Такий підхід дає змогу оцінювати кібербезпеку й надійність не як ізольовані властивості, а як взаємопов'язані характеристики транспортної системи. Порушення кібербезпеки може проявлятися як технічна відмова, а технічна відмова може створювати умови для реалізації кіберзагрози. Тому особливу увагу приділено взаємозв'язку функціональної безпеки, експлуатаційної надійності, захисту даних і кіберстійкості транспортних сервісів.

У монографії послідовно розглянуто концептуальні основи інтелектуальних транспортних систем, роль підключеного автомобільного транспорту, особливості V2X-комунікацій, цифрових платформ і транспортних даних. Проаналізовано типові кіберзагрози для транспортних засобів та інфраструктури, зокрема несанкціонований доступ до електронних блоків керування, компрометацію телематичних модулів, підміну повідомлень, порушення доступності сервісів, атаки на канали зв'язку, маніпулювання сенсорними даними,

ризики дистанційного оновлення програмного забезпечення та вразливості інтегрованих транспортних платформ. Окрему увагу приділено сценаріям, у яких кіберінциденти можуть впливати на безпеку дорожнього руху, якість транспортних послуг, стабільність логістичних процесів і довіру користувачів до цифрових рішень.

Значну частину роботи присвячено проблемі надійності автомобільного транспорту в умовах цифровізації. У сучасних інтелектуальних транспортних системах надійність охоплює не лише справність механічних компонентів, а й працездатність електронних елементів, датчиків, каналів зв'язку, програмного забезпечення, серверної інфраструктури, баз даних, центрів керування та організаційних процедур. У монографії розглянуто підходи до оцінювання надійності цифровізованих транспортних систем, визначення критичних компонентів, аналізу відмов, планування резервування, моніторингу технічного стану та організації відновлення після порушень. Наголошено, що забезпечення надійності потребує не лише технічних рішень, а й експлуатаційних регламентів, навчання персоналу, системного контролю якості даних і постійного оновлення процедур безпеки.

Практичне значення монографії полягає у формуванні цілісного підходу до побудови безпечної та надійної архітектури автомобільного транспорту в інтелектуальних транспортних системах. Матеріал може бути використаний під час аналізу ризиків, розроблення вимог до цифрових транспортних сервісів, підготовки політик кібербезпеки, планування реагування на інциденти, оцінювання стійкості транспортної інфраструктури та організації експлуатаційної підтримки підключених транспортних засобів. Особливий акцент зроблено на необхідності поєднання технічних, інформаційних, організаційних і управлінських заходів, оскільки ізольоване використання окремих інструментів не може забезпечити належний рівень кіберстійкості.

Монографія призначена для здобувачів освіти транспортних і кібербезпекових спеціальностей, студентів, аспірантів, викладачів, науковців, фахівців автомобільного транспорту, інженерів з експлуатації інтелектуальних транспортних систем, спеціалістів з інформаційної безпеки, працівників органів управління транспортом і розробників цифрових сервісів мобільності. Видання може використовуватися для розроблення навчальних курсів, виконання курсових робіт, кваліфікаційних і магістерських робіт, прикладних розрахун-

ків, аналізу реальних транспортних ситуацій та обґрунтування управлінських рішень у сфері безпечної цифрової мобільності.

Ключові слова: автомобільний транспорт, кібербезпека, надійність, інтелектуальні транспортні системи, V2X-комунікації, кіберфізична система, транспортні дані, функціональна безпека, експлуатаційна надійність, кібер-стійкість, цифрова мобільність.

Зміст

Вступ

Автомобільний транспорт у XXI столітті перебуває у стані глибокої технологічної трансформації. Якщо раніше його розвиток переважно пов'язували з удосконаленням конструкції транспортних засобів, підвищенням ефективності двигунів, поліпшенням дорожньої інфраструктури та організацією перевезень, то нині визначального значення набувають цифрові технології, програмне забезпечення, телекомунікації, дані та інтелектуальні системи керування. Сучасний автомобіль дедалі більше перетворюється на підключений кіберфізичний об'єкт, що функціонує не ізольовано, а у взаємодії з іншими транспортними засобами, дорожньою інфраструктурою, сервісними платформами, центрами керування рухом, навігаційними системами, хмарними ресурсами та користувачами транспортних послуг.

Така зміна природи автомобільного транспорту відкриває нові можливості для підвищення ефективності, безпеки, екологічності та якості мобільності. Інтелектуальні транспортні системи дають змогу збирати й обробляти значні обсяги даних про дорожній рух, технічний стан транспортних засобів, поведінку водіїв, інтенсивність транспортних потоків, аварійні ситуації, погодні умови та стан інфраструктури. На основі цих даних можуть формуватися адаптивні режими керування рухом, рекомендації щодо маршрутизації, попередження про небезпеки, сервіси моніторингу, прогнозування заторів, підтримки громадського транспорту, логістики та аварійного реагування. Унаслідок цього автомобільний транспорт стає складником ширшої цифрової екосистеми міста, регіону або держави.

Водночас цифровізація автомобільного транспорту суттєво ускладнює вимоги до його безпечної експлуатації. Підключення транспортних засобів до зовнішніх мереж, використання V2X-комунікацій, дистанційних оновлень програмного забезпечення, хмарних платформ, мобільних застосунків і цифрових сервісів розширює поверхню потенційних атак. Якщо традиційні ризики автомобільного транспорту здебільшого були пов'язані з технічними відмовами, дорожніми умовами, помилками водія або організаційними недоліками, то в середовищі інтелектуальних транспортних систем до них додаються кібера-

таки, компрометація даних, несанкціонований доступ, підміна повідомлень, порушення доступності сервісів, вразливості програмного забезпечення та помилки в алгоритмах прийняття рішень.

Кібербезпека в автомобільному транспорті вже не може розглядатися лише як допоміжний напрям інформаційних технологій. Вона стає однією з базових умов безпечного функціонування транспортної системи. Порушення кібербезпеки може мати не тільки інформаційні або фінансові наслідки, а й безпосередньо впливати на безпеку дорожнього руху, доступність транспортних послуг, надійність логістичних процесів і довіру користувачів до цифрових рішень. Зокрема, некоректне повідомлення від інфраструктурного об'єкта, підроблені дані датчика, порушення роботи навігаційного сервісу або збій у системі дистанційного оновлення можуть спричинити помилки в керуванні, затримки, аварійні ситуації чи масові збої в роботі транспортної мережі.

Не менш важливою є проблема надійності автомобільного транспорту в середовищі інтелектуальних транспортних систем. Надійність більше не обмежується механічною справністю транспортного засобу або ресурсом його окремих вузлів. Вона охоплює стабільність роботи програмного забезпечення, коректність даних, безперервність зв'язку, узгодженість роботи датчиків, електронних блоків керування, телематичних платформ, дорожньої інфраструктури та центрів керування. У цифровізованій транспортній системі відмова одного компонента може швидко поширюватися на інші елементи й порушувати роботу сервісів, які залежать від своєчасного та достовірного обміну інформацією.

Актуальність дослідження зумовлена тим, що інтелектуальні транспортні системи дедалі активніше впроваджуються в міське управління, логістику, громадський транспорт, дорожню інфраструктуру та сервіси мобільності. Розвиток підключених транспортних засобів, автоматизованого водіння, цифрових двійників, систем моніторингу транспортних потоків, адаптивного світлофорного регулювання та інтегрованих платформ даних потребує нових підходів до оцінювання ризиків. Недостатня увага до кібербезпеки й надійності на етапах проєктування, впровадження або експлуатації може призвести до накопичення системних вразливостей, зростання витрат на усунення помилок, зниження довіри до інноваційних рішень і виникнення загроз для користувачів

транспортної системи.

Для України ця проблематика має особливе значення. Відновлення, модернізація та цифровізація транспортної інфраструктури повинні здійснюватися з урахуванням вимог кіберстійкості, сумісності з європейськими підходами, захисту персональних і транспортних даних, безпечної інтеграції цифрових сервісів та забезпечення безперервності транспортних процесів. Упровадження інтелектуальних транспортних систем без належної уваги до архітектури безпеки, стандартів обміну даними, процедур оновлення, резервування, контролю доступу й моніторингу може посилити залежність від окремих технологічних рішень і збільшити вразливість транспортної системи до зовнішніх та внутрішніх загроз.

Метою цієї монографії є системне висвітлення теоретичних і прикладних засад забезпечення кібербезпеки та надійності автомобільного транспорту в середовищі інтелектуальних транспортних систем. У роботі автомобільний транспорт розглядається як багаторівнева кіберфізична система, у якій транспортні засоби, інфраструктура, комунікації, цифрові платформи, дані, користувачі та організаційні процеси формують єдине середовище функціонування. Такий підхід дає змогу не лише описати окремі загрози чи технічні рішення, а й показати взаємозалежність між архітектурою системи, якістю даних, стійкістю сервісів, безпекою комунікацій, надійністю компонентів і управлінням ризиками.

У монографії послідовно розглядаються концептуальні основи інтелектуальних транспортних систем, роль підключеного автомобільного транспорту, особливості V2X-комунікацій, кіберзагрози та вразливості, питання функціональної безпеки, експлуатаційної надійності, захисту даних, керування оновленнями, моніторингу інцидентів і побудови кіберстійкої транспортної архітектури. Окрему увагу приділено практичним аспектам використання цифрових технологій для підвищення безпеки руху, надійності сервісів, ефективності перевезень і стійкості транспортної системи до збоїв та атак.

Матеріали монографії можуть бути корисними для науковців, викладачів, здобувачів освіти транспортних і кібербезпекових спеціальностей, фахівців автомобільного транспорту, розробників інтелектуальних транспортних систем, працівників органів управління транспортом, спеціалістів з інформаційної безпеки та всіх, хто бере участь у проєктуванні, впровадженні й експлуа-

тації цифрових транспортних рішень. Практичне значення роботи полягає у формуванні цілісного бачення того, як поєднати технологічний розвиток автомобільного транспорту з вимогами безпеки, надійності, стійкості та відповідального управління цифровою мобільністю.

1 Теоретичні основи кібербезпеки та надійності автомобільного транспорту в інтелектуальних транспортних системах

Сучасний автомобільний транспорт швидко перетворюється на складну кіберфізичну систему, у якій механічні, електронні, програмні, телекомунікаційні та організаційні компоненти працюють як єдине середовище мобільності. Автомобіль уже не є лише автономним технічним засобом, що рухається дорогою за командами водія. Він стає підключеним об'єктом, який обмінюється даними з іншими транспортними засобами, дорожньою інфраструктурою, сервісними платформами, центрами керування рухом, виробником, постачальником програмного забезпечення та користувацькими цифровими сервісами. Такий розвиток створює значний потенціал для підвищення безпеки, ефективності та комфорту перевезень, але одночасно формує нові вимоги до кібербезпеки й надійності [1, 2, 3, 5].

Інтелектуальні транспортні системи (ITS) є технологічною та організаційною основою цієї трансформації. Вони забезпечують збирання, передавання, оброблення й використання транспортних даних для керування рухом, інформування користувачів, підтримки кооперативних сервісів, прогнозування транспортних станів, реагування на інциденти та інтеграції автомобільного транспорту з ширшою цифровою екосистемою міста або регіону [6, 28, 29, 30]. У межах ITS безпека дорожнього руху, функціональна безпека, кібербезпека, захист персональних даних і надійність сервісів стають взаємозалежними поняттями.

Особливість теми полягає у тому, що розвиток автомобільного транспорту відбувається одночасно в кількох напрямах: підключені транспортні засоби, автоматизоване й автономне водіння, V2X-комунікації, програмно-визначені автомобілі, дистанційні оновлення, хмарні сервіси, машинне навчання, цифрові двійники транспортної мережі та інтеграція з міськими платформами даних [43, 44, 33, 61]. Кожний із цих напрямів збільшує функціональні можливості системи, але також розширює поверхню атак, підвищує складність перевірки безпеки та створює нові сценарії відмов.

1.1 Актуальність теми

Актуальність дослідження зумовлена тим, що автомобільний транспорт залишається одним із ключових елементів економічної, соціальної та оборонної стійкості держави. Він забезпечує щоденну мобільність населення, функціонування логістичних ланцюгів, доставку критичних вантажів, роботу громадського транспорту, екстрених служб і міської інфраструктури. Будь-яке порушення надійності автомобільного транспорту безпосередньо впливає на безпеку людей, економічні втрати, доступність послуг і стабільність територій. У цифровому середовищі такі порушення можуть бути спричинені не лише фізичними відмовами, дорожніми подіями або помилками водія, а й програмними дефектами, кібератаками, недостовірними даними або відмовами комунікаційних сервісів [9, 11, 12, 37].

Підключення транспортних засобів до зовнішніх мереж змінило саму природу автомобільних ризиків. Раніше відмова або помилка переважно локалізувалася в межах одного транспортного засобу чи окремої ділянки інфраструктури. Сьогодні вразливість програмного забезпечення, компрометація сервера, помилка оновлення або атака на V2X-комунікації можуть одночасно вплинути на велику кількість автомобілів, сервісів і користувачів. Тому кібербезпека більше не є допоміжною функцією інформаційних технологій; вона стає умовою безпечної експлуатації транспортної системи [1, 9, 40, 39].

Не менш важливою є проблема надійності. Надійність у сучасному автомобільному транспорті охоплює працездатність механічних вузлів, електронних блоків, внутрішніх мереж, датчиків, програмного забезпечення, телематичних модулів, дорожньої інфраструктури, центрів керування та цифрових сервісів. Якщо хоча б один із цих компонентів працює нестабільно, загальна якість транспортної послуги знижується. Наприклад, неточний датчик може сформувати неправильне повідомлення, нестабільний канал зв'язку — затримати попередження, помилка аналітичної моделі — створити хибний прогноз, а збій центру керування — порушити координацію дорожнього руху [2, 4, 6, 31].

У межах ITS кібербезпека й надійність пов'язані через спільну мету — забезпечення передбачуваної, безпечної та стійкої роботи транспортної системи. Кіберінцидент може проявитися як відмова сервісу, а технічна відмова

може створити умови для кібератаки. Наприклад, відсутність своєчасного оновлення програмного забезпечення збільшує ризик використання відомої вразливості; компрометація даних датчика може виглядати як технічна помилка; порушення доступності хмарного сервісу може призвести до деградації функцій маршрутизації або моніторингу [3, 10, 38, 56].

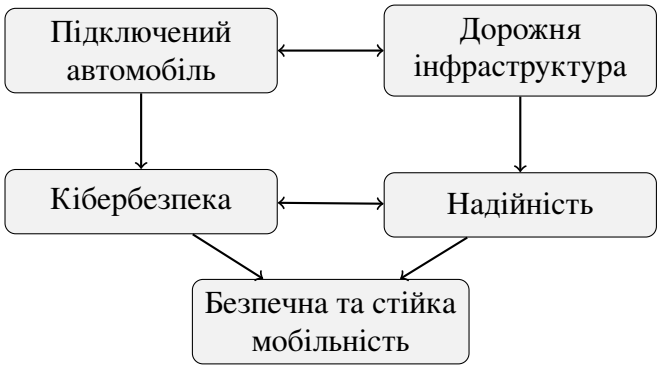

Рис. 1.1: Зв'язок кібербезпеки, надійності та безпечної мобільності в ITS

Актуальність теми посилюється нормативними змінами. Міжнародні документи ISO/SAE 21434, ISO 24089, Правила ООН № 155 та Правила ООН № 156 встановлюють вимоги до кібербезпеки, керування оновленнями й організаційних процесів у життєвому циклі транспортних засобів [1, 3, 9, 10]. Для ITS важливими є також стандарти архітектури й комунікацій, зокрема ISO 14813-1, ISO 21217, ETSI EN 302 665 та специфікації ETSI щодо CAM, DENM і безпеки повідомлень [5, 6, 13, 14, 15, 16]. Це означає, що дослідження має не лише теоретичне, а й прикладне значення для гармонізації практик проєктування, впровадження й експлуатації автомобільного транспорту.

Для України тема має додаткову практичну вагу. Відновлення й модернізація транспортної інфраструктури потребують рішень, які одразу враховують цифровізацію, кіберстійкість, сумісність із європейськими підходами та захист даних. Якщо нові ITS-рішення створюватимуться без єдиних принципів архітектури, безпеки та надійності, у майбутньому це призведе до високих витрат на інтеграцію, залежності від окремих постачальників і зниження довіри користувачів. Отже, актуальність теми визначається одночасно технологічними, безпековими, нормативними та управлінськими факторами.

1.2 Мета і завдання дослідження

Метою дослідження є обґрунтування теоретичних і прикладних засад забезпечення кібербезпеки та надійності автомобільного транспорту в середовищі інтелектуальних транспортних систем, а також формування системного підходу до аналізу ризиків, компонентів, даних, комунікацій і організаційних процесів, що впливають на безпечне функціонування підключеного автомобільного транспорту.

Досягнення цієї мети потребує розгляду автомобільного транспорту як багаторівневої кіберфізичної системи. У такій системі транспортний засіб, дорожня інфраструктура, V2X-комунікації, центри керування, цифрові платформи, нормативні вимоги й користувацькі сервіси взаємодіють між собою та формують спільний рівень ризику. Тому дослідження не може бути обмежене лише автомобільною електронікою або лише дорожньою інфраструктурою. Воно повинно охоплювати зв'язки між технічними, інформаційними й організаційними складовими [6, 5, 37].

Для реалізації поставленої мети визначено такі завдання:

1. проаналізувати поняття, структуру та основні компоненти інтелектуальних транспортних систем як середовища функціонування сучасного автомобільного транспорту;
2. дослідити роль транспортних засобів, дорожньої інфраструктури, центрів керування, V2X-комунікацій і цифрових сервісів у забезпеченні безпеки й надійності перевезень;
3. систематизувати типові кіберзагрози, вразливості та сценарії атак на підключені й автоматизовані транспортні засоби;
4. визначити взаємозв'язок між кібербезпекою, функціональною безпекою, безпекою передбачуваної функціональності та експлуатаційною надійністю;
5. розглянути методи оцінювання ризиків, виявлення аномалій, захисту комунікацій, керування оновленнями та підтримки життєвого циклу автомобільних систем;
6. сформувати практичні рекомендації щодо побудови кіберстійкої та надійної архітектури ITS для автомобільного транспорту.

Формально мету дослідження можна подати через мінімізацію інтеграль-

Табл. 1.1: Відповідність мети, завдань і очікуваних результатів дослідження

Складова	**Зміст**	**Очікуваний результат**
Мета	Системне обґрунтування кібербезпеки та надійності автомобільного транспорту в ITS	Концептуальна основа дослідження та логіка подальших розділів
Аналітичні завдання	Аналіз архітектури ITS, V2X, даних, компонентів і загроз	Систематизований опис середовища ризику
Методичні завдання	Вибір методів оцінювання ризиків, надійності, аномалій і захисту	Інструментарій для аналізу та практичного застосування
Практичні завдання	Формування рекомендацій для впровадження й експлуатації	Підходи до підвищення кіберстійкості та надійності

ного ризику функціонування автомобільного транспорту в ITS:

$$R_{int} = w_c R_c + w_f R_f + w_o R_o + w_d R_d \to \min, \tag{1.1}$$

Пояснення до формули: Ця формула використовується для кількісного опису відповідного показника в межах аналізу кібербезпеки, надійності або ефективності автомобільного транспорту в ITS. Вона потрібна для того, щоб перейти від якісного опису проблеми до числової оцінки, яку можна порівнювати між різними об'єктами, сценаріями або періодами спостереження. Ліва частина формули показує шуканий результат, тобто інтегральний показник, ризик, імовірність, витрати, ефект або іншу величину, яку необхідно визначити. Права частина формули містить вхідні параметри, вагові коефіцієнти, часткові складові або функціональні залежності, за допомогою яких виконується розрахунок. Для практичного застосування спочатку збирають вихідні дані з телематики, журналів подій, експлуатаційної статистики, нормативних вимог або експертних оцінок. Після цього параметри приводять до узгоджених одиниць вимірювання, за потреби нормують, перевіряють на повноту і підставляють у відповідні члени формули. Розрахунок виконують послідовно: спочатку визначають проміжні складові, потім об'єднують їх відповідно до математичних операцій у формулі й отримують підсумкове значення. Отриманий результат використовують для порівняння альтернатив,

виявлення критичних компонентів, вибору заходів захисту або обґрунтування управлінського рішення.

де R_c — кіберризик, R_f — ризик функціональної або технічної відмови, R_o — організаційний ризик, R_d — ризик, пов'язаний з даними, а w_c, w_f, w_o, w_d — вагові коефіцієнти, що визначають відносну важливість кожної складової. Така постановка підкреслює, що безпека автомобільного транспорту в ITS не може оцінюватися за одним показником.

Завдання дослідження також передбачають розмежування рівнів аналізу. На мікрорівні розглядаються транспортний засіб, електронні блоки, датчики, внутрішні мережі, програмне забезпечення й бортові засоби захисту. На мезорівні аналізуються дорожня інфраструктура, V2X-вузли, світлофорні контролери, центри керування та операторські сервіси. На макрорівні досліджуються нормативні вимоги, політика даних, організаційні процеси, взаємодія суб'єктів і стратегія розвитку ITS. Поєднання цих рівнів дає змогу уникнути вузького трактування кібербезпеки як суто технічної проблеми.

1.3 Об'єкт і предмет дослідження

Об'єктом дослідження є процеси функціонування автомобільного транспорту в середовищі інтелектуальних транспортних систем, зокрема процеси інформаційної взаємодії транспортних засобів, дорожньої інфраструктури, центрів керування, цифрових сервісів і користувачів. Об'єкт охоплює як фізичний рух транспортних засобів, так і цифрові процеси, що супроводжують цей рух: збирання даних, передавання повідомлень, оброблення інформації, формування керуючих впливів, оновлення програмного забезпечення, моніторинг стану та реагування на інциденти.

Предметом дослідження є методи, моделі, принципи й організаційно-технічні підходи до забезпечення кібербезпеки та надійності автомобільного транспорту в ITS. До предметної області належать архітектура ITS, комунікації V2V, V2I і V2X, безпека даних, захист автомобільних мереж, виявлення аномалій, оцінювання ризиків, стандартизовані вимоги, керування оновленнями, резервування критичних функцій і підтримка експлуатаційної стійкості [17, 20, 22, 3].

Межі дослідження визначаються тим, що основна увага приділяється автомобільному транспорту в ITS, а не всім видам транспорту загалом. Во-

дночас окремі положення можуть бути застосовані до міської мобільності, громадського транспорту, логістичних систем і автоматизованих транспортних сервісів. Дослідження не зводиться до розроблення конкретного криптографічного алгоритму або програмного продукту; воно спрямоване на системне узагальнення підходів, які можуть використовуватися під час проєктування, оцінювання й експлуатації комплексних транспортних рішень.

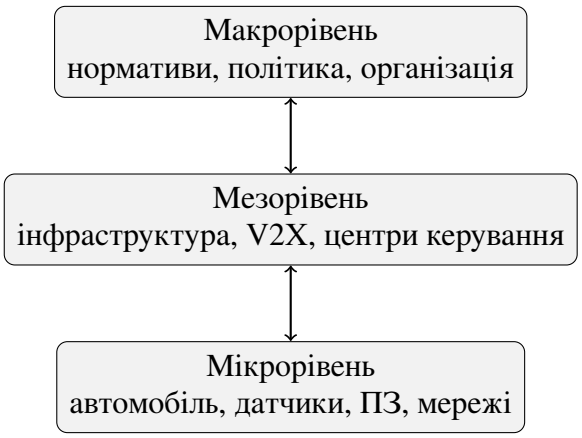

Рис. 1.2: Рівні об'єкта і предмета дослідження

Предмет дослідження має міждисциплінарний характер. Він поєднує транспортну інженерію, автомобільну електроніку, теорію надійності, кібербезпеку, системний аналіз, телекомунікації, оброблення даних і нормативне регулювання. Така міждисциплінарність є необхідною, оскільки реальні інциденти в підключених транспортних системах рідко мають лише одну причину. Зазвичай вони виникають на перетині технічної вразливості, помилки конфігурації, недостатнього моніторингу, організаційного розриву або некоректної інтерпретації даних [62, 38, 63].

Об'єкт і предмет дослідження можна також описати через взаємодію стану транспортної системи та керуючих впливів. Якщо X позначає множину можливих станів автомобільного транспорту, U — множину керуючих впливів ITS, Z — множину загроз і збурень, то предмет дослідження охоплює правила вибору таких впливів $u \in U$, які забезпечують прийнятний рівень безпеки й надійності за наявності $z \in Z$:

$$u^* = \arg\min_{u \in U} L(x, u, z), \tag{1.2}$$

Пояснення до формули: Ця формула використовується для кількісного опису відповідного показника в межах аналізу кібербезпеки, надійності

або ефективності автомобільного транспорту в ITS. Вона потрібна для того, щоб перейти від якісного опису проблеми до числової оцінки, яку можна порівнювати між різними об'єктами, сценаріями або періодами спостереження. Ліва частина формули показує шуканий результат, тобто інтегральний показник, ризик, імовірність, витрати, ефект або іншу величину, яку необхідно визначити. Права частина формули містить вхідні параметри, вагові коефіцієнти, часткові складові або функціональні залежності, за допомогою яких виконується розрахунок. Для практичного застосування спочатку збирають вихідні дані з телематики, журналів подій, експлуатаційної статистики, нормативних вимог або експертних оцінок. Після цього параметри приводять до узгоджених одиниць вимірювання, за потреби нормують, перевіряють на повноту і підставляють у відповідні члени формули. Розрахунок виконують послідовно: спочатку визначають проміжні складові, потім об'єднують їх відповідно до математичних операцій у формулі й отримують підсумкове значення. Отриманий результат використовують для порівняння альтернатив, виявлення критичних компонентів, вибору заходів захисту або обґрунтування управлінського рішення.

де $L(x, u, z)$ — функція втрат, що враховує затримки, аварійні ризики, кіберризики, відмови сервісів і витрати на відновлення.

1.4 Методи дослідження

Методологічну основу роботи становить системний підхід, який дає змогу розглядати автомобільний транспорт в ITS як сукупність взаємопов'язаних технічних, інформаційних і організаційних елементів. Системний підхід необхідний тому, що локальне підвищення захищеності одного компонента не завжди гарантує підвищення безпеки всієї системи. Наприклад, криптографічний захист повідомлень не усуває ризик помилкових даних від несправного датчика, а резервування сервера не вирішує проблему неправильної організації доступу операторів.

Для аналізу нормативної та технічної бази застосовується метод порівняльного аналізу стандартів і рекомендацій. Він передбачає зіставлення вимог ISO/SAE 21434, ISO 26262, ISO 21448, ISO 24089, Правила ООН № 155, Правила ООН № 156, ETSI та IEEE щодо кібербезпеки, функціональної безпеки, оновлень, комунікацій і сертифікації [1, 2, 4, 3, 9, 10]. Такий аналіз

дає змогу визначити спільні принципи та прогалини між різними групами вимог.

Методи моделювання використовуються для опису транспортних потоків, каналів зв'язку, процесів деградації, ризиків і сценаріїв атак. Для ITS важливими є як детерміновані, так і ймовірнісні моделі. Детерміновані моделі описують структурні зв'язки між компонентами, а ймовірнісні — невизначеність відмов, затримок, атак і похибок даних. Наприклад, імовірність безвідмовної роботи компонента за експоненційного закону відмов може бути подана як:

$$P(t) = e^{-\lambda t}, \tag{1.3}$$

Пояснення до формули: Ця формула використовується для кількісного опису відповідного показника в межах аналізу кібербезпеки, надійності або ефективності автомобільного транспорту в ITS. Вона потрібна для переходу від якісного опису процесу до числової оцінки, яку можна порівнювати між різними об'єктами, сценаріями або періодами спостереження. У лівій частині подано шуканий результат, тобто ризик, імовірність, рівень надійності, ефект, витрати або інший інтегральний показник. Права частина містить параметри, вагові коефіцієнти, часткові складові чи функціональні залежності, за допомогою яких формується підсумкове значення. Для розрахунку спочатку збирають вихідні дані з телематики, журналів подій, експлуатаційної статистики, нормативних вимог або експертних оцінок. Далі ці дані перевіряють, приводять до узгоджених одиниць вимірювання, за потреби нормують і підставляють у відповідні елементи формули. Після цього послідовно обчислюють проміжні складові, виконують зазначені математичні операції та отримують підсумковий результат. Отримане значення застосовують для порівняння альтернатив, визначення критичних компонентів, вибору заходів захисту або обґрунтування управлінського рішення.

де λ — інтенсивність відмов, а t — час експлуатації. Для складної ITS цей показник аналізується не ізольовано, а з урахуванням резервування, залежностей і можливості відновлення.

Для оцінювання ризиків застосовуються методи ідентифікації активів, загроз, вразливостей, сценаріїв впливу та наслідків. У транспортній сфері такі методи мають враховувати не лише конфіденційність інформації, а й фізичні наслідки для дорожнього руху. Ризик може бути оцінений як добуток

імовірності події та тяжкості наслідків:

$$R = P_{event} \cdot S_{impact}, \tag{1.4}$$

Пояснення до формули: Ця формула використовується для кількісного опису відповідного показника в межах аналізу кібербезпеки, надійності або ефективності автомобільного транспорту в ITS. Вона потрібна для переходу від якісного опису процесу до числової оцінки, яку можна порівнювати між різними об'єктами, сценаріями або періодами спостереження. У лівій частині подано шуканий результат, тобто ризик, імовірність, рівень надійності, ефект, витрати або інший інтегральний показник. Права частина містить параметри, вагові коефіцієнти, часткові складові чи функціональні залежності, за допомогою яких формується підсумкове значення. Для розрахунку спочатку збирають вихідні дані з телематики, журналів подій, експлуатаційної статистики, нормативних вимог або експертних оцінок. Далі ці дані перевіряють, приводять до узгоджених одиниць вимірювання, за потреби нормують і підставляють у відповідні елементи формули. Після цього послідовно обчислюють проміжні складові, виконують зазначені математичні операції та отримують підсумковий результат. Отримане значення застосовують для порівняння альтернатив, визначення критичних компонентів, вибору заходів захисту або обґрунтування управлінського рішення.

де P_{event} — імовірність реалізації загрози або відмови, а S_{impact} — оцінка наслідків. У розширених моделях до цієї формули додають коефіцієнти виявлення, експозиції, керованості та відновлюваності [64, 11].

Методи аналізу даних використовуються для оброблення потоків від датчиків, транспортних засобів, V2X-повідомлень, центрів керування та цифрових сервісів. До них належать статистичний аналіз, фільтрація, виявлення аномалій, прогнозування часових рядів, класифікація подій, кореляційний аналіз і методи машинного навчання. У роботі такі методи розглядаються як інструмент підтримки кібербезпеки й надійності, оскільки вони дають змогу виявляти нетипові режими руху, підозрілі повідомлення, деградацію датчиків або відхилення в роботі автомобільних мереж [55, 57, 56].

Метод сценарного аналізу використовується для розгляду типових ситуацій: відмова датчика, компрометація V2X-повідомлення, недоступність хмарного сервісу, помилка оновлення, атака на дорожній контролер, поширен-

Табл. 1.2: Методи дослідження та їх призначення

Метод	**Призначення**	**Результат застосування**
Системний аналіз	Визначення компонентів, зв'язків і рівнів ITS	Структурна модель транспортної системи
Порівняльний аналіз стандартів	Зіставлення вимог безпеки, надійності й оновлень	Узгоджені принципи та нормативні орієнтири
Моделювання ризиків	Оцінювання загроз, відмов і наслідків	Показники ризику та пріоритети захисту
Аналіз даних	Виявлення аномалій і прогнозування станів	Підтримка моніторингу й керування
Узагальнення практик	Формування рекомендацій для впровадження	Прикладні висновки для ITS

ня неправдивої інформації про дорожню подію або порушення доступності центру керування. Сценарний підхід дає змогу оцінити не лише ймовірність окремої події, а й ланцюг наслідків, що виникає в кіберфізичному середовищі.

Використання зазначених методів забезпечує комплексність дослідження. Системний аналіз визначає межі проблеми; порівняльний аналіз стандартів задає нормативну рамку; моделювання формалізує зв'язки й ризики; аналіз даних підтримує виявлення аномалій; сценарний підхід показує практичні наслідки; узагальнення дає змогу сформувати рекомендації для подальших розділів монографії.

1.5 Практичне значення дослідження

Практичне значення роботи полягає у формуванні системного підходу до впровадження, оцінювання та експлуатації кіберстійких і надійних рішень автомобільного транспорту в ITS. Результати дослідження можуть бути використані під час проєктування архітектури інтелектуальних транспортних систем, підготовки вимог до підключених транспортних засобів, модернізації дорожньої інфраструктури, створення центрів керування рухом, організації V2X-сервісів, розроблення політик даних і планування заходів кіберзахисту.

Для органів управління транспортом робота має значення як методична основа для визначення пріоритетів цифровізації. Вона допомагає відрізняти технологічно привабливі, але другорядні сервіси від критичних функцій, що

безпосередньо впливають на безпеку та надійність. Наприклад, перед упровадженням складних сервісів автоматизованого керування доцільно забезпечити якісні базові дані, стабільну роботу світлофорних контролерів, захищені канали зв'язку, резервування центру керування та процедури реагування на інциденти.

Для операторів автомобільного транспорту практичне значення полягає у можливості використовувати результати дослідження для підвищення надійності перевезень. Дані ITS можуть підтримувати прогнозування часу прибуття, контроль технічного стану, оптимізацію маршрутів, виявлення небезпечних режимів руху, зменшення простоїв і підвищення регулярності. Водночас оператори повинні враховувати кіберризики телематичних платформ, мобільних застосунків, систем оплати, диспетчерського програмного забезпечення та каналів зв'язку [58, 59, 60].

Для виробників і розробників автомобільних систем результати роботи можуть бути використані під час формування вимог до безпечної архітектури, оновлень, журналювання, діагностики, виявлення аномалій і взаємодії з інфраструктурою. Особливе значення має принцип узгодження кібербезпеки з функціональною безпекою: захисний механізм не повинен створювати небезпечну затримку, а безпечний режим деградації повинен враховувати можливість кібератаки [2, 1, 4].

Рис. 1.3: Напрями практичного використання результатів роботи

Практичне значення роботи також полягає у підтримці навчального процесу. Матеріали монографії можуть бути використані для підготовки

фахівців з автомобільного транспорту, кібербезпеки транспортних систем, транспортної інженерії, інтелектуальних транспортних систем і цифрової мобільності. Структуроване подання понять, стандартів, ризиків, моделей і практичних вимог дає змогу формувати у здобувачів не фрагментарне, а системне бачення безпеки сучасного автомобільного транспорту.

Очікуваний практичний ефект від застосування результатів роботи можна подати як зменшення втрат від інцидентів і відмов:

$$\Delta C = C_{before} - C_{after}, \tag{1.5}$$

Пояснення до формули: Ця формула показує, як кількісно оцінити відповідний показник у системі кібербезпеки, надійності або ефективності автомобільного транспорту в ITS. Вона потрібна для того, щоб не обмежуватися описовим аналізом, а отримати числовий результат для порівняння різних варіантів, сценаріїв або технічних рішень. Шукана величина розміщена в лівій частині формули, а права частина містить параметри, коефіцієнти, складові ризику, імовірності, витрати або інші вхідні дані. Для розрахунку спочатку визначають значення всіх змінних за результатами вимірювань, телематичних даних, експлуатаційної статистики, нормативних вимог або експертного оцінювання. Після цього дані перевіряють на коректність, приводять до однакових одиниць вимірювання, за потреби нормують і підставляють у відповідні елементи формули. Далі послідовно виконують зазначені математичні операції, обчислюють проміжні складові та отримують підсумкове значення показника. Результат використовують для пояснення стану системи, вибору кращої альтернативи, визначення критичних компонентів і обґрунтування практичних заходів управління або захисту.

де C_{before} — очікувані витрати, пов'язані з інцидентами, відмовами, затримками та відновленням до впровадження рекомендацій, а C_{after} — відповідні витрати після впровадження організаційно-технічних заходів. Якщо $\Delta C > 0$, то запропоновані підходи мають позитивний економічний або експлуатаційний ефект.

Узагальнено практичне значення полягає в тому, що робота створює основу для прийняття рішень у складному середовищі, де технологічні інновації повинні бути збалансовані з безпекою, надійністю, нормативною відповідністю, захистом даних і довірою користувачів. Такий підхід є необхідним для

розвитку автомобільного транспорту в умовах цифровізації, кооперативної мобільності та зростання залежності від програмного забезпечення.

Логіка побудови монографії відповідає поступовому переходу від загального опису проблеми до конкретних інженерних, організаційних і безпекових рішень. Перший розділ визначає актуальність, мету, завдання, об'єкт, предмет, методи та практичне значення роботи. Він формує вихідну рамку, у якій автомобільний транспорт розглядається не як сукупність окремих машин, а як елемент інтелектуального, підключеного й керованого середовища. Така постановка потрібна для того, щоб подальші розділи не зводилися лише до опису технологій, а були пов'язані з проблемами безпеки, надійності й управління ризиками.

Другий розділ присвячено інтелектуальним транспортним системам як основі сучасного автомобільного транспорту. У ньому розглядаються поняття, структура, компоненти ITS, технології V2V, V2I і V2X, а також роль даних і цифрових сервісів у керуванні рухом. Цей розділ є фундаментом для подальшого аналізу, оскільки саме в ITS виникає більшість нових взаємозв'язків між автомобілем, інфраструктурою, центрами керування та користувачами [5, 6, 33].

Наступні розділи доцільно будувати навколо аналізу загроз, моделей ризику, методів захисту, надійності автомобільних компонентів, безпеки даних, організації оновлень, моніторингу та практичних рекомендацій. Така послідовність дає змогу рухатися від опису середовища до оцінювання небезпек, а потім — до заходів зниження ризику. У результаті монографія набуває прикладної спрямованості: вона не лише описує стан технологій, а й показує, як ці технології повинні впроваджуватися безпечно.

Важливо, що така логіка враховує життєвий цикл автомобільних і транспортних систем. Кібербезпека й надійність не можуть забезпечуватися лише на етапі експлуатації. Вони повинні враховуватися під час планування, проєктування, закупівлі, інтеграції, тестування, введення в експлуатацію, супроводу, оновлення та виведення з експлуатації. Саме тому стандарти й регуляторні документи приділяють увагу не лише технічним механізмам захисту, а й процесам керування, відповідальності, документації, моніторингу та реагування [1, 3, 9, 10].

Для оцінювання зрілості підходу до кібербезпеки та надійності в роботі

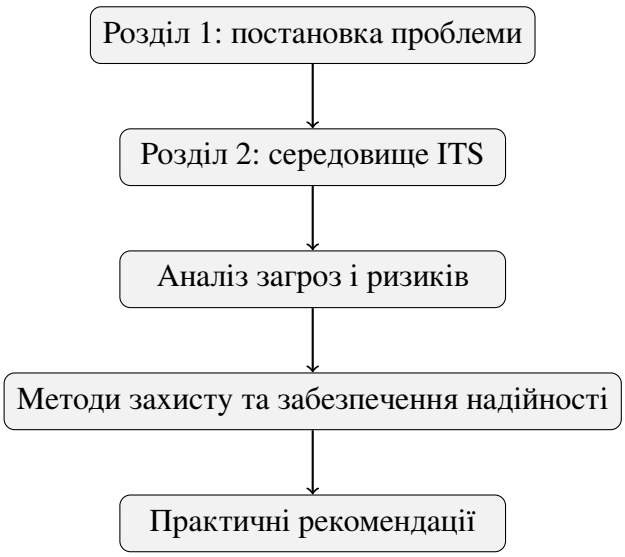

Рис. 1.4: Логіка переходу від постановки проблеми до практичних рекомендацій

використовується ідея узгодження трьох контурів: технічного, організаційного та інформаційного. Технічний контур охоплює транспортні засоби, датчики, контролери, мережі та виконавчі пристрої. Організаційний контур охоплює ролі, процедури, відповідальність, навчання персоналу й нормативну відповідність. Інформаційний контур охоплює дані, моделі, алгоритми, сервіси, журнали подій і політики доступу. Якщо хоча б один із цих контурів залишається слабким, загальна стійкість ITS знижується.

Узагальнену зрілість можна подати як добуток часткових коефіцієнтів:

$$G = M_t \cdot M_o \cdot M_i, \tag{1.6}$$

Пояснення до формули: Ця формула задає кількісний спосіб опису показника, який використовується в межах відповідного розділу монографії. Вона потрібна для того, щоб перетворити якісний опис процесу, ризику або властивості системи на числову оцінку. У лівій частині формули подано шуканий результат, а в правій частині наведено параметри, коефіцієнти або складові, через які цей результат визначається. Для розрахунку спочатку встановлюють значення всіх змінних за даними спостережень, телематики, експлуатаційної статистики, нормативних вимог або експертних оцінок. Після цього вихідні дані перевіряють, узгоджують за одиницями вимірювання, за потреби нормують і підставляють у формулу. Далі послідовно виконують математичні операції, обчислюють проміжні величини та отримують підсумкове

значення показника. Отриманий результат використовують для порівняння альтернатив, оцінювання рівня ризику чи надійності, вибору захисних заходів і обґрунтування управлінських рішень.

де M_t — технічна зрілість, M_o — організаційна зрілість, M_i — інформаційна зрілість. Добуткова форма підкреслює, що низьке значення будь-якого компонента суттєво обмежує загальний результат. Наприклад, високий рівень технічного оснащення не компенсує відсутність процедур реагування, а якісна організація не може повністю компенсувати застаріле й незахищене обладнання.

Очікуваними результатами дослідження є систематизація понятійного апарату, уточнення ролі ITS у сучасному автомобільному транспорті, визначення ключових компонентів ризику, узагальнення підходів до забезпечення кібербезпеки й надійності, а також формування практичних рекомендацій для суб'єктів, які проєктують, експлуатують або регулюють транспортні системи. Результати мають бути корисними для наукових досліджень, освітнього процесу, інженерної практики та управління транспортною інфраструктурою.

Очікуваний науково-прикладний результат полягає у встановленні зв'язку між трьома групами вимог: вимогами до безпеки дорожнього руху, вимогами до кібербезпеки та вимогами до експлуатаційної надійності. У реальних ITS ці вимоги не існують окремо. Наприклад, захист V2X-повідомлення цифровим підписом підвищує довіру до нього, але потребує часу на перевірку; резервування каналу підвищує доступність, але ускладнює керування конфігурацією; збирання детальних даних покращує аналітику, але створює вимоги до приватності й правового режиму оброблення [17, 20, 52, 53].

До обмежень дослідження належить те, що монографія орієнтована переважно на автомобільний транспорт і дорожні ITS. Питання залізничного, авіаційного або морського транспорту можуть використовувати подібні принципи кіберстійкості, але мають інші нормативні рамки, іншу архітектуру керування та інші експлуатаційні сценарії. Також робота не ставить за мету розроблення нового криптографічного протоколу або конкретної програмної реалізації системи моніторингу; її завданням є формування системної основи, придатної для подальших прикладних розробок.

Ще одним обмеженням є швидка зміна технологічного середовища. Стандарти V2X, вимоги до автоматизованого водіння, архітектури програмно-

визначених автомобілів, підходи до машинного навчання та нормативні вимоги до даних продовжують розвиватися. Тому результати дослідження слід розглядати як структурну й методичну основу, яку необхідно оновлювати відповідно до нових стандартів, регуляторних рішень і практики експлуатації.

Табл. 1.3: Очікувані результати та сфери їх застосування

Результат	**Сфера застосування**	**Практичний ефект**
Систематизація понять ITS, кібербезпеки й надійності	Освіта, дослідження, стандартизація	Єдина термінологічна база
Опис компонентів і взаємозв'язків	Проєктування ITS	Менше інтеграційних помилок
Моделі ризику та надійності	Аудит, експлуатація, планування	Пріоритезація захисних заходів
Практичні рекомендації	Органи управління, оператори, розробники	Підвищення кіберстійкості сервісів

Таким чином, вступний розділ задає методичну рамку всієї монографії. Він пояснює, чому тема є актуальною, що саме досліджується, які завдання потрібно розв'язати, якими методами доцільно користуватися та в чому полягає практична цінність результатів. Подальший виклад спирається на цю рамку й послідовно розкриває роль інтелектуальних транспортних систем, кіберзагроз, надійності, даних, комунікацій і організаційних процесів у розвитку сучасного автомобільного транспорту.

2 Інтелектуальні транспортні системи як основа сучасного автомобільного транспорту

Інтелектуальні транспортні системи (ITS) перетворилися з набору окремих технічних засобів регулювання руху на комплексну цифрову основу сучасного автомобільного транспорту. Їх сутність полягає у поєднанні транспортних засобів, дорожньої інфраструктури, телекомунікаційних мереж, центрів керування, цифрових платформ і сервісів даних у єдину кіберфізичну систему. Така система не лише спостерігає за транспортними процесами, а й підтримує прийняття рішень, прогнозує розвиток дорожньої ситуації, координує учасників руху, забезпечує інформаційну взаємодію між транспортними засобами та інфраструктурою, а також створює передумови для автоматизованого й автономного керування [5, 6, 28, 30].

Для автомобільного транспорту значення ITS особливо велике, оскільки саме автомобільні перевезення найчастіше стикаються з перевантаженням вулично-дорожньої мережі, нерівномірністю попиту, аварійністю, екологічними обмеженнями, потребою у точній логістиці та необхідністю інтеграції з іншими видами мобільності. У традиційній транспортній системі значна частина рішень приймалася реактивно: світлофорні режими коригувалися після виникнення заторів, аварійні служби отримували повідомлення із запізненням, водій обирав маршрут на основі неповної інформації, а перевізник аналізував ефективність руху після завершення рейсів. ITS змінює цю логіку: дані надходять у реальному або близькому до реального часу, обробляються алгоритмами прогнозування, а керуючі впливи можуть формуватися до того, як небажана ситуація стане критичною [32, 35, 36, 61].

У межах цієї монографії ITS розглядаються не як ізольований інформаційний додаток до транспорту, а як середовище, у якому одночасно реалізуються функції безпеки руху, кібербезпеки, надійності, сервісної інтеграції та управління життєвим циклом транспортних технологій. Це важливо для подальшого аналізу кібербезпеки автомобільного транспорту, адже будь-яке підключення транспортного засобу до зовнішніх мереж, будь-який обмін V2X-повідомленнями або використання хмарного сервісу створює не лише

нові функціональні можливості, а й нові ризики [1, 9, 12, 37].

2.1 Поняття та структура інтелектуальних транспортних систем

Під інтелектуальною транспортною системою доцільно розуміти організаційно-технічну систему, у якій інформаційні, телекомунікаційні, сенсорні, навігаційні та керуючі технології застосовуються для підвищення безпеки, ефективності, доступності, екологічності та надійності транспортних процесів. У цьому визначенні принциповими є три ознаки. По-перше, ITS має системний характер і охоплює не лише окремий автомобіль або світлофорний об'єкт, а взаємодію багатьох компонентів. По-друге, ITS працює з даними як з основним ресурсом управління. По-третє, ITS орієнтована на досягнення практичного транспортного результату: скорочення затримок, зменшення аварійності, підвищення пропускної здатності, стабілізацію руху, підтримку користувацьких сервісів і забезпечення стійкості транспортної мережі [5, 7, 13, 29].

Міжнародна стандартизація підкреслює, що ITS охоплює множину сервісних доменів: керування рухом, інформаційне забезпечення подорожніх, громадський транспорт, вантажні перевезення, екстрене реагування, електронну оплату, кооперативні системи, управління даними та підтримку автоматизованого водіння [5, 6]. Тому структура ITS не може бути зведена лише до технічної схеми передавання сигналів. Вона повинна описувати і фізичні об'єкти, і функціональні процеси, і потоки даних, і відповідальність організацій, що експлуатують транспортну систему.

У загальному вигляді ITS складається з чотирьох взаємопов'язаних рівнів: польового, комунікаційного, платформного та сервісного. Польовий рівень охоплює транспортні засоби, дорожні контролери, датчики, відеокамери, радари, дорожні метеостанції, табло змінної інформації та інші пристрої, що безпосередньо взаємодіють із транспортним середовищем. Комунікаційний рівень забезпечує передавання даних між об'єктами за допомогою дротових, стільникових, короткодіапазонних або гібридних технологій. Платформний рівень відповідає за збирання, нормалізацію, зберігання, аналітику та кіберзахист даних. Сервісний рівень надає кінцеві функції: адаптивне світлофорне керування, навігацію, диспетчеризацію, прогнозування часу прибуття, попередження про небезпеки, пріоритезацію громадського транспорту, підтримку

аварійних служб і цифрові послуги для користувачів.

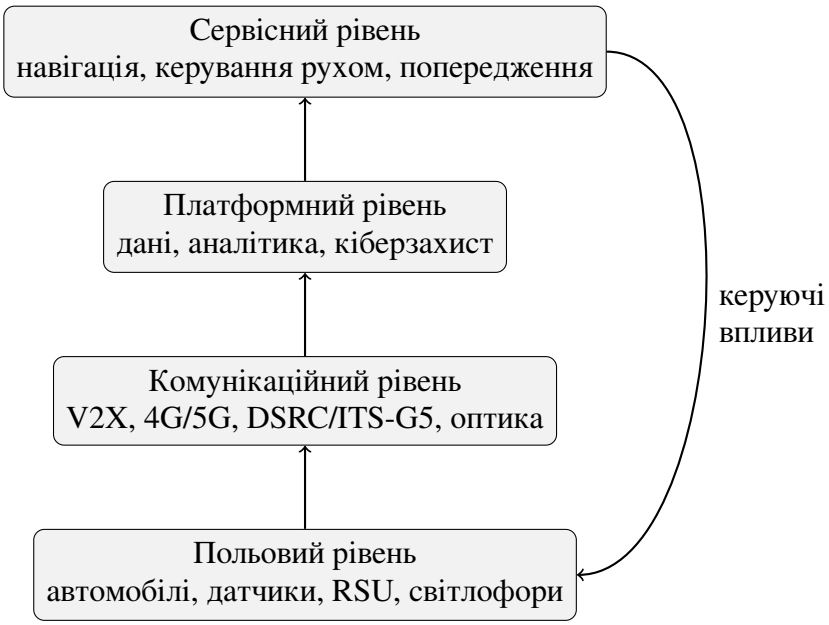

Рис. 2.1: Узагальнена багаторівнева структура інтелектуальної транспортної системи

Структура, показана на рис. 2.1, демонструє замкнений контур керування: транспортне середовище генерує дані, мережі передають їх до платформ оброблення, сервіси формують рішення, а керуючі впливи повертаються до інфраструктури або учасників руху. Такий контур можна описати як дискретну систему спостереження й керування. Якщо стан транспортної мережі у момент часу t позначити вектором $x(t)$, потік вимірювань — $y(t)$, а керуючий вплив — $u(t)$, то спрощена модель має вигляд:

$$x(t+1) = f\big(x(t), u(t), d(t)\big), \qquad y(t) = h\big(x(t)\big) + \varepsilon(t), \tag{2.1}$$

де $d(t)$ позначає зовнішні збурення, зокрема погодні умови, дорожні роботи, аварії або нерівномірний попит, а $\varepsilon(t)$ — похибки вимірювання. Завдання ITS полягає у виборі такого $u(t)$, який мінімізує затримки, ризики, витрати енергії або інший критерій ефективності.

Для транспортного коридору типовий критерій можна подати у вигляді функціонала:

$$J = \sum_{t=1}^{T} \left(\alpha D(t) + \beta Q(t) + \gamma E(t) + \delta R(t)\right), \tag{2.2}$$

де $D(t)$ — сумарна затримка, $Q(t)$ — довжина черг, $E(t)$ — екологічні або енергетичні витрати, $R(t)$ — інтегральний показник ризику, а $\alpha, \beta, \gamma, \delta$ — вагові коефіцієнти, що відображають пріоритети управління. На практиці такі критерії можуть використовуватися в адаптивному світлофорному керуванні, маршрутизації, диспетчеризації громадського транспорту або керуванні доступом до перевантажених зон.

Важливою властивістю ITS є ієрархічність. На локальному рівні система може керувати окремим перехрестям, пішохідним переходом, паркувальним майданчиком або дорожнім сегментом. На мережевому рівні вона координує групи перехресть, магістральні коридори, маршрути громадського транспорту й зони міської логістики. На стратегічному рівні ITS використовується для планування транспортної політики, оцінювання сценаріїв розвитку інфраструктури, інтеграції з екологічними обмеженнями та управління попитом на мобільність [29, 28, 34].

Ще однією ознакою сучасних ITS є кооперативність. Якщо ранні системи переважно спиралися на централізовані датчики та диспетчерські центри, то кооперативні ITS передбачають активну участь самих транспортних засобів як рухомих сенсорів і вузлів комунікаційної мережі. Автомобіль може повідомляти про свою швидкість, напрям руху, екстрене гальмування, небезпечну ділянку, слизьке покриття або перешкоду. Інші автомобілі та інфраструктурні вузли використовують ці повідомлення для підвищення ситуаційної обізнаності [14, 15, 8].

Функціонально ITS можна поділити на інформаційні, керуючі, кооперативні, аналітичні та захисні підсистеми. Інформаційні підсистеми надають користувачам дані про маршрути, час прибуття, затори, паркування, тарифи або обмеження руху. Керуючі підсистеми змінюють режими світлофорів, швидкісні обмеження, пріоритети смуг або плани об'їзду. Кооперативні підсистеми організовують обмін V2X-повідомленнями. Аналітичні підсистеми прогнозують транспортні стани, виявляють аномалії та підтримують оптимізаційні рішення. Захисні підсистеми забезпечують автентичність, цілісність, доступність і конфіденційність даних, що є критичним для безпеки дорожнього руху [11, 16, 17, 40].

З позиції надійності автомобільного транспорту ITS виконує роль інструменту раннього виявлення деградації транспортної системи. Деградація

може проявлятися у збільшенні часу поїздки, нестабільності інтервалів руху, зниженні пропускної здатності, зростанні кількості конфліктних ситуацій або відмовах інфраструктурних пристроїв. Завдяки постійному моніторингу ITS дає змогу переходити від періодичного контролю до безперервного оцінювання стану. Це наближує транспортну систему до принципів прогнозного обслуговування, які широко застосовуються в промисловості та автомобільній галузі [58, 59, 60].

Водночас розширення функцій ITS ускладнює питання відповідальності. Якщо водій отримав попередження від дорожньої інфраструктури, але не відреагував, відповідальність може залишатися за водієм. Якщо ж автоматизований транспортний засіб виконав маневр на основі помилкового V2X-повідомлення, виникає складний ланцюг відповідальності між виробником автомобіля, оператором інфраструктури, постачальником зв'язку, розробником програмного забезпечення та органом управління дорожнім рухом. Тому архітектура ITS повинна містити не лише технічні інтерфейси, а й процедури аудиту, журналювання подій, керування оновленнями, сертифікації та реагування на інциденти [3, 10, 1, 9].

Для України розвиток ITS має додатковий вимір, пов'язаний із відновленням транспортної інфраструктури, гармонізацією з європейськими підходами, підвищенням безпеки перевезень та інтеграцією в цифровий простір мобільності. Європейська політика у сфері ITS орієнтується на сумісність, безперервність сервісів, доступність транспортних даних і координацію між видами транспорту [28, 29]. Для національної практики це означає, що ITS доцільно проектувати не як набір несумісних локальних систем, а як масштабовану архітектуру з єдиними вимогами до даних, кібербезпеки, інтерфейсів і сервісної взаємодії.

2.2 Основні компоненти інтелектуальних транспортних систем: транспортні засоби, інфраструктура та центри керування

Транспортний засіб у сучасній ITS є не лише об'єктом керування, а й активним інформаційним вузлом. Він оснащується електронними блоками керування, датчиками, навігаційними приймачами, телематичними модулями, внутрішніми мережами, системами допомоги водієві, засобами діагностики та інтерфейсами зовнішнього зв'язку. У підключеному автомобілі дані про

швидкість, прискорення, положення, стан агрегатів, спрацювання систем безпеки, дорожнє оточення та поведінку водія можуть використовуватися для локального керування, передавання до хмарних сервісів або обміну з іншими учасниками руху [43, 44, 45].

З технічної точки зору автомобіль можна розглядати як кіберфізичну платформу, у якій фізичні процеси руху взаємодіють з обчислювальними процесами. Датчики вимірюють стан середовища, контролери обчислюють керуючі впливи, виконавчі механізми змінюють режим руху, а комунікаційні модулі забезпечують взаємодію з ITS. Така платформа має внутрішні обмеження за затримкою, пропускною здатністю, енергоспоживанням, надійністю та безпекою. Наприклад, попередження про екстрене гальмування має бути доставлене швидше, ніж інформаційне повідомлення про доступність паркування, а відмова датчика критичної системи потребує іншого реагування, ніж тимчасова недоступність розважального сервісу.

Усередині транспортного засобу функції розподіляються між доменами: силова установка, шасі, кузовна електроніка, системи безпеки, інформаційно-розважальні системи, телематика, ADAS та автоматизоване водіння. Традиційні архітектури використовували велику кількість окремих електронних блоків, з'єднаних мережами CAN, LIN, FlexRay або Ethernet. Нові архітектури поступово переходять до доменних і зональних контролерів, сервісно-орієнтованого програмного забезпечення та централізованіших обчислювальних платформ [49, 50, 51]. Це підвищує гнучкість оновлень, але збільшує значення кібербезпеки та керування конфігураціями.

Дорожня інфраструктура ITS охоплює стаціонарні об'єкти, які спостерігають за рухом, передають інформацію або здійснюють керуючий вплив. До них належать світлофорні контролери, дорожні датчики, відеокамери, радари, лідари, детектори транспорту, метеостанції, табло змінної інформації, дорожні бортові пристрої RSU, автоматизовані пункти вагового контролю, паркувальні сенсори, зарядна інфраструктура для електромобілів і обладнання пріоритету громадського транспорту. На відміну від транспортного засобу, інфраструктурний компонент часто має триваліший життєвий цикл і експлуатується різними організаціями, тому проблема сумісності поколінь обладнання є особливо актуальною [31, 7, 13].

Центр керування рухом є організаційним і технологічним ядром ITS.

Він збирає дані з польових пристроїв, транспортних засобів, навігаційних платформ, операторів громадського транспорту, аварійних служб і зовнішніх джерел; аналізує ці дані; формує рішення; координує операторів; забезпечує інформування користувачів. У великих містах центр керування може функціонувати цілодобово й мати спеціалізовані робочі місця для моніторингу магістралей, перехресть, тунелів, громадського транспорту, дорожніх робіт, аварійних подій та кіберінцидентів.

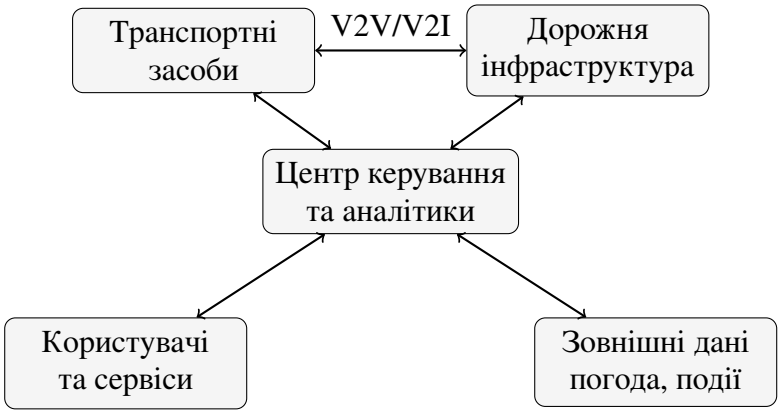

Рис. 2.2: Взаємодія ключових компонентів ITS

На рис. 2.2 показано, що компоненти ITS взаємодіють не лінійно, а мережево. Транспортний засіб може отримувати інформацію безпосередньо від іншого автомобіля, від дорожнього пристрою, від центру керування або від цифрового сервісу. Інфраструктура може працювати автономно на локальному рівні, але також передавати дані до центральної платформи. Центр керування може формувати команди для світлофорних контролерів, інформаційні повідомлення для водіїв і запити до аварійних служб.

Взаємодія компонентів потребує узгоджених інтерфейсів. Якщо різні виробники датчиків, контролерів і транспортних засобів використовують несумісні формати, то система втрачає масштабованість. Саме тому стандарти архітектури ITS, станцій ITS і комунікаційних сервісів мають фундаментальне значення [6, 13, 22]. Вони визначають не лише фізичні канали зв'язку, а й логіку адресації, мережеві сервіси, безпекові заголовки, сертифікати та прикладні повідомлення.

Одним із ключових параметрів для оцінювання роботи компонентів ITS є затримка передавання й оброблення інформації. Нехай T_s — час сенсорного вимірювання, T_c — час передавання каналом зв'язку, T_p — час оброблення на платформі, T_a — час доставки або виконання керуючого впливу. Тоді повна

затримка контуру становить:

$$T_{ITS} = T_s + T_c + T_p + T_a. \tag{2.3}$$

Для критичних застосувань має виконуватися умова $T_{ITS} \leq T_{max}$, де T_{max} визначається сценарієм безпеки. Наприклад, повідомлення про небезпечне гальмування або перешкоду на смузі має значно жорсткіші часові вимоги, ніж статистичне оновлення карти заторів.

Інфраструктурні датчики відрізняються за точністю, вартістю та умовами застосування. Індукційні петлі надійні для підрахунку транспортних засобів, але потребують втручання в дорожнє покриття. Відеокамери надають багату інформацію, проте залежать від освітлення, погодних умов і алгоритмів комп'ютерного зору. Радари краще працюють у складну погоду, але можуть мати нижчу семантичну деталізацію. Лідари забезпечують точну просторову картину, однак дорожчі й чутливі до забруднення оптики. Комбінування різних джерел зменшує ймовірність помилки, але потребує процедур синхронізації, калібрування та оцінювання достовірності [31, 45, 46].

Надійність ITS залежить від резервування й деградаційних режимів. Якщо один детектор на перехресті вийшов з ладу, система може тимчасово використовувати дані відеоаналітики або історичні профілі інтенсивності. Якщо недоступний стільниковий канал, критичні локальні функції мають зберігатися через короткодіапазонний зв'язок або автономне керування контролером. Якщо центр керування недоступний, світлофорні об'єкти не повинні переходити у хаотичний режим, а мають використовувати безпечні локальні плани. Таким чином, ITS повинна проектуватися за принципом контрольованої деградації, коли відмова окремого компонента не призводить до втрати всієї транспортної функції.

Окреме місце займають центри оброблення даних і хмарні сервіси. Вони дають змогу накопичувати історичні дані, навчати моделі прогнозування, виконувати масштабну аналітику, оновлювати програмне забезпечення, підтримувати цифрові двійники транспортної мережі та інтегрувати сервіси сторонніх постачальників. Однак винесення функцій у хмару підвищує залежність від каналів зв'язку, політик доступу, захисту персональних даних і процедур реагування на інциденти [52, 53, 54, 11].

Для автомобільного транспорту особливо важливо, щоб центр керування

не замінював локальну безпеку транспортного засобу. Автомобіль повинен мати власні механізми перевірки достовірності повідомлень, оцінювання ситуації та безпечного переходу в мінімально ризиковий стан. Цей принцип узгоджується з підходами функціональної безпеки, безпеки передбачуваної функціональності та кібербезпеки автомобільних систем [2, 4, 1]. ITS може підвищувати ситуаційну обізнаність, але не повинна створювати єдину точку небезпечної залежності.

Ефективність взаємодії компонентів ITS можна оцінювати через показник доступності сервісу:

$$A = \frac{MTBF}{MTBF + MTTR}, \tag{2.4}$$

де $MTBF$ — середній час між відмовами, а $MTTR$ — середній час відновлення. Для критичних сервісів, таких як керування тунелем, екстрене попередження або координація аварійних служб, потрібні високі значення доступності, що досягаються резервуванням каналів, дублюванням серверів, моніторингом стану, регламентованим технічним обслуговуванням і кіберзахистом.

Організаційно компоненти ITS повинні підтримувати розподіл ролей. Оператор дороги відповідає за інфраструктурні пристрої та безпечну організацію руху. Міський або регіональний центр керування відповідає за координацію й політику керування. Виробник транспортного засобу відповідає за безпеку автомобільної платформи та оновлення. Постачальник зв'язку забезпечує доступність мережевих сервісів. Постачальник цифрової платформи відповідає за оброблення даних, інтерфейси й захист сервісів. Без визначення цих ролей технічна архітектура може працювати нестабільно навіть за наявності якісного обладнання.

2.3 Комунікаційні технології в інтелектуальних транспортних системах

Комунікації є основою кооперативних ITS, оскільки саме вони перетворюють окремі транспортні засоби та інфраструктурні об'єкти на взаємодіючу систему. У найпростішому випадку автомобіль отримує інформацію від навігаційного сервісу через стільникову мережу. У складнішому випадку транспортні засоби безпосередньо обмінюються повідомленнями про положення,

швидкість, напрям руху, гальмування або небезпечні події. Узагальнено такі взаємодії позначаються як V2X, а їх основними різновидами є V2V, V2I, V2N, V2P і V2G [33, 26, 27, 8].

V2V означає зв'язок між транспортними засобами. Його головна перевага полягає в можливості швидкого локального обміну інформацією без обов'язкового проходження через центральну інфраструктуру. Це важливо для попередження про екстрене гальмування, небезпечну зміну смуги, зіткнення на перехресті, обмежену видимість або формування колон руху. V2I описує взаємодію автомобіля з дорожньою інфраструктурою: світлофорами, RSU, дорожніми знаками, пунктами оплати, паркувальними системами або зарядними станціями. V2N охоплює зв'язок із хмарними й операторськими сервісами, V2P — взаємодію з пішоходами та велосипедистами через мобільні пристрої або спеціалізовані маяки, а V2G — зв'язок електромобіля з енергетичною мережею.

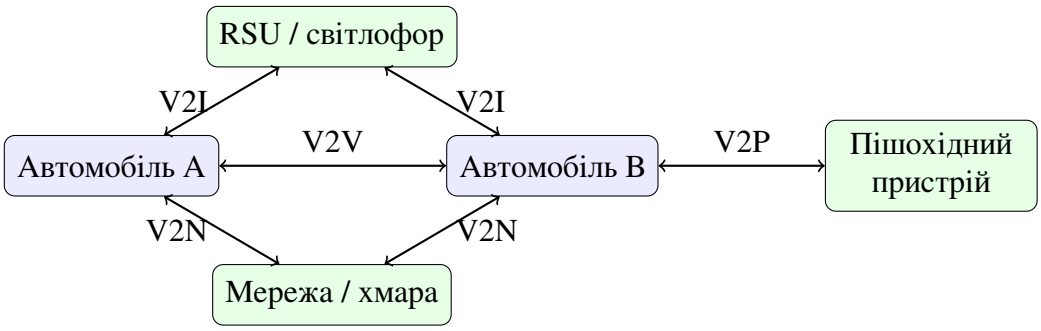

Рис. 2.3: Основні типи V2X-взаємодії в інтелектуальних транспортних системах

На практиці V2X може реалізовуватися різними технологіями. До короткодіапазонних технологій належать IEEE 802.11p/ITS-G5 та споріднені рішення, що забезпечують прямий обмін повідомленнями у виділених частотних діапазонах. До стільникових технологій належать C-V2X та подальші розвитки в межах 4G/5G, які підтримують як прямий sidelink-зв'язок, так і взаємодію через мережеву інфраструктуру [23, 22, 24, 25]. Гібридна модель передбачає, що критичні локальні повідомлення передаються короткодіапазонним або прямим каналом, а широкомасштабні сервіси, оновлення карт і хмарна аналітика використовують стільникові або дротові мережі [8, 18, 19].

Ключовими параметрами комунікацій ITS є затримка, надійність доставки, дальність, пропускна здатність, масштабованість, стійкість до завад і захищеність. Для повідомлення кооперативної обізнаності важливо регулярно

передавати базовий стан транспортного засобу. Для повідомлення про небезпечну подію важливо забезпечити швидке поширення в релевантній географічній зоні. Для завантаження оновлення програмного забезпечення потрібна висока пропускна здатність і контроль цілісності, але затримка в мілісекундах не є критичною. Таким чином, одна технологія не може оптимально покрити всі сценарії, тому архітектура ITS повинна підтримувати вибір каналу відповідно до вимог сервісу.

Нехай імовірність успішної доставки одного повідомлення дорівнює p, а повідомлення дублюється через n незалежних каналів або повторів. Тоді ймовірність того, що хоча б одна копія буде доставлена, можна оцінити як:

$$P_{delivery} = 1 - (1 - p)^n. \tag{2.5}$$

Ця формула пояснює, чому для критичних попереджень застосовують повторення, резервування каналів або географічне широкомовлення. Водночас надмірне дублювання збільшує навантаження на радіоканал, тому система повинна балансувати між надійністю та перевантаженням мережі.

Типовими прикладними повідомленнями в європейській C-ITS-архітектурі є кооперативне повідомлення про стан (CAM) і децентралізоване повідомлення про подію (DENM). CAM передає регулярну інформацію про стан транспортного засобу, тоді як DENM використовується для повідомлень про події, наприклад аварію, дорожні роботи, небезпечну ділянку або раптове гальмування [14, 15]. Для таких повідомлень важлива не лише доставка, а й правильне визначення релевантної зони: водій або автоматизована система повинні отримувати попередження тоді, коли воно впливає на їх траєкторію, але не бути перевантаженими нерелевантними сигналами.

Безпека V2X-комунікацій є критичною, оскільки помилкове або підроблене повідомлення може безпосередньо вплинути на поведінку водія чи автоматизованої системи. Архітектури безпеки передбачають автентифікацію повідомлень, цифрові підписи, сертифікати, псевдоніми для захисту приватності, керування довірою, відкликання сертифікатів і захист від повторного відтворення повідомлень [16, 17, 20, 21]. Проте безпекові механізми не повинні створювати надмірну затримку, тому криптографічні операції мають бути оптимізовані для умов транспортної мережі.

Для V2X характерні специфічні загрози: підроблення координат, атаки

Сивілли, коли один вузол видає себе за багато транспортних засобів, придушення каналу, поширення неправдивих повідомлень про події, відстеження траєкторії користувача, компрометація RSU або атаки на центр сертифікації. Огляди безпеки V2X показують, що захист має поєднувати криптографічні методи, виявлення аномалій, перевірку правдоподібності фізичних параметрів і управління довірою [40, 41, 42, 39].

Модель правдоподібності повідомлення може спиратися на кінематичні обмеження. Якщо транспортний засіб повідомляє положення $s(t)$ і швидкість $v(t)$, то прогнозоване положення через інтервал Δt можна наближено визначити як:

$$\hat{s}(t + \Delta t) = s(t) + v(t)\Delta t + \frac{1}{2}a(t)\Delta t^2. \tag{2.6}$$

Якщо отримане наступне положення істотно відрізняється від $\hat{s}$ і ця різниця не пояснюється допустимим прискоренням, похибкою GPS або маневром, повідомлення може бути позначене як підозріле. Такі перевірки не замінюють криптографію, але доповнюють її семантичним контролем.

Стільникові V2X-сервіси відкривають можливість інтеграції ITS із мережевими зрізами, периферійними обчисленнями та хмарними платформами. Периферійні обчислення дають змогу обробляти дані ближче до дороги, зменшуючи затримку для сервісів, що потребують швидкої реакції. Наприклад, вузол периферійні обчислення біля транспортного коридору може агрегувати дані з RSU, камер і транспортних засобів, виявляти небезпечні події та передавати попередження локальним учасникам руху швидше, ніж віддалений центр оброблення даних. Водночас така архітектура збільшує кількість вузлів, які потрібно адмініструвати й захищати.

Гібридні комунікації є найбільш реалістичним напрямом розвитку ITS. У міському середовищі один і той самий автомобіль може одночасно використовувати GNSS, стільникову мережу, Wi-Fi, Bluetooth, V2X-радіомодуль і внутрішні автомобільні мережі. Завдання архітектури полягає у тому, щоб вибір каналу був керованим і передбачуваним. Для критичних повідомлень пріоритетом є затримка й надійність, для мультимедійних сервісів — пропускна здатність, для оновлень — цілісність і контроль версій, для персональних сервісів — приватність і згода користувача [3, 52, 54].

Отже, V2V, V2I та V2X не слід розглядати лише як технології зв'язку. Вони формують новий спосіб організації автомобільного транспорту, у яко-

му інформація про дорожню ситуацію поширюється між учасниками руху, інфраструктурою та цифровими платформами. Це підвищує потенціал безпеки й ефективності, але водночас робить кібербезпеку, стандартизацію та управління довірою невід'ємними умовами функціонування ITS.

2.4 Роль даних і цифрових сервісів в управлінні транспортом

Дані є центральним ресурсом ITS. Якщо традиційна транспортна інженерія переважно спиралася на періодичні обстеження інтенсивності, ручні підрахунки, статистику ДТП і вибіркові вимірювання часу поїздки, то сучасна ITS використовує безперервні потоки даних із транспортних засобів, інфраструктури, мобільних пристроїв, систем оплати, навігаційних сервісів, камер, датчиків навколишнього середовища та адміністративних реєстрів. Саме ці потоки створюють основу для оперативного керування, прогнозування та стратегічного планування [32, 34, 61].

Дані ITS можна класифікувати за джерелом, часовою природою, просторовою прив'язкою, ступенем персоналізації та призначенням. За джерелом розрізняють дані транспортних засобів, інфраструктурні дані, користувацькі дані, дані операторів перевезень, зовнішні дані про погоду й події, а також нормативно-довідкові дані. За часовою природою виділяють потокові дані реального часу, історичні архіви, прогнозні дані та планові дані. За просторовою прив'язкою дані можуть належати до точки, сегмента дороги, маршруту, транспортної зони або всієї мережі. Така класифікація потрібна для вибору методів оброблення, політик доступу та вимог до якості.

Якість даних безпосередньо впливає на якість керування. Неповні, застарілі або помилкові дані можуть призвести до неправильного світлофорного плану, хибного маршруту, некоректного прогнозу часу прибуття або зайвого попередження водія. Тому в ITS використовують показники повноти, точності, своєчасності, узгодженості, достовірності та просторової деталізації. Інтегральний показник якості набору даних можна подати як зважену суму:

$$Q_d = w_1 C + w_2 A + w_3 T + w_4 S + w_5 V, \tag{2.7}$$

де C — повнота, A — точність, T — своєчасність, S — узгодженість, V — перевіреність, а w_i — вагові коефіцієнти. Якщо Q_d нижчий за встановлений

поріг, дані можуть використовуватися лише для довідкової аналітики, але не для критичного керування.

Цифрові сервіси ITS перетворюють дані на практичну цінність. До таких сервісів належать прогнозування заторів, адаптивне світлофорне керування, інформування про час прибуття громадського транспорту, керування паркуванням, електронна оплата, динамічне ціноутворення, пріоритет аварійних і маршрутних транспортних засобів, управління вантажними коридорами, контроль екологічних зон, попередження про небезпеки та підтримка мультимодальних поїздок. Усі вони базуються на однаковій логіці: зібрати дані, перевірити їх якість, побудувати оцінку стану, спрогнозувати розвиток ситуації, сформувати рекомендацію або керуючу дію.

Рис. 2.4: Цикл перетворення даних ITS на керуючі рішення

На рис. 2.4 показано, що дані мають цінність лише в замкненому циклі. Якщо система збирає великі обсяги інформації, але не використовує їх для прийняття рішень, вона залишається пасивною. Якщо система приймає рішення без контролю якості даних, вона стає небезпечною. Якщо відсутній зворотний зв'язок, неможливо оцінити, чи був керуючий вплив ефективним. Тому сучасна ITS повинна мати не тільки сховище даних, а й процедури валідації, аналітики, моніторингу результатів і безперервного вдосконалення.

Прогнозування транспортного потоку є одним із найважливіших напрямів використання даних. Класичні моделі спиралися на співвідношення між інтенсивністю, щільністю та швидкістю. Сучасні підходи використовують машинне навчання, глибокі нейронні мережі, рекурентні моделі, графові структури дорожньої мережі та дані з багатьох джерел [35, 36, 47, 48]. Для ділянки дороги базовий зв'язок між інтенсивністю q, щільністю k і середньою швидкістю v описується формулою:

$$q = k \cdot v. \tag{2.8}$$

Хоча ця формула є простою, вона залишається фундаментальною для інтерпретації даних ITS: зниження швидкості при зростанні щільності може свідчити про наближення до нестабільного режиму, а різке падіння інтенсивності при високій щільності — про формування затору.

Для цифрових сервісів важливим є прогноз часу поїздки. Якщо маршрут складається з m сегментів довжиною l_i, а прогнозована швидкість на сегменті дорівнює $v_i(t)$, то очікуваний час руху можна оцінити як:

$$\hat{T}_{route}(t) = \sum_{i=1}^{m} \frac{l_i}{v_i(t)} + \sum_{j=1}^{r} \tau_j(t), \tag{2.9}$$

де $\tau_j(t)$ — очікувані затримки на перехрестях, пунктах оплати, зупинках або інших контрольних точках. У реальних системах до цієї оцінки додаються ймовірнісні інтервали, що відображають невизначеність прогнозу.

Дані ITS також підтримують управління попитом на транспорт. Навігаційні сервіси можуть розподіляти потоки між альтернативними маршрутами, паркувальні сервіси — зменшувати холостий пробіг у пошуках місця, сервіси громадського транспорту — підвищувати передбачуваність поїздки, а мультимодальні платформи — поєднувати автомобіль, громадський транспорт, мікромобільність і пішохідні переміщення. При цьому виникає ризик локальної оптимізації: якщо всі навігаційні сервіси одночасно перенаправляють водіїв на другорядні вулиці, це може погіршити безпеку й якість життя в житлових районах. Тому цифрові сервіси мають узгоджуватися з політикою міського управління, а не лише з індивідуальним мінімумом часу поїздки.

Особливої уваги потребують персональні дані. Підключені автомобілі та мобільні сервіси можуть обробляти геолокацію, ідентифікатори пристроїв, стиль водіння, історію маршрутів, платіжну інформацію та дані про поведінку користувача. Європейські підходи до захисту даних вимагають правової підстави оброблення, мінімізації даних, прозорості, обмеження мети, захисту за замовчуванням і контролю прав суб'єкта даних [53, 52, 54]. Для ITS це означає, що технічна архітектура повинна містити механізми анонімізації, псевдонімізації, керування згодою, розмежування доступу та журналювання операцій з даними.

Кібербезпека даних ITS має три основні виміри: цілісність, доступність і конфіденційність. Цілісність потрібна, щоб керуючі рішення базувалися на

незміненій інформації. Доступність потрібна, щоб критичні сервіси не припиняли роботу під час відмов або атак. Конфіденційність потрібна для захисту користувачів і комерційно чутливої інформації. У контексті автомобільного транспорту особливо небезпечним є порушення цілісності, коли атакувальник не просто викрадає дані, а змінює їх так, щоб система прийняла неправильне рішення [11, 1, 37, 38].

Виявлення аномалій у даних є одним із практичних інструментів захисту та підвищення надійності. Аномалією може бути неможлива швидкість, стрибок координат, різка зміна інтенсивності без фізичного пояснення, несумісність показників сусідніх датчиків або повідомлення від вузла з підозрілою поведінкою. Прості статистичні методи використовують порогові значення, тоді як складніші підходи застосовують машинне навчання, часові ряди й графові моделі [55, 56, 57]. Наприклад, нормалізоване відхилення вимірювання можна подати як:

$$z = \frac{x - \mu}{\sigma}, \tag{2.10}$$

де x — поточне значення, μ — очікуване середнє, σ — стандартне відхилення. Якщо $|z|$ перевищує встановлений поріг, система ініціює додаткову перевірку.

Цифрові сервіси також змінюють економіку транспортного управління. Дані стають активом, який може використовуватися для планування інвестицій, оцінювання ефективності ремонтів, оптимізації маршрутів перевізників, страхових продуктів, прогнозного технічного обслуговування та розвитку нових сервісів мобільності. Однак економічна цінність даних не повинна суперечити суспільним цілям: безпеці, недискримінації, доступності транспорту й захисту приватності. Саме тому нормативні акти щодо доступу до даних і розгортання ITS підкреслюють необхідність прозорих правил обміну та сумісності сервісів [28, 54, 29].

Для центрів керування дані дають змогу переходити від ручного диспетчерського спостереження до ситуаційної аналітики. Оператор повинен бачити не просто десятки відеопотоків, а пріоритезовані події: аварія з високим впливом на мережу, зростання затримки на маршруті громадського транспорту, відмова контролера, кібераномалія, небезпечна погодна зона. Це зменшує когнітивне навантаження й підвищує швидкість реагування. Водночас остаточні рішення у критичних ситуаціях часто залишаються за людиною, тому інтерфейси ITS мають бути зрозумілими, пояснюваними й придатними

для аудиту.

У перспективі роль даних зростатиме через поширення автоматизованих транспортних засобів, цифрових двійників, периферійні обчислення, федеративного навчання та інтеграції транспортних і енергетичних систем. Автомобільний транспорт ставатиме частиною ширшої цифрової екосистеми міста, де рішення про рух пов'язані з екологічними обмеженнями, енергоспоживанням, безпекою громадського простору та індивідуальними потребами користувачів. Тому дані ITS слід розглядати не лише як технічний ресурс, а як об'єкт управління, правового регулювання, кіберзахисту та етичної відповідальності.

Підсумовуючи, інтелектуальні транспортні системи є основою сучасного автомобільного транспорту тому, що вони поєднують фізичну мобільність із цифровим керуванням. Їх структура охоплює транспортні засоби, інфраструктуру, центри керування, комунікаційні мережі та сервіси даних. Їх ефективність залежить від стандартизованих архітектур, надійних V2X-комунікацій, якісних даних, кібербезпеки та узгодженої організації відповідальності. Саме на цій основі в наступних розділах доцільно аналізувати кіберзагрози, методи захисту та вимоги до надійності автомобільного транспорту в ITS.

2.5 Практичні вимоги до впровадження інтелектуальних транспортних систем в автомобільному транспорті

Для того щоб ITS стала реальною основою автомобільного транспорту, недостатньо встановити окремі датчики або створити диспетчерський екран. Потрібна послідовна програма впровадження, у якій технічні рішення пов'язані з транспортними цілями, нормативними вимогами, експлуатаційними процесами та фінансовою моделлю. Першим етапом є інвентаризація транспортної мережі: визначення критичних перехресть, аварійно небезпечних ділянок, коридорів громадського транспорту, вантажних маршрутів, зон із нестачею паркування, місць концентрації пішоходів і ділянок з нестабільним зв'язком. Без такої інвентаризації ITS ризикує перетворитися на фрагментарний набір обладнання, яке не вирішує головних проблем мережі.

Другим етапом є формування цільової архітектури. Вона повинна відповідати на питання, які дані збираються, де вони обробляються, хто має до них доступ, які сервіси мають пріоритет, які функції залишаються локальни-

ми, а які передаються до центру керування або хмари. Для автомобільного транспорту особливо важливо відокремлювати критичні функції безпеки від інформаційно-довідкових сервісів. Наприклад, попередження про небезпечну подію, керування світлофором на аварійному маршруті та координація екстрених служб повинні мати вищий пріоритет, ніж статистична аналітика або інформація про комерційні сервіси поблизу маршруту.

Третім етапом є забезпечення сумісності. ITS зазвичай розвивається поступово: частина світлофорів модернізується раніше, частина транспортних засобів уже має V2X-модулі, інші працюють лише через мобільний зв'язок, а деякі датчики залишаються автономними. Тому архітектура повинна підтримувати роботу в умовах неоднорідності. Практичним принципом є відкритість інтерфейсів і документованість форматів даних. Якщо місто або оператор дороги залежить від одного закритого постачальника, подальше масштабування стає дорогим і технічно ризикованим.

Четвертим етапом є експлуатаційна готовність. ITS потребує не лише монтажу, а й постійного обслуговування: калібрування датчиків, перевірки каналів зв'язку, оновлення програмного забезпечення, аналізу журналів подій, навчання операторів, резервного копіювання конфігурацій і тестування планів відновлення. Для цього доцільно запроваджувати регламенти життєвого циклу, подібні до тих, що застосовуються в автомобільній кібербезпеці та інженерії оновлень [1, 3, 9, 10]. Система, яка не має регламенту супроводу, швидко втрачає точність і довіру користувачів.

П'ятим етапом є оцінювання результативності. ITS повинна мати вимірювані показники ефективності: середній час поїздки, варіативність часу поїздки, затримка на перехрестях, кількість зупинок, регулярність громадського транспорту, час реагування на інциденти, кількість аварійних ситуацій, доступність сервісів, рівень помилкових спрацювань і задоволеність користувачів. Якщо до та після впровадження не вимірюються однакові показники, неможливо довести, що система дала очікуваний ефект.

Інтегральний ефект ITS можна подати як порівняння базового та впровадженого сценаріїв:

$$E_{ITS} = \frac{K_0 - K_1}{K_0} \cdot 100\%, \tag{2.11}$$

де K_0 — значення небажаного показника до впровадження, наприклад середня затримка або кількість інцидентів, а K_1 — значення після впровадження.

Для комплексної оцінки замість одного показника можна використовувати зважений індекс, що поєднує транспортну, безпекову, екологічну та сервісну складові.

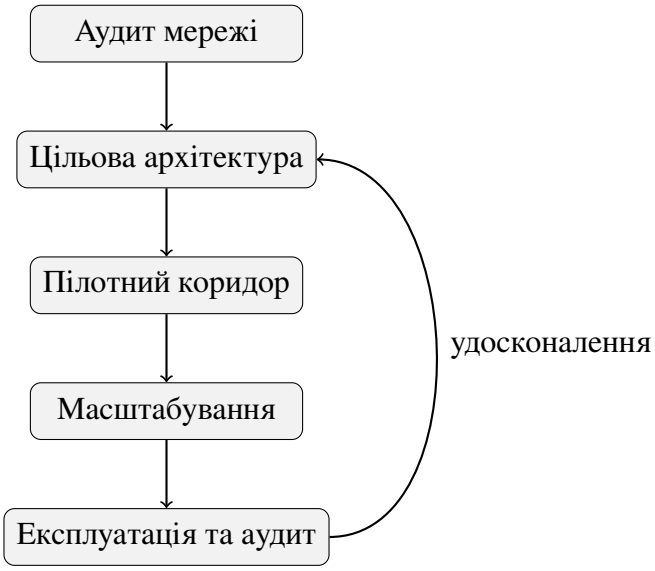

Рис. 2.5: Життєвий цикл практичного впровадження ITS

Пілотне впровадження доцільно починати з транспортного коридору, де проблема є достатньо суттєвою, а ефект можна швидко виміряти. Це може бути магістраль із заторами, маршрут громадського транспорту з нерегулярним рухом, ділянка з високою аварійністю або логістичний під'їзд до промислової зони. Пілот повинен включати не лише обладнання, а й методику оцінювання, навчання персоналу, сценарії відмов, кібербезпекові перевірки та план масштабування. Якщо пілотний проєкт не містить плану переходу до мережевого рівня, його результати часто залишаються локальними.

Управління ризиками є наскрізною вимогою для впровадження ITS. Ризики можуть бути технічними, організаційними, фінансовими, правовими та кібербезпековими. Технічний ризик полягає у несумісності обладнання або недостатній якості даних. Організаційний ризик виникає, коли між власником дороги, поліцією, перевізником, оператором зв'язку та міським центром немає узгоджених процедур. Фінансовий ризик пов'язаний з недооцінкою витрат на експлуатацію. Правовий ризик стосується персональних даних, відповідальності та доступу до інформації. Кібербезпековий ризик охоплює можливість несанкціонованого доступу, зміни даних або порушення доступності сервісів [11, 52, 37].

Для автомобільного транспорту перспективним є створення цифрового

двійника транспортної мережі. Цифровий двійник поєднує карту, поточні дані руху, моделі попиту, характеристики інфраструктури, сценарії керування та історичні архіви. Він дає змогу перевіряти зміни світлофорних режимів, організацію об'їздів, вплив дорожніх робіт, наслідки обмеження швидкості або введення пріоритету громадського транспорту до фактичного застосування на дорозі. Такий підхід зменшує ризик експериментів у реальному русі й підтримує доказове управління.

Не менш важливою є підготовка персоналу. Оператор ITS повинен розуміти не тільки інтерфейс програмного комплексу, а й транспортну логіку подій, обмеження датчиків, значення показників, процедури реагування та ознаки кіберінцидентів. Інженер з експлуатації повинен уміти діагностувати відмови польового обладнання й каналів зв'язку. Аналітик повинен відрізняти статистичну закономірність від артефакту даних. Керівник транспортної системи повинен бачити зв'язок між цифровими сервісами, безпекою, бюджетом і суспільною довірою.

Упровадження ITS має бути поетапним, але архітектурно цілісним. На першому рівні можна забезпечити моніторинг і базове інформування. На другому — адаптивне керування окремими об'єктами. На третьому — мережеву координацію та інтеграцію громадського транспорту. На четвертому — кооперативні V2X-сервіси. На п'ятому — підтримку автоматизованого руху й цифрових двійників. Кожний наступний рівень спирається на якість попереднього: неможливо надійно впровадити V2X, якщо базові дані про інфраструктуру неточні, а центр керування не має процедур реагування.

Отже, практичне значення ITS полягає не тільки у технологічній модернізації, а й у зміні культури управління автомобільним транспортом. Система стає вимірюваною, прогнозованою, сервісно орієнтованою та здатною до адаптації. Проте така перевага досягається лише за умови стандартизованої архітектури, якісних даних, захищених комунікацій, експлуатаційної дисципліни та постійного оцінювання результатів.

2.6 Узагальнення архітектурних принципів інтелектуальних транспортних систем

Розгляд ITS як основи сучасного автомобільного транспорту дає змогу сформулювати низку архітектурних принципів, які мають практичне значе-

ння для подальшого проектування, експлуатації та захисту систем. Перший принцип — системність. Кожний елемент, від бортового датчика до центру керування, повинен розглядатися не ізольовано, а як частина єдиного контуру спостереження, аналізу й керування. Якщо дані з автомобіля не можуть бути коректно інтерпретовані інфраструктурою, а центр керування не має механізму впливу на дорожню ситуацію, то інтелектуальність системи залишається декларативною.

Другий принцип — пріоритет безпеки. ITS має підвищувати безпеку руху, а не створювати додаткові неконтрольовані залежності. Тому будь-який цифровий сервіс повинен мати визначений рівень критичності, допустиму затримку, вимоги до достовірності даних і безпечний режим деградації. Для інформаційного сервісу достатньо попередити користувача про обмежену точність даних. Для сервісу, що впливає на рух, потрібні перевірка повідомлень, резервування джерел і контроль наслідків керуючого впливу.

Третій принцип — інтероперабельність. Автомобільний транспорт є відкритою системою: дорогами користуються транспортні засоби різних виробників, перевізники застосовують різні платформи, а міста поступово модернізують інфраструктуру. Через це ITS повинна підтримувати стандартизовані повідомлення, документовані інтерфейси, сумісні профілі безпеки та можливість інтеграції нових сервісів без повної заміни наявних компонентів [5, 6, 13].

Четвертий принцип — керованість даних. Дані повинні мати власний життєвий цикл: створення, передавання, перевірка, зберігання, використання, архівування та видалення. Для кожного етапу необхідно визначити відповідального суб'єкта, допустиму мету оброблення, строк зберігання, рівень доступу й вимоги до захисту. Без такого підходу накопичення великих масивів інформації не гарантує кращого управління, а лише збільшує ризики помилок, витоків і правової невизначеності.

П'ятий принцип — доказовість рішень. ITS повинна не тільки генерувати рекомендації, а й надавати можливість перевірити, на яких даних і правилах вони ґрунтувалися. Це особливо важливо для спірних ситуацій: зміни організації руху, автоматичного пріоритету, обмеження доступу, реагування на аварії або кіберінциденти. Журналювання подій, часові мітки, версії алгоритмів і збереження критичних повідомлень формують основу технічного аудиту.

Шостий принцип — адаптивність. Транспортна система змінюється під впливом попиту, погоди, дорожніх робіт, аварій, сезонності, поведінки користувачів і розвитку міста. Тому ITS не може бути статичною. Вона повинна підтримувати оновлення моделей, зміну правил керування, додавання нових джерел даних, масштабування обчислювальних ресурсів і перегляд політик доступу. При цьому адаптивність не повинна суперечити стабільності: кожне оновлення має проходити перевірку, документування та контроль сумісності [3, 10].

Сьомий принцип — кіберстійкість. Оскільки ITS є кіберфізичною системою, порушення цифрового компонента може мати фізичні наслідки на дорозі. Кіберстійкість означає здатність не лише запобігати атакам, а й виявляти їх, обмежувати поширення, підтримувати критичні функції та відновлювати нормальну роботу. Для цього потрібні сегментація мереж, керування ідентичностями, криптографічний захист, моніторинг аномалій, резервні сценарії та регулярне навчання персоналу [11, 1, 16].

У підсумку ITS можна представити як багатокритеріальну систему, у якій технічна ефективність повинна узгоджуватися з безпекою, правом, економікою та довірою користувачів. Узагальнений показник зрілості ITS можна описати формально:

$$M_{ITS} = \lambda_1 I + \lambda_2 S + \lambda_3 D + \lambda_4 C + \lambda_5 R, \tag{2.12}$$

де I — рівень інтероперабельності, S — рівень безпеки, D — якість керування даними, C — спроможність до координації, R — надійність і стійкість, а λ_i — ваги, визначені цілями конкретної транспортної системи. Така модель не замінює детального аудиту, але допомагає структурувати вимоги та порівнювати альтернативні сценарії розвитку.

Отже, другий розділ показує, що інтелектуальні транспортні системи є не допоміжним цифровим шаром, а базовою архітектурою сучасного автомобільного транспорту. Вони забезпечують перехід від розрізненого керування до мережевої координації, від епізодичних вимірювань до потокових даних, від локальних рішень до сервісної інтеграції, від реактивного реагування до прогнозного управління. Саме тому питання кібербезпеки, надійності та стандартизації ITS мають розглядатися як невід'ємна частина розвитку автомобільного транспорту.

3 Кіберзагрози автомобільному транспорту в інтелектуальних транспортних системах

Розвиток інтелектуальних транспортних систем істотно розширює функціональні можливості автомобільного транспорту, однак одночасно формує складне середовище кіберризиків. Якщо традиційна безпека автомобіля переважно пов'язувалася з механічною справністю, поведінкою водія, дорожніми умовами та конструктивними характеристиками, то в ITS до цих чинників додаються програмне забезпечення, телекомунікації, цифрові ідентичності, хмарні сервіси, V2X-повідомлення, центри керування, мобільні застосунки та великі масиви телематичних даних. У такому середовищі кіберзагроза може перетворитися на фізичну небезпеку, порушити дорожній рух, спричинити витік персональних даних або знизити довіру до цифрових сервісів мобільності [1, 9, 11, 37].

Особливість кіберзагроз для автомобільного транспорту полягає у поєднанні інформаційних і фізичних наслідків. Атака на звичайну інформаційну систему часто оцінюється через втрату конфіденційності, цілісності або доступності даних. В автомобільному транспорті ці самі порушення можуть вплинути на керування транспортним засобом, роботу світлофорів, маршрутизацію потоків, реагування аварійних служб або поведінку автоматизованих систем допомоги водієві. Тому кібербезпека ITS має розглядатися як складова загальної безпеки та надійності транспортної системи [2, 4, 40, 39].

У цьому розділі кіберзагрози розглядаються за п'ятьма напрямами: загальна класифікація, атаки на бортові системи автомобіля, загрози для каналів V2X, атаки на дорожню інфраструктуру й центри керування, а також ризики витоку персональних і телематичних даних. Така структура відповідає архітектурі ITS, у якій транспортний засіб, комунікаційне середовище, інфраструктура, платформи керування та дані утворюють єдиний ланцюг довіри. Порушення будь-якої ланки може вплинути на всю систему.

3.1 Класифікація кіберзагроз

Класифікація кіберзагроз є необхідною умовою їх аналізу, оцінювання та пріоритезації. Без систематизації загроз складно визначити, які активи потрібно захищати, які сценарії є критичними, які заходи мають бути першочерговими, а які ризики можна прийняти або контролювати організаційними процедурами. Для автомобільного транспорту в ITS загрози доцільно класифікувати не лише за технічним вектором атаки, а й за об'єктом впливу, наслідками, рівнем доступу атакувальника, тривалістю, масштабом і можливістю фізичного впливу [1, 64, 11].

За об'єктом впливу кіберзагрози можна поділити на загрози для бортових систем автомобіля, внутрішніх мереж, телематичних модулів, V2X-комунікацій, дорожньої інфраструктури, центрів керування, хмарних платформ, мобільних застосунків, цифрових карт, систем оновлення та баз даних. Такий поділ дає змогу пов'язати загрозу з конкретним активом. Наприклад, підроблення V2X-повідомлення впливає на комунікаційну довіру, атака на CAN-шину — на внутрішню взаємодію електронних блоків, а компрометація центру керування — на організацію руху в мережі [65, 66, 67].

За характером впливу загрози поділяються на порушення конфіденційності, цілісності, доступності, автентичності, невідмовності та приватності. Для ITS найбільш небезпечними часто є порушення цілісності й доступності. Якщо атакувальник змінює дані про дорожню подію, координати транспортного засобу або стан світлофора, система може прийняти неправильне рішення. Якщо сервіс стає недоступним, це може призвести до втрати моніторингу, деградації маршрутизації або неможливості доставити критичне попередження. Конфіденційність також важлива, особливо для персональних і телематичних даних, але її порушення частіше має правові, репутаційні та економічні наслідки [52, 53, 54].

За рівнем доступу атакувальника можна виділити віддалені, локальні, фізичні та інсайдерські загрози. Віддалені атаки здійснюються через стільникові мережі, Wi-Fi, Bluetooth, V2X, хмарні API або мобільні застосунки. Локальні атаки потребують перебування поблизу автомобіля або інфраструктурного вузла. Фізичні атаки передбачають доступ до діагностичного роз'єму, електронного блока, дорожнього контролера або серверного обладнання. Інсайдерські загрози пов'язані з діями працівників, підрядників або операторів,

Табл. 3.1: Класифікація кіберзагроз для автомобільного транспорту в ITS

Критерій	**Групи загроз**	**Приклади прояву**
Об'єкт впливу	Автомобіль, V2X, інфраструктура, центр керування, дані	Компрометація ECU, підроблення DENM, атака на світлофорний контролер
Властивість безпеки	Конфіденційність, цілісність, доступність, автентичність, приватність	Витік маршруту, зміна координат, DDoS на сервіс керування
Рівень доступу	Віддалений, локальний, фізичний, внутрішній	Атака через телематику, OBD-II, сервісний доступ, обліковий запис оператора
Масштаб	Один автомобіль, група транспортних засобів, коридор, міська мережа	Масове помилкове оновлення, атака на центр керування
Наслідки	Інформаційні, експлуатаційні, фізичні, правові, економічні	Затримки, ДТП-ризик, штрафи за витік даних, втрата довіри

які мають легітимний доступ, але використовують його неналежно або стають жертвами соціальної інженерії [68, 62, 63].

За тривалістю та поведінкою атаки можуть бути одноразовими, повторюваними, прихованими, персистентними або комбінованими. Одноразова атака може полягати у надсиланні неправдивого повідомлення про небезпеку. Персистентна атака може передбачати тривале перебування шкідливого коду в телематичній платформі або центрі керування. Комбінована атака може починатися з фішингу оператора, переходити до компрометації облікового запису, далі — до зміни налаштувань інфраструктурного пристрою, а потім — до порушення руху на транспортному коридорі.

Ризик кіберзагрози доцільно оцінювати через поєднання ймовірності реалізації та тяжкості наслідків. У простому вигляді:

$$R_i = P_i \cdot I_i, \tag{3.1}$$

де R_i — ризик i-го сценарію, P_i — імовірність реалізації загрози, I_i — вплив на безпеку, надійність, економічні втрати або приватність. Для ITS цю модель доцільно розширювати коефіцієнтами експозиції E_i, виявлюваності D_i та

Рис. 3.1: Узагальнена схема джерел і наслідків кіберзагроз в ITS

керованості C_i:

$$R_i = P_i \cdot I_i \cdot E_i \cdot \frac{1}{D_i} \cdot \frac{1}{C_i}. \tag{3.2}$$

Чим важче виявити атаку й керувати її наслідками, тим вищим є інтегральний ризик.

Класифікація також повинна враховувати ланцюг постачання. Сучасний автомобіль і ITS складаються з компонентів багатьох виробників: електронних блоків, мікропрограм, бібліотек, хмарних сервісів, картографічних платформ, мобільних застосунків, засобів сертифікації та дорожнього обладнання. Вразливість може бути закладена не лише під час експлуатації, а й на етапі розроблення, інтеграції, оновлення або технічного обслуговування. Тому стандарти кібербезпеки автомобільної галузі наголошують на процесному підході протягом життєвого циклу [1, 3, 9, 10].

Окрему групу становлять загрози, пов'язані з помилками машинного навчання й аналітичних моделей. Якщо ITS використовує алгоритми прогнозування потоку, виявлення аномалій, розпізнавання об'єктів або оптимізації маршрутів, атакувальник може впливати на вхідні дані, навчальні вибірки або параметри моделі. Це може призвести до хибних прогнозів, неправильної класифікації небезпечної ситуації або приховування аномальної поведінки. Такі загрози особливо важливі для автоматизованого водіння та цифрових сервісів управління рухом [44, 47, 48].

Таким чином, класифікація кіберзагроз для автомобільного транспорту в ITS повинна бути багатовимірною. Вона має одночасно описувати технічний

вектор атаки, об'єкт впливу, властивість безпеки, масштаб, наслідки, життєвий цикл і організаційний контекст. Саме така класифікація створює основу для подальшого аналізу атак на бортові системи, V2X-комунікації, інфраструктуру та дані.

3.2 Атаки на бортові системи автомобіля

Бортові системи автомобіля є одним із найкритичніших об'єктів кіберзахисту, оскільки вони безпосередньо пов'язані з рухом, гальмуванням, кермуванням, стабілізацією, діагностикою, телематикою та взаємодією з водієм. Сучасний автомобіль містить десятки або сотні електронних блоків керування, які взаємодіють через CAN, LIN, FlexRay, Automotive Ethernet та інші внутрішні мережі. Розширення програмних функцій і зовнішніх інтерфейсів підвищує зручність експлуатації, але також створює шляхи для несанкціонованого доступу [65, 66, 67, 49].

Типова архітектура бортової системи включає домени силової установки, шасі, кузовної електроніки, інформаційно-розважальної системи, телематики, ADAS, діагностики та шлюзів. Найбільша небезпека виникає тоді, коли менш критичний домен, наприклад мультимедійний або телематичний, має шлях до критичних керуючих доменів. Якщо сегментація недостатня, компрометація зовнішнього інтерфейсу може стати початковою точкою для атаки на внутрішні мережі автомобіля [68, 62, 38].

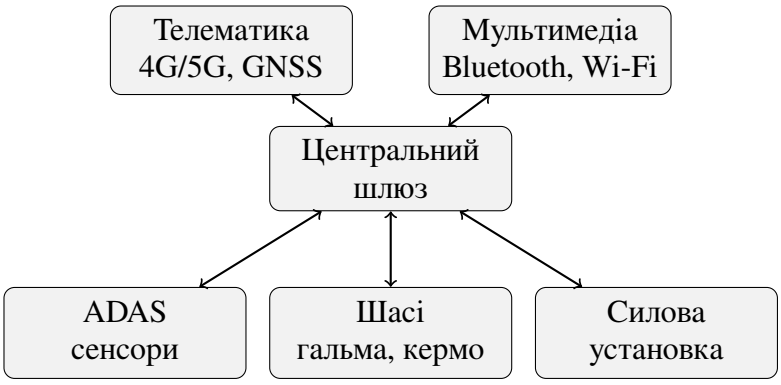

Рис. 3.2: Спрощена схема потенційних шляхів атаки на бортові системи автомобіля

Поширеним об'єктом дослідження є CAN-шина, яка історично проєктувалася для надійного обміну повідомленнями між електронними блоками, але не для протидії зловмиснику. Базові CAN-повідомлення зазвичай не містять

криптографічної автентифікації відправника, шифрування або вбудованих механізмів контролю прав доступу. Тому атакувальник, який отримав доступ до шини, може надсилати підроблені повідомлення, повторювати легітимні кадри, створювати перевантаження або маскувати власні дії під звичайний трафік [65, 66, 69].

Атаки на бортові мережі можна поділити на ін'єкцію повідомлень, атаки повторного відтворення, придушення легітимних повідомлень, DoS-перевантаження, зміну діагностичних параметрів, несанкціоноване перепрограмування, маніпуляцію датчиками та ескалацію доступу через шлюз. Наприклад, ін'єкція повідомлень може імітувати стан натиснутої педалі, змінену швидкість, помилковий сигнал датчика або команду для виконавчого механізму. Навіть якщо сучасні автомобілі мають захисні механізми, ризик залишається актуальним через складність конфігурацій і довгий життєвий цикл транспортних засобів.

Для формалізації атаки на внутрішню мережу можна описати трафік як послідовність повідомлень $m_j = (id_j, data_j, t_j)$, де id_j — ідентифікатор, $data_j$ — поле даних, t_j — час надходження. Аномальність повідомлення може оцінюватися за функцією:

$$A(m_j) = \alpha \Delta id_j + \beta \Delta data_j + \gamma \Delta t_j, \tag{3.3}$$

де Δid_j показує нетиповість ідентифікатора, $\Delta data_j$ — відхилення значення даних від очікуваного діапазону, Δt_j — порушення часової періодичності, а α, β, γ — вагові коефіцієнти. Якщо $A(m_j)$ перевищує поріг, повідомлення може бути позначене як підозріле.

Окрему небезпеку становлять атаки через діагностичні інтерфейси. Діагностичний доступ потрібен для технічного обслуговування, виявлення несправностей, налаштування параметрів і оновлення програмного забезпечення. Проте за недостатньої автентифікації або контролю процедур він може використовуватися для зміни конфігурації, очищення журналів, перепрограмування блоків або отримання чутливої інформації. Тому захист діагностичних сервісів має поєднувати криптографію, контроль ролей, журналювання й обмеження фізичного доступу [50, 51, 1].

Телематичні модулі є важливим вектором атак, оскільки вони мають зовнішній зв'язок і взаємодіють з внутрішньою електронною архітектурою.

Табл. 3.2: Типові атаки на бортові системи автомобіля

Тип атаки	**Механізм**	**Можливі наслідки**
Ін'єкція CAN-повідомлень	Надсилання підроблених кадрів у внутрішню мережу	Хибні стани, небезпечні команди, помилки діагностики
Атака повторного передавання	Повтор раніше записаних легітимних повідомлень	Обхід перевірок, некоректна реакція системи
DoS на шині	Перевантаження мережі високопріоритетними кадрами	Затримка або втрата критичних повідомлень
Компрометація телематики	Використання зовнішнього мережевого інтерфейсу	Віддалений доступ, викрадення даних, поширення атаки
Несанкціоноване оновлення	Підміна або порушення процесу перепрограмування	Встановлення шкідливого ПЗ, відмова функцій

Через телематику реалізуються екстрені виклики, віддалена діагностика, оновлення, навігація, керування автопарком, страхові сервіси та мобільні застосунки. Компрометація такого модуля може дати змогу атакувальнику отримати дані про місцезнаходження, стан автомобіля, поведінку водія або спробувати перейти до внутрішніх мереж. Саме тому телематичний домен повинен бути відокремлений від критичних керуючих доменів шлюзами й політиками доступу.

Атаки на датчики автомобіля можуть бути фізичними або інформаційними. Камери, радари, лідари, ультразвукові датчики та GNSS-приймачі можуть піддаватися засліпленню, спуфінгу, зашумленню або поданню спеціально сформованих сигналів. Для ADAS і автоматизованого водіння це особливо небезпечно, оскільки система може неправильно оцінити дорожнє середовище. Наприклад, GNSS-спуфінг може змінити уявне місцезнаходження, а атака на візуальне сприйняття може вплинути на розпізнавання дорожнього знака або перешкоди [70, 43, 45].

Надійність захисту бортових систем значною мірою залежить від сегментації. Якщо ймовірність компрометації зовнішнього домену дорівнює P_e, а ймовірність успішного переходу через шлюз до критичного домену — P_g, то

ймовірність компрометації критичного домену можна оцінити як:

$$P_{crit} = P_e \cdot P_g. \tag{3.4}$$

Зменшення P_g за рахунок шлюзів, фільтрації, автентифікації та моніторингу суттєво знижує загальний ризик навіть тоді, коли повністю усунути зовнішні загрози неможливо.

Методи захисту бортових систем включають безпечну архітектуру, розподіл доменів, захищені шлюзи, автентифікацію повідомлень, контроль діагностичних процедур, безпечне завантаження, підписані оновлення, апаратні модулі довіри, системи виявлення вторгнень, журналювання подій і принцип мінімальних привілеїв. Важливо, щоб ці методи були інтегровані в життєвий цикл розроблення, а не додавалися після завершення проєктування [1, 3, 56, 57].

Отже, атаки на бортові системи автомобіля є критичним класом загроз, оскільки вони можуть мати прямі фізичні наслідки. Їх аналіз вимагає поєднання знань про автомобільну електроніку, внутрішні мережі, програмне забезпечення, діагностику, сенсори, телематику та експлуатаційні процеси. У середовищі ITS ці атаки стають ще небезпечнішими, адже підключений автомобіль взаємодіє з інфраструктурою, V2X-сервісами та хмарними платформами.

3.3 Загрози для каналів кооперативної комунікації транспортних засобів

V2X-комунікації є одним із ключових елементів кооперативних ITS. Вони забезпечують обмін інформацією між транспортними засобами, інфраструктурою, пішоходами, мережевими сервісами та іншими учасниками мобільності. Завдяки V2X автомобіль може отримувати попередження про небезпеку за межами прямої видимості, дані про фази світлофора, інформацію про дорожні роботи, аварії, слизьке покриття або екстрене гальмування іншого транспортного засобу. Проте саме відкритість і динамічність V2X-середовища робить його привабливою ціллю для атак [33, 40, 41].

Основна складність захисту V2X полягає в тому, що повідомлення мають передаватися швидко, часто широкомовно, у середовищі з високою мобільністю та великою кількістю учасників. Традиційні підходи до автен-

тифікації з тривалими сесіями не завжди придатні для коротких безпекових повідомлень. Крім того, потрібно одночасно забезпечити автентичність повідомлень і приватність користувачів, щоб транспортний засіб не можна було легко відстежувати протягом тривалого часу [16, 17, 20, 21].

Типовими загрозами для V2X є підроблення повідомлень, атаки повторного відтворення, атаки Сивілли, спуфінг координат, придушення радіоканалу, DDoS на мережеві сервіси, компрометація сертифікатів, відстеження транспортних засобів, поширення неправдивих повідомлень про дорожні події та атаки на механізми довіри. Наприклад, підроблене DENM-повідомлення про аварію може змусити транспортні засоби змінити маршрут, створити штучний затор або відволікти увагу оператора центру керування [15, 40, 39].

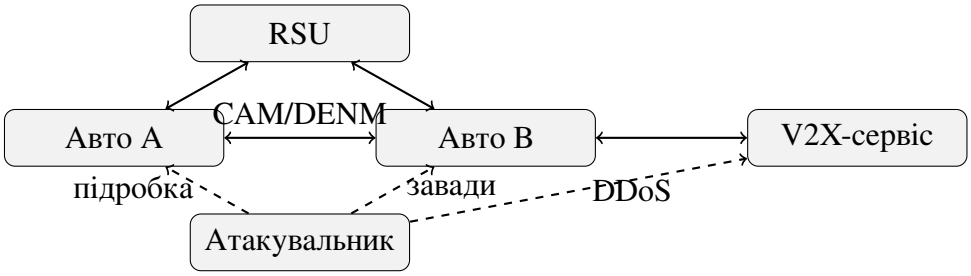

Рис. 3.3: Приклади загроз у V2X-комунікаційному середовищі

Підроблення повідомлень є базовим сценарієм атаки. Атакувальник може надіслати повідомлення про неіснуючу небезпеку, помилкову швидкість, неправильне місцезнаходження або фіктивний транспортний засіб. Якщо отримувач довіряє такому повідомленню без перевірки, це може призвести до непотрібного гальмування, зміни маршруту або хибної оцінки дорожньої ситуації. Захист полягає в цифрових підписах, сертифікатах, перевірці часових міток, географічної релевантності та фізичної правдоподібності [17, 20, 42].

Атака повторного передавання полягає у повторному передаванні раніше дійсного повідомлення. Наприклад, повідомлення про аварію або обмеження руху може бути записане й відтворене пізніше в іншому місці або в інший час. Навіть якщо повідомлення було підписане легітимним учасником, повторне використання робить його небезпечним. Для протидії застосовують часові мітки, лічильники, обмеження зони дії та перевірку актуальності повідомлення.

атака Сивілли виникає, коли один фізичний вузол видає себе за багато різних транспортних засобів. У V2X це може створити ілюзію затору, колони автомобілів, масової події або небезпечного скупчення. Така атака особливо

небезпечна для алгоритмів, які приймають рішення на основі кількості повідомлень від різних учасників. Протидія потребує керування сертифікатами, обмеження одночасних псевдонімів, перевірки фізичної правдоподібності та кореляції з інфраструктурними датчиками [41, 40].

Імовірність прийняття неправдивого повідомлення можна описати як функцію технічної автентифікації та семантичної перевірки:

$$P_{accept} = P_{auth} \cdot P_{plaus}, \tag{3.5}$$

де P_{auth} — імовірність проходження криптографічної перевірки, а P_{plaus} — імовірність того, що повідомлення виглядає фізично правдоподібним. Якщо повідомлення має дійсний підпис, але суперечить кінематиці руху або даним інфраструктури, воно не повинно автоматично прийматися як достовірне.

Табл. 3.3: Загрози V2X та рекомендовані механізми протидії

Загроза	**Наслідок**	**Механізми протидії**
Підроблення повідомлень	Хибні попередження, неправильні маневри	Цифровий підпис, сертифікати, перевірка правдоподібності
Атака повторного передавання	Повтор застарілих подій	Часові мітки, лічильники, обмеження зони дії
атака Сивілли	Імітація багатьох учасників	Керування псевдонімами, кореляція з датчиками, довірчі моделі
Придушення каналу	Втрата доступності каналу	Резервні канали, адаптивна потужність, виявлення завад
Відстеження	Порушення приватності маршруту	Псевдоніми, мінімізація даних, політики зміни сертифікатів

Придушення каналу або придушення каналу є загрозою доступності. У щільному міському середовищі V2X-канали можуть бути перевантажені, а цілеспрямовані завади можуть зменшити дальність або надійність доставки повідомлень. Для критичних сервісів це означає, що система не повинна покладатися лише на один канал. Гібридна комунікаційна архітектура, яка поєднує короткодіапазонний зв'язок, стільникові мережі та локальну автономність, підвищує стійкість [8, 18, 19].

Загрози V2X також пов'язані з керуванням сертифікатами. Якщо сертифікат скомпрометовано, атакувальник може підписувати повідомлення як легітимний учасник. Якщо механізм відкликання працює повільно, небезпечний вузол може тривалий час залишатися в системі. Якщо політика псевдонімів неправильна, користувач може бути відстежений. Отже, інфраструктура відкритих ключів для V2X повинна бути швидкою, масштабованою, приватною та придатною до аудиту [16, 17, 21].

Для оцінювання доступності V2X-сервісу можна використати показник успішної доставки критичного повідомлення в допустимий час:

$$A_{v2x} = P(T_{delivery} \leq T_{max}) \cdot P_{valid}, \tag{3.6}$$

де $T_{delivery}$ — фактичний час доставки, T_{max} — гранично допустима затримка, P_{valid} — імовірність того, що повідомлення є дійсним і прийнятим після перевірки. Цей показник поєднує мережеву доступність і безпекову валідність.

Важливо, що не всі V2X-повідомлення мають однакову критичність. Попередження про екстрене гальмування, небезпечну перешкоду або транспортний засіб аварійної служби потребує жорстких часових вимог. Інформація про паркування або рекомендація маршруту може мати більшу затримку. Тому захист V2X повинен бути диференційованим: критичні повідомлення мають пріоритет доставки й перевірки, а менш критичні сервіси можуть використовувати менш жорсткі вимоги.

Отже, V2X-комунікації створюють нову якість кооперативної мобільності, але водночас є складним середовищем кіберзагроз. Їх захист потребує поєднання криптографічних механізмів, керування довірою, перевірки фізичної правдоподібності, резервування каналів, захисту приватності та процедур реагування на компрометацію учасників.

3.4 Атаки на дорожню інфраструктуру та центри керування

Дорожня інфраструктура та центри керування рухом є критичними компонентами ITS. Вони забезпечують моніторинг транспортної мережі, керування світлофорами, інформування водіїв, координацію аварійних служб, збір даних, оброблення подій і взаємодію з транспортними засобами. На відміну від окремого автомобіля, атака на інфраструктуру може вплинути на велику

кількість учасників руху одночасно. Саме тому інфраструктурні компоненти мають розглядатися як об'єкти критичної кіберфізичної безпеки [5, 13, 28, 37].

До дорожньої інфраструктури ITS належать світлофорні контролери, дорожні датчики, камери відеоспостереження, радари, RSU, табло змінної інформації, метеостанції, системи автоматичного зважування, паркувальні системи, зарядні станції, контролери тунелів, дорожні сервери та мережеве обладнання. Кожний з цих компонентів може мати власні вразливості: застаріле програмне забезпечення, слабкі паролі, відкриті порти, незахищені протоколи, відсутність журналювання, недостатню фізичну охорону або залежність від віддаленого адміністрування.

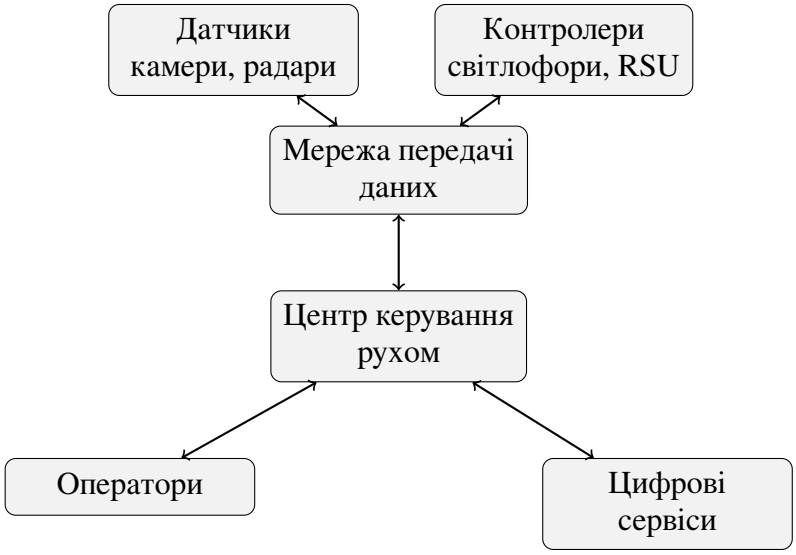

Рис. 3.4: Інфраструктурний контур ITS як об'єкт кібератак

Атаки на світлофорні контролери можуть призводити до зміни фаз, порушення координації, вимкнення адаптивного керування або створення небезпечних конфліктів. Навіть якщо контролери мають локальні захисні режими, атака може спричинити затори, затримки громадського транспорту, збільшення аварійного ризику або ускладнення руху екстрених служб. Особливо небезпечними є сценарії, коли атакувальник не просто вимикає систему, а змінює режими так, щоб вони виглядали як технічна помилка або нетипова транспортна ситуація.

Атаки на датчики та відеоаналітику можуть впливати на якість даних, які використовує центр керування. Якщо камера або радар повідомляє неправильну інтенсивність, система може змінити світлофорний план у невідповідний спосіб. Якщо атакувальник приховує затор або створює ілюзію транспортного

потоку, оператор може прийняти неправильне рішення. Такі атаки можуть бути цифровими, наприклад через зміну даних у мережі, або фізичними, наприклад через засліплення камери, пошкодження датчика чи зміну його положення [31, 45].

Центри керування є особливо цінною ціллю, оскільки вони концентрують дані, повноваження та інтерфейси впливу. Компрометація центру може дати змогу атакувальнику змінювати налаштування інфраструктури, переглядати відеопотоки, отримувати оперативні дані, впливати на повідомлення для водіїв, блокувати операторські робочі місця або приховувати інциденти. Загрози для центрів керування включають фішинг, компрометацію облікових записів, шкідливе ПЗ, програма-вимагач, DDoS, атаки на API, порушення сегментації мережі та інсайдерські дії [11, 12, 37].

Табл. 3.4: Атаки на інфраструктуру ITS та можливі наслідки

Об'єкт	**Сценарій атаки**	**Наслідки**
Світлофорний контролер	Зміна фаз або планів координації	Затори, небезпечні конфлікти, затримка екстрених служб
Датчики руху	Підміна або спотворення вимірювань	Неправильне адаптивне керування, хибні прогнози
RSU	Компрометація V2I-повідомлень	Поширення неправдивих попереджень, втрата довіри
Центр керування	Захоплення облікового запису або програма-вимагач	Втрата моніторингу, блокування операторів, порушення сервісів
Табло змінної інформації	Несанкціонована зміна повідомлень	Дезінформація водіїв, репутаційні втрати

Для інфраструктури ITS важливо враховувати каскадний ефект. Нехай p_k — імовірність відмови або компрометації k-го вузла, а c_k — коефіцієнт його впливу на мережу. Тоді інтегральний інфраструктурний ризик можна оцінити як:

$$R_{infra} = \sum_{k=1}^{n} p_k c_k. \tag{3.7}$$

Вузол із невеликою ймовірністю компрометації, але дуже високим коефіцієнтом впливу, наприклад центральний сервер керування, може бути критичнішим

за численні менш важливі датчики.

Інфраструктурні атаки часто поєднують кібернетичні та фізичні вектори. Дорожні шафи, контролери, камери й мережеве обладнання розташовані у відкритому середовищі, тому атакувальник може отримати фізичний доступ, підключитися до сервісного порту, пошкодити пристрій або встановити проміжне обладнання. Через це захист має включати фізичну безпеку, контроль доступу, пломбування, відеоспостереження, датчики відкриття шаф, інвентаризацію та регулярні перевірки.

Центри керування потребують сегментації мереж. Операторські робочі місця, сервери відеоаналітики, бази даних, системи керування світлофорами, зовнішні API та адміністративні сервіси не повинні перебувати в одному неконтрольованому сегменті. Компрометація одного робочого місця не повинна автоматично давати доступ до критичних команд. Практичні заходи включають багатофакторну автентифікацію, контроль привілеїв, журналювання дій, резервне копіювання, тестування відновлення, моніторинг подій і регулярний аудит.

Для оцінювання стійкості центру керування можна використати показник часу відновлення критичної функції:

$$S_{tmc} = \frac{T_{max} - T_{restore}}{T_{max}}, \qquad 0 \leq S_{tmc} \leq 1, \tag{3.8}$$

де $T_{restore}$ — фактичний час відновлення функції після інциденту, T_{max} — максимально допустимий час простою. Чим ближче S_{tmc} до одиниці, тим вищою є експлуатаційна стійкість центру.

Важливим елементом захисту є сценарне планування. Центр керування повинен мати готові процедури для ситуацій, коли недоступні камери, порушено зв'язок із групою світлофорів, скомпрометовано обліковий запис, виявлено підозрілі V2X-повідомлення або відбувається атака на публічний сервіс. Без таких процедур оператори можуть втратити час на неузгоджені дії, а технічний інцидент переросте в транспортну кризу.

Отже, дорожня інфраструктура та центри керування є не менш важливими об'єктами кіберзахисту, ніж транспортні засоби. Їх компрометація може мати мережевий ефект, впливаючи на транспортні потоки, безпеку руху, доступність сервісів і довіру користувачів. Захист повинен поєднувати технічні,

фізичні, організаційні та процедурні заходи.

3.5 Ризики витоку персональних і телематичних даних

Персональні й телематичні дані є одним із найцінніших ресурсів сучасного автомобільного транспорту. Підключені автомобілі, мобільні застосунки, навігаційні сервіси, системи оплати, страхові платформи, диспетчерські системи та центри керування можуть обробляти місцезнаходження, маршрути, швидкість, стиль водіння, дані про поїздки, технічний стан автомобіля, ідентифікатори пристроїв, платіжну інформацію, відео, голосові команди та інформацію про користувацькі звички. Такі дані мають високу аналітичну й комерційну цінність, але водночас створюють значні ризики приватності [52, 53, 54].

Ризик витоку даних у ITS полягає не лише у незаконному доступі до бази даних. Навіть окремі фрагменти телематичної інформації можуть дати змогу відновити поведінковий профіль людини: місце проживання, місце роботи, регулярні маршрути, час поїздок, відвідування медичних, релігійних, політичних або комерційних об'єктів. Якщо такі дані поєднати з іншими наборами, ризик повторної ідентифікації зростає навіть після часткової анонімізації [34, 52].

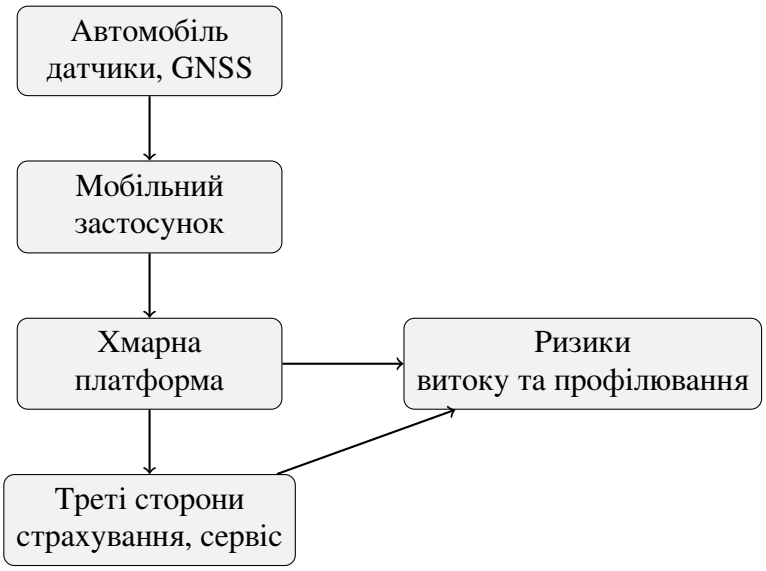

Рис. 3.5: Потоки телематичних даних і точки виникнення ризиків приватності

Джерела витоку можна поділити на технічні, організаційні та правові. Технічні джерела включають вразливості API, незахищені бази даних, слабке шифрування, помилки автентифікації, некоректні мобільні застосунки, надмірні журнали, компрометацію хмарного сервісу або перехоплення трафіку.

Організаційні джерела пов'язані з надмірними правами доступу, відсутністю контролю підрядників, помилками операторів, недостатнім аудитом або неузгодженим обміном даними. Правові джерела виникають тоді, коли дані збираються без чіткої мети, зберігаються довше, ніж потрібно, або передаються третім сторонам без належної підстави.

Табл. 3.5: Категорії даних ITS та ризики їх оброблення

Категорія даних	**Приклади**	**Основні ризики**
Геолокаційні дані	Координати, маршрути, зупинки	Відстеження, профілювання, повторна ідентифікація
Поведінкові дані	Швидкість, гальмування, стиль водіння	Дискримінація, страхове профілювання, помилкові висновки
Технічні дані	Помилки, стан агрегатів, діагностика	Комерційна чутливість, зловживання сервісним доступом
Ідентифікатори	VIN, сертифікати, пристрої, акаунти	Зв'язування наборів даних, викрадення облікових записів
Медіадані	Відео, аудіо, зображення салону або дороги	Біометричні й приватні відомості, сторонні особи

Для оцінювання ризику повторної ідентифікації можна використовувати узагальнену залежність:

$$P_{reid} = 1 - \prod_{j=1}^{m}(1 - q_j), \tag{3.9}$$

де q_j — імовірність ідентифікації особи за j-ю ознакою або набором ознак. Чим більше незалежних або напівнезалежних ознак зберігається, тим вищою є загальна ймовірність повторної ідентифікації. Для телематичних даних такими ознаками можуть бути регулярні координати, часові шаблони, стиль водіння або зв'язок з мобільним пристроєм.

Захист персональних даних у ITS повинен базуватися на принципах мінімізації, обмеження мети, прозорості, точності, обмеження строку зберігання, цілісності, конфіденційності та підзвітності. Це означає, що система повинна збирати лише ті дані, які справді потрібні для конкретного сервісу; не

використовувати їх для несумісних цілей; надавати користувачеві зрозумілу інформацію; забезпечувати механізми доступу, виправлення й видалення; а також документувати операції оброблення [53, 52, 54].

Технічні методи захисту включають шифрування під час передавання та зберігання, псевдонімізацію, анонімізацію, диференційований доступ, токенізацію, безпечне журналювання, сегментацію баз даних, контроль API, управління ключами та регулярне тестування захищеності. Водночас анонімізація телематичних даних є складною, оскільки траєкторії руху часто мають унікальний характер. Тому просте видалення імені або VIN не завжди достатнє для захисту приватності.

Ризик витоку даних можна оцінити як очікувані втрати:

$$L_{data} = P_{leak} \cdot (C_{legal} + C_{rep} + C_{oper} + C_{user}), \tag{3.10}$$

де P_{leak} — імовірність витоку, C_{legal} — правові витрати, C_{rep} — репутаційні втрати, C_{oper} — експлуатаційні витрати на реагування, C_{user} — шкода для користувачів. Така модель показує, що витік даних має не лише технічний, а й соціально-економічний вимір.

Особливої уваги потребує обмін даними між учасниками екосистеми: виробниками автомобілів, операторами доріг, страховими компаніями, сервісними станціями, навігаційними платформами, органами влади та третіми розробниками. Кожне передавання даних повинно мати правову підставу, визначену мету, мінімальний обсяг, захищений канал і договірні обмеження щодо подальшого використання. Без цього телематична екосистема може перетворитися на неконтрольований ринок даних.

Витоки можуть також впливати на фізичну безпеку. Якщо атакувальник отримує інформацію про місцезнаходження службового транспорту, маршрути цінних вантажів, графік переміщення посадових осіб або домашні адреси користувачів, ризик виходить за межі приватності. Тому для критичних автопарків і спеціальних перевезень потрібно застосовувати підвищені вимоги до геолокаційних даних, доступу операторів і журналювання запитів.

Отже, персональні й телематичні дані є одночасно ресурсом для підвищення ефективності ITS і джерелом значних ризиків. Їх захист потребує поєднання правових, організаційних і технічних заходів. Без належного управління даними навіть технологічно досконала ITS може втратити довіру користувачів

і зіткнутися з правовими обмеженнями.

3.6 Матриця сценаріїв атак і оцінювання залишкового ризику

Для практичного використання класифікації кіберзагроз недостатньо лише перелічити можливі атаки. Потрібно встановити, які сценарії є найбільш небезпечними для конкретної ITS, які активи вони зачіпають, які наслідки можуть мати та які заходи знижують ризик до прийнятного рівня. З цією метою доцільно застосовувати матрицю сценаріїв атак, що поєднує вектор атаки, об'єкт впливу, початкову умову, наслідок, засоби виявлення та заходи протидії. Такий підхід узгоджується з процесною логікою кібербезпеки автомобільної галузі, де аналіз загроз повинен бути пов'язаний з активами, життєвим циклом і вимогами до захисту [1, 64, 11].

Сценарій атаки в ITS можна описати як послідовність переходів між станами системи. Початковий стан відповідає нормальній роботі, проміжні стани — компрометації окремих компонентів або порушенню довіри, кінцевий стан — небажаному наслідку. Наприклад, фішинг оператора може призвести до викрадення облікових даних, далі — до несанкціонованого входу в систему керування, потім — до зміни налаштувань світлофорного плану, а кінцевим наслідком стане затор або небезпечна конфліктна ситуація. Такий ланцюг важливий, бо окремо кожна дія може здаватися малозначущою, але разом вони утворюють критичний сценарій.

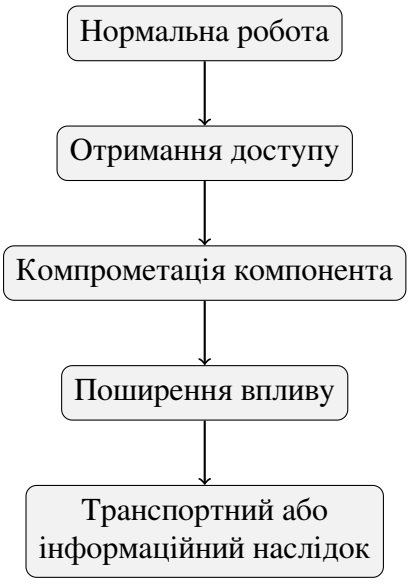

Рис. 3.6: Узагальнений ланцюг розвитку кіберінциденту в ITS

Матриця сценаріїв має враховувати не тільки технічні параметри, а й експлуатаційний контекст. Одна й та сама атака може мати різні наслідки залежно від місця, часу та транспортного навантаження. Підроблене повідомлення про аварію на малозавантаженій ділянці може спричинити лише незначне відхилення маршруту. Те саме повідомлення в години пік на магістральному коридорі може створити масштабний затор, затримати громадський транспорт і вплинути на роботу екстрених служб. Тому оцінювання ризику має бути контекстним.

Табл. 3.6: Матриця прикладних сценаріїв атак для автомобільного транспорту в ITS

Сценарій	**Об'єкт впливу**	**Ключовий наслідок**	**Пріоритет протидії**
Підроблення V2X-події	V2X-канал, автомобілі	Хибні маневри, зміна маршрутів	Високий
Ін'єкція CAN-кадрів	Бортова мережа	Некоректні стани та команди	Критичний
Компрометація світлофора	Дорожній контролер	Затори, конфліктні фази	Критичний
Програма-вимагач у центрі керування	Сервери та робочі місця	Втрата моніторингу й керування	Критичний
Витік геолокації	Хмарна платформа, застосунок	Профілювання й відстеження	Високий
Підміна даних датчика	Інфраструктурний сенсор	Хибне адаптивне керування	Високий

Залишковий ризик після впровадження захисних заходів можна подати як:

$$R_{res} = R_0 \prod_{k=1}^{n} (1 - ho_k), \tag{3.11}$$

де R_0 — початковий ризик сценарію, ρ_k — ефективність k-го захисного заходу. Формула показує, що декілька незалежних або частково незалежних заходів можуть суттєво знизити ризик, але ефективність кожного з них має бути реально оцінена. Якщо заходи дублюють один одного або залежать від однієї вразливої точки, фактичне зниження ризику буде меншим.

Для бортових систем залишковий ризик зменшується завдяки сегментації доменів, захищеним шлюзам, контролю діагностичного доступу, системам

виявлення вторгнень і безпечним оновленням. Для V2X — завдяки цифровим підписам, сертифікатам, перевірці правдоподібності, часовим міткам і резервним каналам. Для інфраструктури — завдяки фізичному захисту, сегментації мереж, резервним планам керування, моніторингу та аудитам. Для даних — завдяки мінімізації, шифруванню, псевдонімізації, контролю доступу й правовим процедурам [17, 20, 3, 52].

Важливо оцінювати не лише залишковий ризик, а й ризик надмірної складності захисту. Якщо захисні механізми створюють значні затримки, ускладнюють експлуатацію, генерують багато помилкових спрацювань або блокують легітимні дії операторів, система може стати менш надійною. Наприклад, надмірно сувора політика доступу без аварійних процедур може затримати реагування на інцидент, а погано налаштована IDS може перевантажити оператора попередженнями. Отже, заходи протидії мають бути не максимальними, а збалансованими.

Для вибору пріоритетів можна використовувати індекс критичності сценарію:

$$K_s = \omega_1 I_s + \omega_2 M_s + \omega_3 T_s + \omega_4 P_s - \omega_5 D_s, \tag{3.12}$$

де I_s — тяжкість наслідків, M_s — масштаб впливу, T_s — часовий тиск реагування, P_s — імовірність реалізації, D_s — здатність до виявлення, а ω_i — вагові коефіцієнти. Сценарії з високим K_s повинні отримувати пріоритет у планах захисту, тестування й резервування.

Практичне застосування матриці сценаріїв передбачає регулярне оновлення. Після появи нового сервісу, зміни постачальника, оновлення програмного забезпечення, підключення нового типу датчика або зміни регуляторних вимог матриця має переглядатися. Так само вона повинна оновлюватися після реальних інцидентів, навчань або тестів на проникнення. Без цього матриця швидко втрачає актуальність і перетворюється на формальний документ.

Окремим елементом є розподіл відповідальності. Для кожного сценарію потрібно визначити власника ризику: виробника автомобіля, оператора дороги, центр керування, постачальника зв'язку, хмарного провайдера, перевізника або орган управління. Якщо власник не визначений, заходи протидії можуть залишитися невиконаними, навіть якщо технічне рішення відоме. Тому матриця сценаріїв має містити не лише технічні поля, а й організаційні: відповідальний суб'єкт, процедура реагування, строк відновлення, канали повідомлення та

критерії закриття інциденту.

Таким чином, матриця сценаріїв атак поєднує класифікацію загроз із практичним управлінням ризиками. Вона дає змогу перейти від загального переліку небезпек до конкретних рішень: що захищати, від чого захищати, хто відповідає, як виявляти, як реагувати та який залишковий ризик є прийнятним. Для автомобільного транспорту в ITS такий інструмент є необхідним, оскільки кількість взаємозв'язків між автомобілем, інфраструктурою, даними й сервісами постійно зростає.

3.7 Узагальнення ризиків і пріоритети їх зниження

Аналіз кіберзагроз показує, що автомобільний транспорт в ITS має багаторівневу поверхню атаки. Вона охоплює транспортний засіб, бортові мережі, датчики, телематику, V2X-канали, дорожню інфраструктуру, центри керування, хмарні платформи, мобільні застосунки та дані. Тому захист не може бути зведений до одного інструмента. Потрібна система заходів, що поєднує безпечну архітектуру, стандартизовані процеси, моніторинг, реагування, резервування, навчання персоналу та контроль життєвого циклу [1, 11, 12].

Пріоритетність протидії повинна визначатися не лише частотою загрози, а й тяжкістю наслідків. Рідкісна атака на центр керування може бути критичнішою, ніж частіші, але локальні спроби несанкціонованого доступу до менш важливого сервісу. Так само витік геолокаційних даних може мати значні правові наслідки, навіть якщо не впливає безпосередньо на рух. Тому доцільно використовувати матрицю ризиків, яка враховує ймовірність, вплив, виявлюваність, масштаб і здатність до відновлення.

Загальну ефективність протидії можна подати як відношення зниженого ризику до початкового:

$$E_{sec} = \frac{R_0 - R_{res}}{R_0} \cdot 100\%, \tag{3.13}$$

де R_0 — початковий рівень ризику, R_{res} — залишковий ризик після впровадження заходів. Мета кіберзахисту полягає не в абсолютному усуненні всіх ризиків, що практично неможливо, а в доведенні залишкового ризику до прийнятного рівня.

Важливим є принцип багаторівневого захисту. Навіть якщо один меха-

Табл. 3.7: Пріоритети протидії кіберзагрозам в ITS

Напрям ризику	**Критичність**	**Першочергові заходи**
Бортові системи	Висока через фізичні наслідки	Сегментація, IDS, захищені оновлення, контроль діагностики
V2X-комунікації	Висока через кооперативні рішення	PKI, підписи, перевірка правдоподібності, резервні канали
Інфраструктура	Висока через мережевий ефект	Сегментація, фізичний захист, резервування, журналювання
Центри керування	Критична через концентрацію повноважень	MFA, SOC-моніторинг, резервування, сценарії реагування
Дані користувачів	Висока через правові та соціальні наслідки	Мінімізація, шифрування, псевдонімізація, контроль доступу

нізм не спрацював, інші мають обмежити наслідки. Наприклад, якщо атакувальник отримав доступ до телематичного модуля, шлюз повинен обмежити його доступ до критичних доменів; якщо підроблене V2X-повідомлення має коректний формат, перевірка фізичної правдоподібності повинна зменшити шанс його прийняття; якщо скомпрометовано операторське робоче місце, сегментація й контроль привілеїв повинні запобігти зміні критичних налаштувань.

Кіберзагрози для автомобільного транспорту в ITS мають динамічний характер. З появою нових сервісів, оновлень, протоколів, моделей машинного навчання та бізнес-процесів змінюються і сценарії атак. Тому захист повинен бути не одноразовим проєктом, а безперервним процесом. Він має включати інвентаризацію активів, аналіз загроз, оцінювання ризиків, тестування, моніторинг, реагування, навчання, аудит і перегляд вимог.

Підсумовуючи, кіберзагрози для автомобільного транспорту в ITS охоплюють усі рівні системи: від бортового контролера до центру керування й хмарного сервісу. Їх наслідки можуть бути технічними, фізичними, експлуатаційними, правовими, економічними та соціальними. Саме тому подальший розвиток ITS має спиратися на інтегровану модель кібербезпеки й надійності, у якій захист автомобіля, інфраструктури, комунікацій і даних розглядається

як єдине завдання.

4 Надійність автомобільного транспорту в умовах цифровізації

Цифровізація автомобільного транспорту змінює зміст поняття надійності. У традиційному розумінні надійність автомобіля або транспортної системи переважно пов'язувалася з безвідмовною роботою механічних вузлів, двигуна, трансмісії, гальмівної системи, підвіски, дорожньої інфраструктури та організаційних процесів експлуатації. У сучасних інтелектуальних транспортних системах до цих складових додаються програмне забезпечення, електронні блоки керування, датчики, телематичні модулі, внутрішні мережі автомобіля, V2X-комунікації, хмарні сервіси, центри керування, цифрові карти й алгоритми оброблення даних. Тому надійність стає властивістю не окремого технічного виробу, а розподіленої кіберфізичної системи [2, 4, 6, 5].

В умовах цифровізації відмова може мати не лише механічну, а й інформаційну природу. Некоректне оновлення програмного забезпечення, помилка алгоритму, нестабільний канал зв'язку, деградація сенсора, збій електронного блока керування або недоступність хмарного сервісу можуть спричинити ті самі експлуатаційні наслідки, що й класична технічна несправність: затримку руху, втрату функції, неправильне керування, зниження безпеки або неможливість виконати транспортну послугу. Саме тому надійність автомобільного транспорту в ITS необхідно аналізувати разом із функціональною безпекою, кібербезпекою та керуванням життєвим циклом програмного забезпечення [1, 3, 9, 10].

У цьому розділі розглядаються поняття надійності транспортних систем, вплив програмного забезпечення на безпеку руху, відмови датчиків, електронних блоків керування й комунікаційних модулів, а також взаємозв'язок кібербезпеки, функціональної безпеки та експлуатаційної надійності. Така структура дає змогу перейти від загальної теорії надійності до практичних проблем цифрового автомобільного транспорту.

4.1 Поняття надійності транспортної системи

Надійність транспортної системи можна визначити як здатність виконувати задані функції перевезення, керування, інформування та забезпечення

безпеки протягом визначеного часу в установлених умовах експлуатації. Для автомобільного транспорту це означає, що транспортні засоби, дорожня інфраструктура, засоби керування рухом, інформаційні сервіси й організаційні процедури повинні спільно забезпечувати передбачуваний, безпечний і доступний транспортний процес. У цифровому середовищі надійність охоплює не тільки фізичну працездатність, а й коректність даних, доступність сервісів, стабільність програмних функцій і здатність системи до відновлення після відмов або інцидентів [2, 4, 5].

Класична теорія надійності оперує поняттями безвідмовності, довговічності, ремонтопридатності, збережуваності та готовності. Безвідмовність характеризує здатність системи працювати без відмов протягом часу. Довговічність описує ресурс до граничного стану. Ремонтопридатність визначає можливість і швидкість відновлення працездатності. Збережуваність пов'язана зі здатністю не втрачати властивості під час зберігання або простою. Готовність відображає імовірність того, що система буде працездатною в потрібний момент. Для ITS особливо важливими є готовність і відновлюваність, оскільки транспортні сервіси мають працювати безперервно або переходити в безпечний деградаційний режим.

Рис. 4.1: Складові надійності автомобільного транспорту в ITS

Для одиничного компонента з постійною інтенсивністю відмов λ імовірність безвідмовної роботи протягом часу t може бути подана як:

$$P(t) = e^{-\lambda t}. \tag{4.1}$$

Середній час безвідмовної роботи для такого випадку становить:

$$MTBF = \frac{1}{\lambda}. \tag{4.2}$$

Однак для автомобільного транспорту в ITS ці формули є лише базовим наближенням, оскільки реальна система складається з багатьох взаємопов'язаних компонентів із різними режимами експлуатації, оновленнями, залежностями та умовами навколишнього середовища.

Готовність системи часто оцінюють за формулою:

$$A = \frac{MTBF}{MTBF + MTTR}, \tag{4.3}$$

де $MTTR$ — середній час відновлення. Для цифровізованого транспорту зменшення $MTTR$ може бути не менш важливим, ніж збільшення $MTBF$. Наприклад, якщо центр керування має резервну інфраструктуру, автоматичне перемикання й актуальні резервні копії, він може швидко відновити критичні функції навіть після збою. Якщо ж відновлення потребує ручного втручання, пошуку конфігурацій або очікування постачальника, фактична готовність системи знижується.

Табл. 4.1: Показники надійності для автомобільного транспорту в ITS

Показник	**Зміст**	**Приклад застосування**
$MTBF$	Середній час між відмовами	Оцінювання стабільності ECU, RSU або сервера
$MTTR$	Середній час відновлення	Відновлення світлофорного контролера або сервісу даних
Готовність A	Імовірність працездатності в потрібний момент	Центр керування, V2X-сервіс, система моніторингу
Інтенсивність відмов λ	Частота виникнення відмов	Датчики, комунікаційні модулі, мережеві пристрої
Залишковий ризик	Ризик після захисних і резервних заходів	Оцінювання прийнятності експлуатації

Надійність транспортної системи має багаторівневу природу. На рівні транспортного засобу вона залежить від стану механічних систем, електроніки,

датчиків, програмного забезпечення та бортових мереж. На рівні інфраструктури — від світлофорів, дорожніх датчиків, контролерів, каналів зв'язку, електроживлення й фізичного захисту. На рівні центрів керування — від серверів, операторських робочих місць, програмних платформ, баз даних, процедур реагування та кваліфікації персоналу. На рівні сервісів — від якості даних, доступності API, захищеності хмари та коректності алгоритмів.

Системна надійність не є простою сумою надійності окремих елементів. Якщо компоненти з'єднані послідовно, відмова одного з них може спричинити відмову всієї функції. Для послідовної структури імовірність безвідмовної роботи дорівнює:

$$P_{series} = \prod_{i=1}^{n} P_i. \tag{4.4}$$

Для паралельного резервування імовірність працездатності може бути оцінена як:

$$P_{parallel} = 1 - \prod_{i=1}^{n} (1 - P_i). \tag{4.5}$$

Ці співвідношення пояснюють, чому критичні ITS-функції потребують резервування, але також показують, що резервування має бути правильно організованим. Якщо резервні компоненти залежать від одного джерела живлення, однієї мережі або однієї вразливої конфігурації, фактична стійкість буде нижчою.

Важливо розрізняти технічну відмову, функціональну небезпеку та експлуатаційну деградацію. Технічна відмова означає втрату працездатності компонента. Функціональна небезпека виникає тоді, коли система виконує функцію неправильно або в невідповідних умовах. Експлуатаційна деградація може проявлятися поступово: збільшення затримок, нестабільність прогнозів, зростання кількості помилкових попереджень, зниження точності датчиків або збільшення часу відновлення. Для ITS усі три форми є важливими.

Цифровізація збільшує роль спостережуваності. Надійна система повинна не лише працювати, а й надавати інформацію про власний стан. Моніторинг температури електронних блоків, якості зв'язку, кількості помилок, затримок, стану пам'яті, версій програмного забезпечення, журналів подій і якості даних дає змогу виявляти деградацію до повної відмови. Це створює передумови для прогнозного технічного обслуговування [58, 59, 60].

У транспортній системі корисно використовувати інтегральний індекс надійності:

$$N_{ITS} = w_1 A_v + w_2 A_i + w_3 A_c + w_4 Q_d + w_5 R_o, \tag{4.6}$$

де A_v — готовність транспортних засобів, A_i — готовність інфраструктури, A_c — готовність комунікацій, Q_d — якість даних, R_o — організаційна готовність до відновлення, а w_i — ваги відповідно до критичності функцій. Такий індекс не замінює детальний аналіз, але дає змогу порівнювати сценарії модернізації.

Отже, поняття надійності транспортних систем в умовах цифровізації має бути розширене. Воно повинно охоплювати безвідмовність технічних компонентів, стійкість програмного забезпечення, якість даних, доступність сервісів, кіберстійкість, відновлюваність і здатність до безпечної деградації. Без такого розширення оцінка надійності буде неповною.

4.2 Вплив програмного забезпечення на безпеку дорожнього руху

Програмне забезпечення стало одним із головних чинників безпеки й надійності автомобільного транспорту. Воно керує двигуном, гальмівними системами, стабілізацією, допомогою водієві, телематикою, діагностикою, оновленнями, навігацією, комунікаціями та взаємодією з користувачем. У програмно-визначених автомобілях частина функціональності може змінюватися після продажу через оновлення, активацію сервісів або зміну алгоритмів. Це підвищує гнучкість, але створює нові ризики для безпеки руху [3, 49, 1].

На відміну від механічних компонентів, програмне забезпечення не зношується фізично, але може містити дефекти проєктування, помилки вимог, некоректну реалізацію, проблеми інтеграції, невраховані граничні умови, вразливості безпеки або залежності від зовнішніх сервісів. Програмна помилка може проявлятися лише за певної комбінації даних, часу, версій, конфігурацій або станів мережі. Тому класичні підходи до надійності, побудовані лише на інтенсивності фізичних відмов, недостатні для оцінювання програмних ризиків.

Програмне забезпечення впливає на безпеку руху через три основні механізми. Перший — пряме керування фізичними функціями, наприклад гальмуванням, кермуванням або прискоренням. Другий — інформаційна

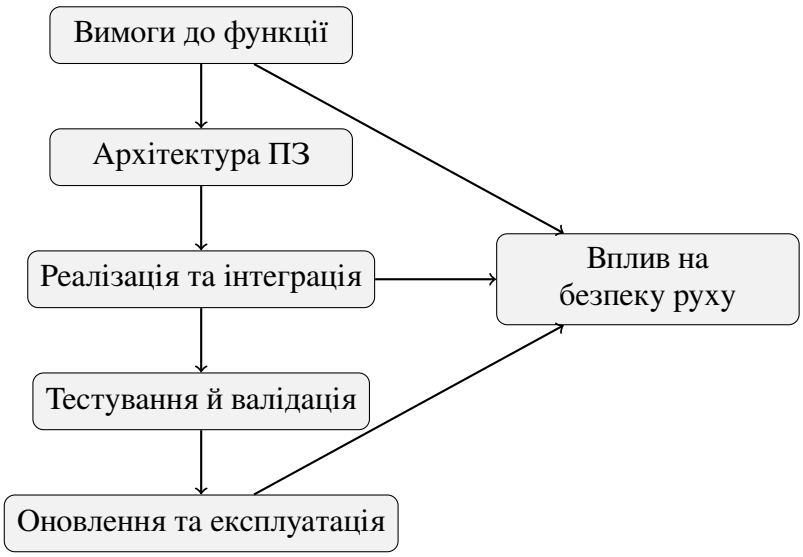

Рис. 4.2: Життєвий цикл програмної функції та її вплив на безпеку руху

підтримка водія або автоматизованої системи, наприклад попередження, навігація, розпізнавання об'єктів або прогноз дорожньої ситуації. Третій — організація взаємодії з іншими системами, наприклад V2X, хмарними сервісами, діагностикою або оновленнями. Помилка в кожному з цих механізмів може мати різну тяжкість наслідків.

Функціональна безпека відповідно до ISO 26262 орієнтована на зменшення ризиків, пов'язаних із відмовами електричних та електронних систем [2]. Проте автоматизовані функції можуть бути небезпечними навіть без класичної відмови, якщо вони неправильно сприймають складну дорожню ситуацію або працюють за межами передбаченого сценарію. Для цього застосовується підхід безпеки передбачуваної функціональності, пов'язаний з ISO 21448 [4]. У цифровізованому транспорті обидва підходи потрібно доповнювати кібербезпекою та керуванням оновленнями.

Ризик програмної функції можна подати як поєднання дефектності, експозиції та критичності:

$$R_{sw} = P_{def} \cdot E_{use} \cdot S_{crit}, \tag{4.7}$$

де P_{def} — імовірність наявності або активації дефекту, E_{use} — експозиція функції в реальних умовах, S_{crit} — тяжкість можливих наслідків. Наприклад, дефект у розважальній системі та дефект у функції автоматичного гальмування мають різну критичність навіть за однакової ймовірності прояву.

Оновлення програмного забезпечення є однією з найважливіших фун-

Табл. 4.2: Типові програмні ризики для автомобільного транспорту

Ризик	**Причина**	**Можливий наслідок**
Помилка вимог	Неповний опис сценаріїв або обмежень	Некоректна функція в реальній дорожній ситуації
Помилка реалізації	Дефект коду, пам'яті або логіки	Відмова, зависання, неправильна команда
Помилка інтеграції	Несумісність версій або інтерфейсів	Нестабільна робота доменів автомобіля
Помилка оновлення	Порушення пакета, процедури або конфігурації	Втрата функції або встановлення некоректної версії
Вразливість ПЗ	Недостатній захист, помилка доступу або API	Кібератака, зміна даних, компрометація сервісу

кцій сучасного автомобіля. Воно дає змогу виправляти помилки, закривати вразливості, покращувати функції та додавати сервіси. Проте саме оновлення може стати джерелом ризику, якщо пакет пошкоджений, підмінений, несумісний або недостатньо протестований. ISO 24089 і UN Regulation No. 156 підкреслюють необхідність керованого процесу оновлень, включно з ідентифікацією версій, оцінкою впливу, перевіркою цілісності, можливістю відновлення й документуванням [3, 10].

Для безпеки оновлень важливо оцінювати ймовірність успішного завершення процедури:

$$P_{upd} = P_{auth} \cdot P_{int} \cdot P_{comp} \cdot P_{rollback}, \tag{4.8}$$

де P_{auth} — імовірність коректної автентифікації джерела, P_{int} — імовірність збереження цілісності пакета, P_{comp} — імовірність сумісності з конфігурацією автомобіля, $P_{rollback}$ — імовірність успішного відновлення у разі помилки. Низьке значення будь-якого множника знижує надійність усього процесу.

Програмні функції, що використовують машинне навчання, створюють окремий клас ризиків. Їх поведінка залежить від навчальних даних, архітектури моделі, умов експлуатації та якості сенсорної інформації. Модель може працювати добре на тестових наборах, але помилятися в рідкісних погодних умовах, нетиповій дорожній розмітці або при змінених сенсорних характеристиках. Тому для таких функцій потрібні валідація на різноманітних сценаріях, моніторинг під час експлуатації та обмеження області застосування

[44, 47, 48, 71].

Важливим принципом є безпечна деградація. Якщо програмна функція не може працювати коректно, вона повинна перейти в стан, який не створює неприйнятного ризику. Для водійських систем це може означати попередження водія, відключення допоміжної функції або перехід до ручного керування. Для інфраструктурних сервісів — використання резервного плану світлофорного керування, локального режиму або ручного диспетчерського втручання.

Показник програмної стабільності можна оцінювати через кількість критичних дефектів на одиницю експлуатаційного часу або функціонального обсягу:

$$S_{sw} = 1 - \frac{N_{crit}}{N_{all} + 1}, \tag{4.9}$$

де N_{crit} — кількість критичних дефектів, а N_{all} — загальна кількість виявлених дефектів. Хоча такий показник є спрощеним, він допомагає відстежувати якість релізів і порівнювати версії програмного забезпечення.

Отже, програмне забезпечення є не допоміжним, а центральним фактором надійності автомобільного транспорту. Його вплив на безпеку руху проявляється через керуючі функції, інформаційні сервіси, оновлення, аналітику, кіберзахист і взаємодію з інфраструктурою. Надійність програмного забезпечення повинна забезпечуватися протягом усього життєвого циклу.

4.3 Відмови датчиків, електронних блоків керування та комунікаційних модулів

Датчики, електронні блоки керування та комунікаційні модулі утворюють технічну основу цифровізованого автомобільного транспорту. Датчики перетворюють фізичне середовище на дані; електронні блоки обробляють інформацію та формують команди; комунікаційні модулі забезпечують обмін із внутрішніми й зовнішніми системами. Відмова будь-якого з цих компонентів може вплинути на безпеку руху, якість сервісів або здатність ITS формувати правильні керуючі рішення [31, 45, 46].

Відмови датчиків можуть бути повними, частковими, періодичними або прихованими. Повна відмова означає відсутність сигналу. Часткова відмова проявляється у зниженні точності, збільшенні шуму, зміщенні калібрування або втраті частини функціональності. Періодична відмова виникає нерегулярно

й ускладнює діагностику. Прихована відмова є найнебезпечнішою, оскільки датчик продовжує передавати дані, але ці дані є помилковими. Для ITS прихована відмова може бути сприйнята як реальна транспортна подія.

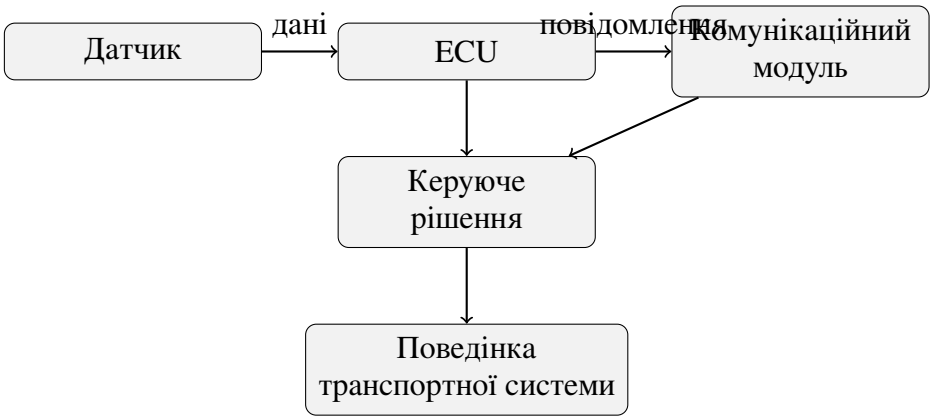

Рис. 4.3: Вплив відмов компонентів на керуюче рішення

Для датчиків автономних і підключених автомобілів характерні специфічні фактори деградації: забруднення, волога, температура, вібрації, засліплення, електромагнітні завади, старіння, некоректне калібрування та програмні помилки оброблення сигналу. Камери залежать від освітлення й видимості, радари можуть мати помилкові відбиття, лідари чутливі до забруднення оптики, GNSS-приймачі — до спуфінгу і втрати сигналу. Тому надійність сприйняття повинна забезпечуватися через сенсорне злиття й перевірку узгодженості [45, 46, 72].

Нехай система використовує n незалежних датчиків для підтвердження події, а імовірність коректної роботи i-го датчика дорівнює p_i. Для схеми, у якій достатньо хоча б одного достовірного джерела, імовірність доступності інформації становить:

$$P_{sense} = 1 - \prod_{i=1}^{n}(1 - p_i). \tag{4.10}$$

Якщо ж потрібне узгодження більшості датчиків, оцінювання стає складнішим, але загальний принцип залишається: різнорідне резервування зменшує ризик одиничної відмови, хоча не усуває спільні причини, наприклад складні погодні умови.

Електронні блоки керування можуть відмовляти через апаратні дефекти, перегрів, порушення живлення, помилки мікропрограми, некоректні вхідні

дані, перевантаження процесора або збої внутрішньої пам'яті. Для критичних блоків важливими є самодіагностика, контроль часу виконання, watchdog-механізми, перевірка пам'яті, безпечне завантаження, контроль цілісності програмного коду та перехід у безпечний стан. У сучасних архітектурах, де функції консолідуються в доменних або зональних контролерах, відмова одного блока може мати ширший вплив, ніж у традиційній розподіленій архітектурі [49, 2].

Табл. 4.3: Відмови компонентів цифрового автомобільного транспорту

Компонент	**Типові відмови**	**Наслідки**
Камера	Засліплення, забруднення, помилка розпізнавання	Неправильне сприйняття об'єктів і розмітки
Радар/лідар	Завади, відбиття, деградація калібрування	Помилкова відстань або швидкість об'єкта
GNSS	Втрата сигналу, спуфінг, мультипас	Некоректне місцезнаходження
ECU	Перегрів, дефект ПЗ, збій пам'яті	Втрата або неправильне виконання функції
Комунікаційний модуль	Втрата мережі, затримка, помилка протоколу	Недоступність V2X або телематичних сервісів

Комунікаційні модулі відповідають за зв'язок автомобіля з зовнішнім середовищем. Їх відмови можуть проявлятися як втрата з'єднання, збільшення затримки, висока частота помилок, нестабільна якість сигналу, некоректне перемикання між мережами, відмова SIM/eSIM, помилка сертифікатів або збій протоколу. Для ITS це особливо важливо, оскільки багато сервісів залежать від своєчасного обміну даними: V2X-попередження, дистанційна діагностика, оновлення, навігація, диспетчеризація й моніторинг автопарків [8, 26, 27].

Повна затримка цифрового транспортного сервісу може бути подана як:

$$T_{service} = T_{sense} + T_{proc} + T_{comm} + T_{decision} + T_{act}, \tag{4.11}$$

де T_{sense} — час вимірювання, T_{proc} — час оброблення, T_{comm} — час передавання, $T_{decision}$ — час прийняття рішення, T_{act} — час виконання дії. Якщо $T_{service}$ перевищує допустимий поріг, функція може стати непридатною для критичного застосування навіть без повної відмови компонента.

Для виявлення деградації датчиків і модулів використовують діагно-

стичні пороги, статистичний контроль, порівняння з резервними джерелами, моделі очікуваної поведінки та алгоритми виявлення аномалій. Наприклад, якщо швидкість, визначена за колесами, GNSS і інерційним датчиком, істотно розходиться, система повинна оцінити, яке джерело є недостовірним. Такий підхід важливий не лише для надійності, а й для кібербезпеки, оскільки атака на дані може виглядати як технічна відмова.

Для прогнозного обслуговування можна використовувати індекс деградації компонента:

$$D_c = \eta_1 \frac{e}{e_{max}} + \eta_2 \frac{T}{T_{max}} + \eta_3 \frac{n_f}{n_{max}} + \eta_4 \frac{\sigma}{\sigma_{max}}, \tag{4.12}$$

де e — кількість помилок, T — робоча температура, n_f — частота відмов або перезапусків, σ — рівень шуму вимірювань, а η_i — вагові коефіцієнти. Якщо D_c перевищує поріг, компонент потребує перевірки, калібрування або заміни.

Відмови компонентів можуть бути незалежними або залежними. Незалежні відмови виникають окремо, наприклад через дефект конкретного датчика. Залежні відмови мають спільну причину: помилка оновлення, відмова живлення, перегрів, кібератака, неправильна конфігурація або погодні умови. Для цифровізованого транспорту залежні відмови особливо небезпечні, оскільки можуть одночасно вплинути на багато компонентів або транспортних засобів.

Отже, датчики, ECU та комунікаційні модулі є критичними елементами надійності автомобільного транспорту в ITS. Їх відмови можуть мати фізичні, інформаційні та експлуатаційні наслідки. Захист від таких відмов потребує резервування, діагностики, сенсорного злиття, контролю затримок, прогнозного обслуговування, безпечної архітектури та узгодження з кібербезпековими механізмами.

4.4 Взаємозв'язок кібербезпеки, функціональної безпеки та експлуатаційної надійності

Кібербезпека, функціональна безпека та експлуатаційна надійність у сучасному автомобільному транспорті не можуть розглядатися окремо. Функціональна безпека спрямована на запобігання небезпеці, що виникає через відмови електричних та електронних систем. Кібербезпека спрямована на захист від навмисних дій, що порушують конфіденційність, цілісність, досту-

пність або автентичність. Експлуатаційна надійність характеризує здатність системи стабільно виконувати функції в реальних умовах. У ITS ці три сфери взаємно впливають одна на одну [2, 1, 4, 11].

Один і той самий небажаний наслідок може мати різну природу. Наприклад, некоректний сигнал датчика може бути спричинений фізичною відмовою, помилкою програмної обробки або кібератакою. Втрата V2X-повідомлення може бути наслідком радіозавад, перевантаження мережі, DoS-атаки або неправильної конфігурації. Неправильна команда виконавчому механізму може виникнути через дефект алгоритму, несправність ECU або компрометацію внутрішньої мережі. Тому аналіз причин повинен бути багатофакторним.

Рис. 4.4: Взаємозв'язок безпеки, кібербезпеки та надійності

Між кібербезпекою та функціональною безпекою можливі як синергії, так і конфлікти. Синергія виникає тоді, коли захисний механізм одночасно зменшує ризик кібератаки й випадкової відмови. Наприклад, перевірка цілісності програмного забезпечення захищає від підміни та допомагає виявити пошкодження. Конфлікт виникає тоді, коли захисний механізм створює затримку, блокує аварійний доступ або ускладнює безпечну деградацію. Тому вимоги безпеки й кібербезпеки повинні узгоджуватися на етапі архітектури.

Взаємозв'язок можна формалізувати через інтегральний показник прийнятності функції:

$$F_{acc} = S_f \cdot S_c \cdot A_e, \tag{4.13}$$

де S_f — рівень функціональної безпеки, S_c — рівень кіберзахищеності, A_e —

експлуатаційна готовність. Добуткова форма підкреслює, що слабкість будь-якої складової зменшує прийнятність функції загалом. Функція з високою функціональною безпекою, але низькою кіберзахищеністю, не може вважатися прийнятною для підключеного автомобіля.

Табл. 4.4: Перетин функціональної безпеки, кібербезпеки та надійності

Сфера	**Основне питання**	**Приклад для ITS**
Функціональна безпека	Що станеться при випадковій відмові?	Відмова гальмівного ECU або датчика швидкості
Кібербезпека	Що станеться при навмисній атаці?	Підроблення V2X-повідомлення або зміна ПЗ
Надійність	Чи буде система стабільно доступною?	Доступність центру керування або телематичного сервісу
SOTIF	Чи безпечна функція без відмови?	Неправильне сприйняття складної дорожньої сцени
Експлуатаційна стійкість	Чи може система відновитися?	Перехід до резервного режиму після збою

Особливе значення має спільний аналіз небезпек і загроз. Небезпека може бути спричинена як випадковою відмовою, так і атакою. Наприклад, втрата достовірності координат може розглядатися як небезпека для функції позиціонування та як загроза у разі GNSS-спуфінгу. Якщо ці аналізи проводяться окремо, можливі прогалини: функціональна безпека не врахує навмисного атакувальника, а кібербезпека не оцінить фізичну тяжкість наслідків. Інтегровані підходи, зокрема SAHARA та інші методики, спрямовані на подолання такого розриву [64, 73, 74].

Кіберінцидент може знижувати надійність навіть без прямого фізичного впливу. Наприклад, програма-вимагач у центрі керування може зробити недоступними панелі моніторингу, але світлофори локально продовжуватимуть працювати. Формально транспортний процес не зупиняється, однак експлуатаційна надійність знижується через втрату спостережуваності, координації та швидкого реагування. Так само витік даних може не вплинути на рух негайно, але призвести до відключення сервісу, правових обмежень або втрати довіри користувачів.

Для управління взаємозв'язком безпеки й надійності потрібні спільні вимоги. Вони повинні визначати критичність функції, допустимі відмови, допустимі затримки, вимоги до автентифікації, правила деградації, журнали подій, процедури оновлення, ролі відповідальних сторін і критерії відновлення. Якщо ці вимоги формуються окремо різними підрозділами, виникає ризик несумісності: кіберзахист може заважати експлуатації, а експлуатаційні обхідні процедури можуть послаблювати захист.

Інтегральний ризик цифровізованої транспортної функції можна подати як:

$$R_{total} = R_{fail} + R_{cyber} + R_{sotif} + R_{oper} - R_{mit}, \tag{4.14}$$

де R_{fail} — ризик випадкової відмови, R_{cyber} — кіберризик, R_{sotif} — ризик небезпечної поведінки без відмови, R_{oper} — експлуатаційний ризик, R_{mit} — зниження ризику завдяки захисним і організаційним заходам. Така модель допомагає показати, що ізольоване зменшення лише одного компонента не гарантує прийнятного загального рівня.

Практичне узгодження кібербезпеки, функціональної безпеки й надійності передбачає спільні рев'ю архітектури, спільні сценарії тестування, трасування вимог, аналіз впливу оновлень, контроль залишкового ризику, моніторинг під час експлуатації та регулярне навчання персоналу. Для автомобільного транспорту в ITS це особливо важливо через розподілену відповідальність між виробником, оператором дороги, постачальником зв'язку, центром керування, сервісною організацією та користувачем.

Отже, в умовах цифровізації надійність автомобільного транспорту неможливо забезпечити без інтеграції з кібербезпекою та функціональною безпекою. Сучасна ITS повинна проектуватися як система, здатна не лише працювати без відмов, а й протидіяти атакам, виявляти деградацію, переходити в безпечні режими та швидко відновлювати критичні функції.

4.5 Моделі оцінювання та практичні заходи підвищення надійності

Для практичного управління надійністю необхідно поєднувати кількісні моделі, інженерні процедури й експлуатаційні дані. Кількісні моделі дають змогу оцінити готовність, імовірність відмови, ефект резервування та очікувані втрати. Інженерні процедури визначають вимоги до архітектури, тестування, оновлень і діагностики. Експлуатаційні дані показують реальну поведінку

системи після введення в дію. Без поєднання цих трьох складових управління надійністю залишається фрагментарним.

Одним із практичних інструментів є аналіз критичності компонентів. Для кожного компонента визначають імовірність відмови, вплив на функцію, час виявлення, час відновлення, наявність резерву та можливість безпечної деградації. На основі цих параметрів формується рейтинг пріоритетів технічного обслуговування. Компоненти з високою критичністю повинні мати підвищені вимоги до моніторингу, запасних частин, резервування й регламентів перевірки.

Табл. 4.5: Практичні заходи підвищення надійності цифровізованого автомобільного транспорту

Напрям	**Заходи**	**Очікуваний ефект**
Архітектура	Сегментація, резервування, безпечні шлюзи	Обмеження поширення відмов і атак
Діагностика	Самоконтроль, журнали, контроль затримок	Раннє виявлення деградації
Оновлення	Підписані пакети, відкат, контроль версій	Зменшення ризику програмних відмов
Дані	Перевірка якості, сенсорне злиття, фільтрація	Зменшення хибних рішень
Експлуатація	Регламенти, навчання, резервні сценарії	Скорочення часу відновлення

Очікувані втрати від відмов можна оцінити як:

$$C_{fail} = \sum_{i=1}^{n} P_i(C_{repair,i} + C_{delay,i} + C_{safety,i} + C_{rep,i}), \tag{4.15}$$

де P_i — імовірність i-го сценарію відмови, $C_{repair,i}$ — витрати на ремонт, $C_{delay,i}$ — втрати від затримок, $C_{safety,i}$ — оцінка безпекових наслідків, $C_{rep,i}$ — репутаційні або організаційні втрати. Така модель допомагає обґрунтувати інвестиції в резервування, моніторинг і прогнозне обслуговування.

Для цифровізованого транспорту особливо корисним є перехід від планово-попереджувального до ризик-орієнтованого й прогнозного обслуговування. Планово-попереджувальний підхід спирається на фіксовані інтервали, тоді як прогнозний використовує фактичний стан компонента. Наприклад,

комунікаційний модуль можна перевіряти не лише за календарем, а й за зростанням кількості помилок, перезапусків, втрат пакетів або температурних перевищень. Такий підхід підвищує ефективність обслуговування та зменшує непередбачені простої [58, 59, 60].

Рис. 4.5: Цикл прогнозного забезпечення надійності

Важливою практичною вимогою є тестування деградаційних режимів. Система повинна перевірятися не лише в нормальних умовах, а й у ситуаціях втрати датчика, нестабільного зв'язку, затримки V2X-повідомлення, недоступності хмарного сервісу, помилки оновлення або компрометації окремого вузла. Такі випробування дають змогу переконатися, що система переходить у безпечний режим, а не створює новий ризик. Для автоматизованих транспортних функцій це має особливе значення [75, 76, 77].

Підвищення надійності також потребує управління конфігураціями. У складній ITS одночасно існують різні версії програмного забезпечення автомобілів, контролерів, RSU, серверів, мобільних застосунків і аналітичних моделей. Несумісність версій може стати причиною відмови або небезпечної поведінки. Тому необхідні реєстри конфігурацій, контроль залежностей, тестування сумісності, політики оновлення та можливість відкату.

Організаційний аспект не менш важливий за технічний. Навіть високонадійне обладнання не забезпечить стабільної роботи без регламентів, навченого персоналу, запасних компонентів, договорів підтримки, процедур реагування й аналізу інцидентів. Після кожної значної відмови або кіберінциденту необхідно проводити розбір причин, оновлювати матрицю ризиків, коригувати

регламенти та перевіряти, чи не повториться аналогічний сценарій.

Отже, моделі оцінювання та практичні заходи підвищення надійності мають бути інтегровані в повний життєвий цикл автомобільного транспорту в ITS. Надійність повинна плануватися на етапі архітектури, перевірятися під час тестування, підтримуватися в експлуатації, відновлюватися після інцидентів і вдосконалюватися на основі даних. Саме такий підхід відповідає умовам цифровізації, де технічні, програмні, комунікаційні й організаційні фактори діють одночасно.

4.6 Цифрові двійники, моніторинг і режими деградації

В умовах цифровізації одним із найперспективніших інструментів забезпечення надійності є цифровий двійник транспортної системи. Під цифровим двійником у цьому контексті доцільно розуміти динамічну модель автомобіля, транспортного коридору, інфраструктурного вузла або центру керування, яка постійно оновлюється на основі фактичних даних експлуатації. Цифровий двійник дає змогу порівнювати очікуваний стан системи з реальним, виявляти відхилення, прогнозувати деградацію, оцінювати наслідки відмов і перевіряти сценарії керування без небезпечного втручання в реальний рух.

Для автомобільного транспорту цифровий двійник може існувати на кількох рівнях. На рівні транспортного засобу він описує технічний стан агрегатів, датчиків, електронних блоків, програмних версій і комунікаційних модулів. На рівні маршруту або коридору він моделює потоки, затримки, світлофорні режими, події та пропускну здатність. На рівні центру керування він відображає доступність сервісів, стан каналів зв'язку, навантаження на операторів і якість даних. Така багаторівневість особливо важлива для ITS, де локальна відмова може мати мережеві наслідки [5, 6, 32].

Формально відхилення реального стану від цифрової моделі можна подати як:

$$\Delta x(t) = \left\| x_{real}(t) - x_{model}(t) \right\|, \tag{4.16}$$

де $x_{real}(t)$ — вектор фактичних параметрів, а $x_{model}(t)$ — очікуваний вектор стану за моделлю. Якщо $\Delta x(t)$ перевищує допустимий поріг, система повинна ініціювати діагностику. Для транспортного коридору такими параметрами можуть бути інтенсивність, середня швидкість, довжина черг, затримка, доступність контролерів і кількість помилок датчиків.

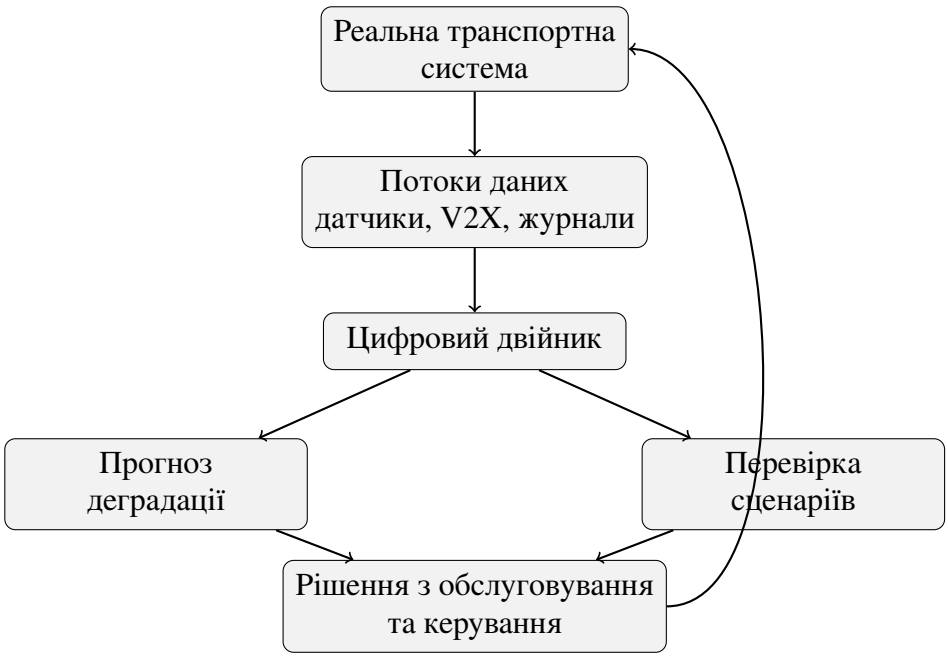

Рис. 4.6: Використання цифрового двійника для підтримки надійності ITS

Моніторинг надійності має охоплювати технічні, програмні, комунікаційні й організаційні показники. Технічні показники включають температуру, напругу, кількість перезапусків, помилки пам'яті та стан датчиків. Програмні показники включають версію, частоту помилок, час відповіді, завантаження процесора, журнали винятків і результати самотестування. Комунікаційні показники включають затримку, втрати пакетів, рівень сигналу, доступність мережі й кількість відмов сертифікатів. Організаційні показники включають час реагування, час відновлення, доступність персоналу та виконання регламентів.

Деградаційні режими є обов'язковим елементом надійної ITS. Деградаційний режим означає, що система втрачає частину функціональності, але зберігає контрольовану й безпечну роботу. Наприклад, у разі втрати зв'язку з центром керування світлофорний контролер може перейти на локальний план. У разі втрати одного датчика автомобіль може використовувати інші джерела або обмежити функцію допомоги водієві. У разі недоступності хмарної аналітики навігаційний сервіс може використовувати останні локальні дані з попередженням про обмежену актуальність.

Для оцінювання якості деградації можна ввести коефіцієнт збереження функції:

$$G_f = \frac{F_{deg}}{F_{nom}}, \tag{4.17}$$

де F_{deg} — функціональна спроможність у деградаційному режимі, а F_{nom} —

Табл. 4.6: Показники моніторингу надійності цифровізованої ITS

Група показників	**Приклади**	**Призначення**
Технічні	Температура, живлення, перезапуски, помилки датчиків	Виявлення фізичної деградації
Програмні	Версія, винятки, час відповіді, стан оновлень	Контроль стабільності ПЗ
Комунікаційні	Затримка, втрата пакетів, доступність V2X/4G/5G	Оцінювання якості зв'язку
Дані	Повнота, точність, узгодженість, своєчасність	Запобігання хибним рішенням
Організаційні	Час реагування, виконання регламентів, доступність персоналу	Оцінювання відновлюваності

номінальна функціональна спроможність. Якщо $G_f = 1$, функція збережена повністю; якщо $G_f = 0$, функція втрачена. Для критичних сервісів важливо, щоб G_f не опускався нижче мінімального безпечного рівня.

Деградаційні режими повинні бути не випадковою реакцією, а наперед визначеною частиною архітектури. Для кожної критичної функції потрібно описати умови переходу, доступні резерви, обмеження, повідомлення оператору або водієві, допустимий час роботи в деградаційному режимі та процедуру повернення до нормального стану. Без такого опису система може поводитися непередбачувано саме тоді, коли потрібна найвища стабільність.

4.7 Керування надійністю протягом життєвого циклу

Надійність автомобільного транспорту в умовах цифровізації повинна підтримуватися протягом усього життєвого циклу. На етапі планування визначаються критичні функції, допустимі рівні ризику, вимоги до доступності, резервування та відновлення. На етапі проєктування формується архітектура, яка враховує відмови, атаки, деградаційні режими й оновлення. На етапі інтеграції перевіряється сумісність компонентів. На етапі експлуатації здійснюється моніторинг, обслуговування, оновлення й реагування. На етапі модернізації оцінюється вплив змін на безпеку й надійність [1, 3, 10].

Життєвий цикл надійності тісно пов'язаний з управлінням конфігураціями. У транспортній системі можуть одночасно працювати автомобілі з різними

версіями програмного забезпечення, різні покоління дорожніх контролерів, різні прошивки RSU, різні карти, різні профілі сертифікатів і різні версії аналітичних моделей. Якщо ці конфігурації не контролюються, виникають приховані ризики несумісності. Тому необхідний реєстр активів і конфігурацій, у якому фіксуються версії, залежності, критичність, історія оновлень і відповідальні особи.

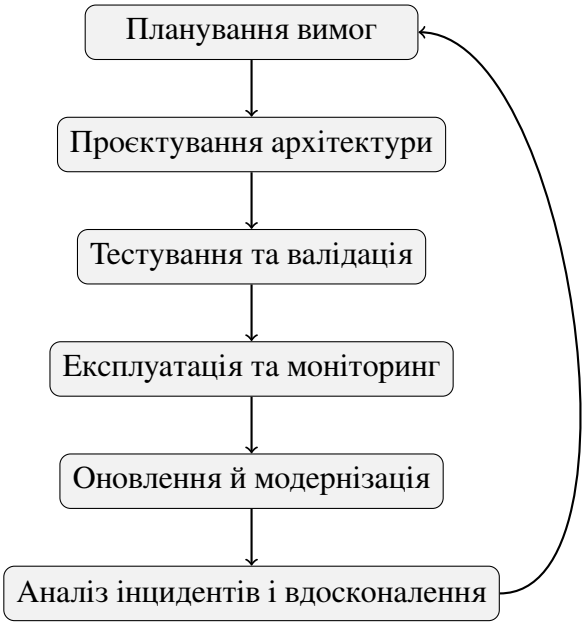

Рис. 4.7: Життєвий цикл управління надійністю цифровізованого транспорту

Після кожної відмови або значного інциденту потрібно виконувати аналіз першопричин. Його мета полягає не лише у відновленні роботи, а й у запобіганні повторенню. Якщо відмова була спричинена дефектом компонента, потрібно оцінити партію, умови експлуатації та регламенти заміни. Якщо причиною була помилка програмного забезпечення, необхідно переглянути вимоги, тестування й процедури оновлення. Якщо інцидент пов'язаний з організаційною дією, потрібно змінити процедури, навчання або розподіл прав доступу.

Ефективність життєвого циклу можна оцінити через коефіцієнт навчання системи:

$$L_c = \frac{N_{closed}}{N_{incidents}}, \tag{4.18}$$

де N_{closed} — кількість інцидентів, за якими виконано аналіз причин і впроваджено коригувальні дії, а $N_{incidents}$ — загальна кількість значних інцидентів. Якщо L_c низький, система повторюватиме ті самі помилки, навіть якщо окремі

відмови швидко усуваються.

Важливо також враховувати старіння цифрових компонентів. Програмне забезпечення може втрачати актуальність через появу нових вразливостей, припинення підтримки бібліотек, зміну протоколів, несумісність із новими сервісами або накопичення технічного боргу. Комунікаційні модулі можуть застарівати через зміну поколінь мереж. Дорожні контролери можуть працювати десятиліттями, тоді як цифрові вимоги змінюються значно швидше. Тому життєвий цикл надійності повинен містити план модернізації, а не лише ремонт після відмови.

Організаційна відповідальність має бути чітко розподілена. Виробник автомобіля відповідає за архітектуру, програмне забезпечення й оновлення транспортного засобу. Оператор дороги відповідає за інфраструктуру та локальні режими керування. Центр керування відповідає за моніторинг, координацію та реагування. Постачальник зв'язку відповідає за доступність мережевих сервісів. Постачальник цифрової платформи відповідає за оброблення даних і доступність сервісів. Без такого розподілу навіть технічно якісна система може мати низьку фактичну надійність.

4.8 Узагальнення вимог до надійності цифровізованого автомобільного транспорту

Узагальнюючи розгляд, можна визначити групу вимог, які повинні виконуватися для забезпечення надійності автомобільного транспорту в ITS. По-перше, архітектура має бути стійкою до одиничних відмов і передбачати резервування критичних функцій. По-друге, програмне забезпечення має розроблятися, тестуватися й оновлюватися відповідно до контрольованого життєвого циклу. По-третє, датчики й комунікаційні модулі повинні постійно контролюватися на предмет деградації. По-четверте, кібербезпека має бути інтегрована з функціональною безпекою. По-п'яте, експлуатаційні процеси повинні забезпечувати швидке відновлення.

Інтегральну готовність цифровізованої транспортної функції можна подати як:

$$A_{func} = A_{hw} \cdot A_{sw} \cdot A_{comm} \cdot A_{data} \cdot A_{org}, \tag{4.19}$$

де A_{hw} — готовність апаратної частини, A_{sw} — готовність програмного

Табл. 4.7: Узагальнені вимоги до надійності в умовах цифровізації

Вимога	**Зміст**	**Очікуваний результат**
Стійка архітектура	Резервування, сегментація, безпечна деградація	Зменшення каскадних відмов
Кероване ПЗ	Контроль версій, тестування, безпечні оновлення	Менше програмних інцидентів
Якісні дані	Перевірка, фільтрація, сенсорне злиття	Коректні керуючі рішення
Кіберстійкість	Автентифікація, моніторинг, реагування	Захист від навмисних впливів
Відновлюваність	Резервні сценарії, навчання, запасні ресурси	Скорочення часу простою

забезпечення, A_{comm} — готовність комунікацій, A_{data} — готовність і якість даних, A_{org} — організаційна готовність. Добуткова форма показує, що низька готовність будь-якої складової знижує готовність функції загалом.

Надійність автомобільного транспорту в умовах цифровізації має оцінюватися не тільки за фактом відмов, а й за здатністю системи попереджати відмови, обмежувати їх наслідки та відновлюватися. Це означає, що ключовими стають не лише показники $MTBF$ і $MTTR$, а й якість моніторингу, повнота журналювання, швидкість діагностики, ефективність оновлень, готовність персоналу й актуальність моделей ризику.

Таким чином, цифровізація не скасовує класичну теорію надійності, але суттєво розширює її. У сучасному автомобільному транспорті надійність формується на перетині механіки, електроніки, програмного забезпечення, даних, комунікацій, кібербезпеки та організаційного управління. Саме такий комплексний підхід дає змогу забезпечити безпечну й стійку роботу ITS у реальних умовах експлуатації.

5 Методи забезпечення кібербезпеки в інтелектуальних транспортних системах

Забезпечення кібербезпеки в інтелектуальних транспортних системах є комплексним інженерним і організаційним завданням. Воно не може бути зведене лише до встановлення криптографічного модуля, міжмережевого екрана або системи виявлення вторгнень. ITS поєднує автомобілі, дорожню інфраструктуру, V2X-комунікації, центри керування, телематичні платформи, мобільні застосунки, хмарні сервіси й бази даних. Тому методи захисту повинні охоплювати весь життєвий цикл: проєктування, виробництво, інтеграцію, експлуатацію, оновлення, моніторинг і реагування на інциденти [1, 9, 11, 12].

Головна особливість кібербезпеки ITS полягає в тому, що цифровий інцидент може мати фізичний транспортний наслідок. Порушення автентичності V2X-повідомлення може вплинути на маневр транспортного засобу; помилка оновлення може відключити критичну функцію; компрометація телематичної платформи може призвести до витоку геолокаційних даних; атака на центр керування може порушити організацію руху. Отже, методи захисту повинні оцінюватися не лише за інформаційними критеріями, а й за впливом на безпеку руху, надійність і відновлюваність [2, 4, 40, 39].

У цьому розділі розглядаються ключові групи методів забезпечення кібербезпеки: автентифікація та шифрування даних; системи виявлення вторгнень для автомобільних мереж; захист CAN, Ethernet і бездротових каналів; безпечне оновлення програмного забезпечення; управління доступом і захист телематичних платформ. Додатково подано питання інтегрованої архітектури захисту, оцінювання ефективності заходів і організації моніторингу.

5.1 Автентифікація та шифрування даних

Автентифікація та шифрування є базовими механізмами захисту даних в ITS. Автентифікація дає змогу переконатися, що повідомлення, команда, запит або оновлення походить від легітимного джерела. Шифрування забезпечує конфіденційність даних під час передавання або зберігання. Контроль цілісності підтверджує, що дані не були змінені. Для автомобільного транспор-

ту ці механізми мають особливе значення, оскільки дані можуть впливати на поведінку транспортного засобу, режим світлофора, маршрут, попередження або рішення оператора [16, 17, 20, 21].

У V2X-середовищі автентифікація складніша, ніж у класичних корпоративних мережах. Транспортні засоби рухаються швидко, взаємодіють з невідомими учасниками, передають короткі повідомлення й не завжди мають можливість встановлювати довгу сесію. Крім того, потрібно одночасно забезпечити довіру та приватність: одержувач має знати, що повідомлення справжнє, але не повинен отримувати зайву можливість постійно відстежувати конкретний автомобіль. Тому в ITS широко застосовуються цифрові підписи, сертифікати, псевдонімні ідентичності й інфраструктура відкритих ключів [16, 17, 41].

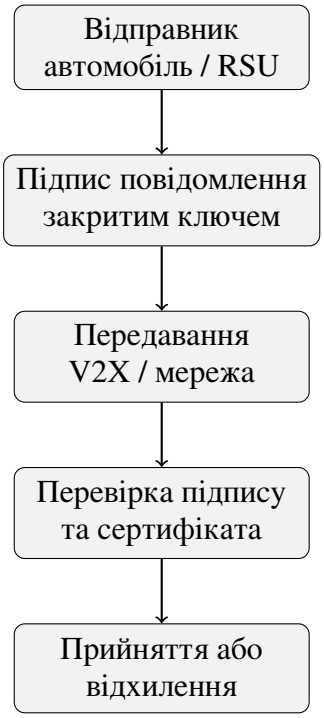

Рис. 5.1: Узагальнена схема автентифікації V2X-повідомлення

Криптографічний захист повідомлення можна подати у вигляді перетворень:

$$C = E_K(M), \qquad M = D_K(C), \tag{5.1}$$

де M — відкрите повідомлення, C — шифротекст, E_K — операція шифрування ключем K, D_K — операція розшифрування. Для контролю цілісності

може використовуватися код автентифікації повідомлення:

$$MAC = H_K(M), \tag{5.2}$$

де H_K — ключова хеш-функція. Для цифрового підпису використовується пара ключів:

$$Sig = Sign_{SK}(h(M)), \qquad Verify_{PK}(Sig, h(M)) \in \{0, 1\}, \tag{5.3}$$

де SK — закритий ключ, PK — відкритий ключ, $h(M)$ — хеш повідомлення.

Табл. 5.1: Криптографічні механізми та їх призначення в ITS

Механізм	**Захищена властивість**	**Приклад застосування**
Симетричне шифрування	Конфіденційність і швидкість оброблення	Захист телематичних сесій і сховищ
Асиметрична криптографія	Автентифікація й обмін ключами	V2X-сертифікати, підпис оновлень
Цифровий підпис	Цілісність, автентичність, невідмовність	CAM/DENM, пакети ПЗ, команди керування
Хеш-функція	Контроль незмінності даних	Перевірка прошивок, журналів, конфігурацій
Псевдонімні сертифікати	Довіра з обмеженням відстеження	Захист приватності V2X-учасників

Ефективність автентифікації залежить не лише від алгоритму, а й від керування ключами. Ключі повинні генеруватися безпечно, зберігатися в захищених модулях, оновлюватися, відкликатися у разі компрометації та використовуватися лише відповідно до політики. У транспортній системі це складно через велику кількість транспортних засобів, довгий життєвий цикл, перетин юрисдикцій і потребу в безперервній роботі. Компрометація ключа може перетворити легітимний вузол на джерело підписаних, але шкідливих повідомлень.

Імовірність прийняття повідомлення як достовірного можна оцінювати з урахуванням криптографічної та семантичної перевірки:

$$P_{trust} = P_{cert} \cdot P_{sig} \cdot P_{time} \cdot P_{plaus}, \tag{5.4}$$

де P_{cert} — імовірність дійсності сертифіката, P_{sig} — успішність перевірки

підпису, P_{time} — актуальність часової мітки, P_{plaus} — фізична правдоподібність повідомлення. Ця формула підкреслює, що цифровий підпис не замінює перевірку змісту повідомлення.

Для захисту телематичних платформ важливим є шифрування каналів між автомобілем, мобільним застосунком і хмарним сервісом. Однак використання захищеного каналу не гарантує безпеку всієї системи, якщо слабкою є автентифікація користувача, неправильно налаштовані API, надмірні права доступу або відсутній контроль сесій. Тому криптографія має бути частиною ширшої архітектури захисту [52, 54, 11].

Окрему роль відіграє захист даних у стані зберігання. Телематичні бази, журнали подій, ключі, діагностичні записи, профілі користувачів і історія маршрутів повинні зберігатися з урахуванням конфіденційності й цілісності. Для критичних журналів важливо забезпечувати незмінність або можливість виявити зміну. Наприклад, ланцюгове хешування журналів можна подати як:

$$H_i = h(H_{i-1} \parallel Event_i \parallel t_i), \tag{5.5}$$

де H_i — хеш поточного запису, $Event_i$ — подія, t_i — часова мітка. Зміна попереднього запису змінить увесь наступний ланцюг.

Табл. 5.2: Типові помилки впровадження криптографії в ITS

Помилка	**Наслідок**	**Запобігання**
Статичні або довгоживучі ключі	Високий вплив компрометації	Ротація ключів, HSM, відкликання
Відсутність перевірки сертифіката	Прийняття підробленого вузла	Повна перевірка ланцюга довіри
Шифрування без автентифікації	Можливість зміни повідомлення	AEAD або MAC
Незахищені журнали	Приховування інцидентів	Хеш-ланцюги, підписи, аудит
Ігнорування приватності	Відстеження транспортного засобу	Псевдоніми, мінімізація даних

Таким чином, автентифікація та шифрування створюють базовий рівень довіри в ITS. Проте їх ефективність залежить від правильного керування ключами, перевірки сертифікатів, захисту приватності, контролю цілісності, журналювання та поєднання з іншими методами, зокрема виявленням аномалій і управлінням доступом.

5.2 Системи виявлення вторгнень для автомобільних мереж

Системи виявлення вторгнень (IDS) є важливим методом забезпечення кібербезпеки автомобільних мереж, оскільки не всі атаки можна повністю запобігти на етапі автентифікації або сегментації. IDS призначена для виявлення підозрілої поведінки, аномального трафіку, відхилень у часових характеристиках, нетипових команд, ознак сканування, ін'єкції повідомлень або компрометації вузлів. Для автомобільних систем IDS має працювати з обмеженими ресурсами, в реальному часі та з урахуванням критичності помилкових спрацювань [65, 66, 67, 56].

IDS для автомобільних мереж можна поділити на сигнатурні, аномальні, специфікаційні та гібридні. Сигнатурні системи шукають відомі шаблони атак. Вони ефективні проти відомих загроз, але слабші проти нових сценаріїв. Аномальні системи будують модель нормальної поведінки й виявляють відхилення. Вони здатні виявляти нові атаки, але можуть давати більше помилкових спрацювань. Специфікаційні системи спираються на правила допустимої поведінки, наприклад періодичність CAN-повідомлень або допустимі діапазони параметрів. Гібридні системи поєднують кілька підходів.

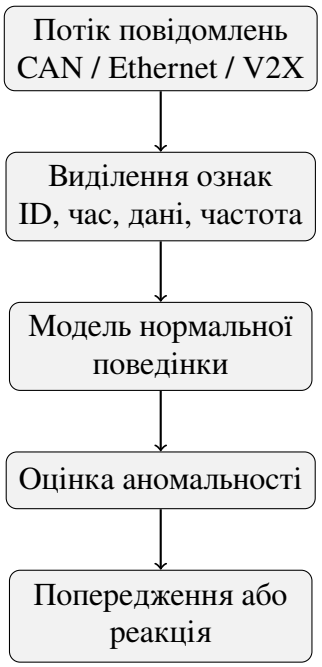

Рис. 5.2: Узагальнена архітектура IDS для автомобільних мереж

Для CAN-мереж типовими ознаками IDS є ідентифікатор повідомлення, періодичність, довжина даних, статистика байтів, зміни фізичних параметрів, послідовність повідомлень і кореляція між сигналами. Якщо повідомлення

з певним ідентифікатором має надходити кожні τ мілісекунд, то відхилення можна оцінити як:

$$\Delta t_i = |t_i - t_{i-1} - \tau|. \tag{5.6}$$

Якщо $\Delta t_i > \theta_t$, де θ_t — допустимий поріг, IDS може сформувати попередження про можливу ін'єкцію, втрату або придушення повідомлення.

Аномальність значення сигналу можна оцінювати через нормалізоване відхилення:

$$z_i = \frac{x_i - \mu_i}{\sigma_i}, \tag{5.7}$$

де x_i — поточне значення сигналу, μ_i — очікуване середнє, σ_i — стандартне відхилення. Якщо $|z_i|$ перевищує поріг, сигнал вважається підозрілим. Для автомобіля важливо враховувати фізичний контекст: різка зміна швидкості, кута керма або прискорення повинна відповідати можливій динаміці транспортного засобу.

Табл. 5.3: Підходи до IDS для автомобільних мереж

Тип IDS	**Переваги**	**Обмеження**
Сигнатурна	Низька кількість хибних спрацювань для відомих атак	Погано виявляє нові атаки
Аномальна	Може виявляти невідомі сценарії	Потребує якісної моделі нормальної поведінки
Специфікаційна	Добре враховує правила автомобільної мережі	Потребує точних специфікацій повідомлень
ML/DL-орієнтована	Виявляє складні закономірності	Потребує даних, валідації та пояснюваності
Гібридна	Баланс точності та гнучкості	Складніша інтеграція й обслуговування

Якість IDS оцінюється через показники істинно позитивних, хибно позитивних, істинно негативних і хибно негативних спрацювань. Основні метрики мають вигляд:

$$Precision = \frac{TP}{TP + FP}, \qquad Recall = \frac{TP}{TP + FN}, \tag{5.8}$$

$$F_1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}. \tag{5.9}$$

Для автомобільних систем важливо не лише максимізувати F_1, а й контро-

лювати хибно негативні спрацювання для критичних атак і хибно позитивні спрацювання, які можуть перевантажити водія або оператора.

IDS може бути розміщена на рівні окремого ECU, центрального шлюзу, телематичного модуля, доменного контролера, центру керування або хмарної платформи. Локальна IDS має меншу затримку й краще підходить для критичних повідомлень, але має обмежені ресурси. Хмарна IDS може використовувати великі обсяги даних і складні моделі, але залежить від зв'язку й не завжди придатна для миттєвої реакції. Тому перспективною є багаторівнева IDS-архітектура [55, 57, 56].

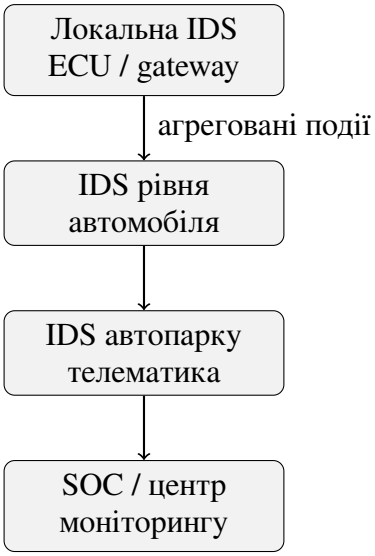

Рис. 5.3: Багаторівневе розміщення IDS у цифровому автомобільному транспорті

Важливим є питання реакції на виявлену атаку. IDS може лише повідомляти про подію або автоматично ініціювати захисну дію: блокування повідомлення, ізоляцію вузла, перехід у деградаційний режим, запис журналу, повідомлення оператора чи відкликання сертифіката. Автоматична реакція повинна бути обережною, оскільки помилкове блокування критичного повідомлення може бути небезпечним. Тому для критичних функцій реакції мають проходити аналіз функціональної безпеки [2, 1].

Для оцінювання корисності IDS можна використати модель очікуваного зменшення ризику:

$$\Delta R_{IDS} = R_0 \cdot P_{detect} \cdot P_{response} \cdot (1 - P_{harm}), \tag{5.10}$$

де R_0 — початковий ризик, P_{detect} — імовірність виявлення атаки, $P_{response}$ —

імовірність ефективної реакції, P_{harm} — імовірність шкоди від неправильної реакції. Така модель підкреслює, що IDS має сенс лише тоді, коли виявлення пов'язане з коректним реагуванням.

Отже, IDS є необхідним елементом багаторівневого захисту автомобільних мереж. Вона доповнює криптографію, сегментацію та управління доступом, виявляючи ті атаки й відмови, які не були заблоковані на попередніх рівнях. Найбільш перспективними є гібридні IDS, що поєднують правила, статистику, машинне навчання та фізичну правдоподібність транспортної поведінки.

5.3 Захист бортових і бездротових каналів зв'язку

Автомобільні мережі мають різну природу, тому методи їх захисту також відрізняються. CAN історично орієнтований на простоту, детермінованість і надійність обміну в реальному часі. Automotive Ethernet забезпечує більшу пропускну здатність і підтримує сервісно-орієнтовані архітектури. Бездротові канали, зокрема V2X, Wi-Fi, Bluetooth, 4G/5G і GNSS, забезпечують взаємодію автомобіля із зовнішнім світом. Кожна з цих технологій має власні вразливості й потребує спеціалізованого захисту [23, 22, 26, 27, 49].

CAN залишається поширеною внутрішньою мережею автомобіля. Її головні проблеми з погляду кібербезпеки — відсутність вбудованої автентифікації повідомлень, широкомовна природа, обмежений розмір кадру, пріоритетність за ідентифікатором і складність додавання криптографії без впливу на затримку. Захист CAN зазвичай передбачає сегментацію, фільтрацію на шлюзах, IDS, контроль діагностичного доступу, автентифікацію критичних повідомлень і безпечну конфігурацію ECU [65, 66, 69, 50].

Для CAN-фільтрації на шлюзі можна визначити правило доступу:

$$Allow(m) = \begin{cases} 1, & id(m) \in ID_{allowed} \wedge domain(m) \in D_{valid}, \\ 0, & \text{інакше.} \end{cases} \tag{5.11}$$

де $id(m)$ — ідентифікатор повідомлення, $ID_{allowed}$ — дозволені ідентифікатори, $domain(m)$ — домен походження, D_{valid} — допустимі домени. Для критичних повідомлень правило може доповнюватися перевіркою часової періодичності, діапазону значень і автентифікації.

Табл. 5.4: Порівняння каналів автомобільної комунікації та методів захисту

Канал	**Типові загрози**	**Методи захисту**	**Критичність**
CAN	Ін'єкція, повторне відтворення, DoS	Шлюзи, IDS, SecOC, діагностичний контроль	Висока
Ethernet	Сканування, бічне переміщення, підміна сервісів	VLAN, MACsec/TLS, сегментація, firewall	Висока
V2X	Підроблення, атаки Сивілли, придушення каналу	PKI, підписи, псевдоніми, перевірка правдоподібності	Висока
Wi-Fi/Bluetooth	Несанкціонований доступ, слабке спарювання	Захищені профілі, оновлення, обмеження сервісів	Середня/висока
4G/5G	DDoS, API-атаки, SIM-ризики	VPN/TLS, APN, моніторинг, керування ключами	Висока

Automotive Ethernet відкриває нові можливості для високошвидкісних функцій, камер, радарів, зональних контролерів і сервісно-орієнтованої архітектури. Проте разом із цим з'являються загрози, характерні для IP-мереж: сканування, підміна сервісів, атаки на маршрутизацію, неправильна сегментація, DoS, вразливості стеків і небезпечні API. Захист Ethernet передбачає VLAN, міжмережеві екрани, контроль доступу до сервісів, TLS, MACsec, IDS, контроль конфігурацій і мінімізацію відкритих портів [49, 1].

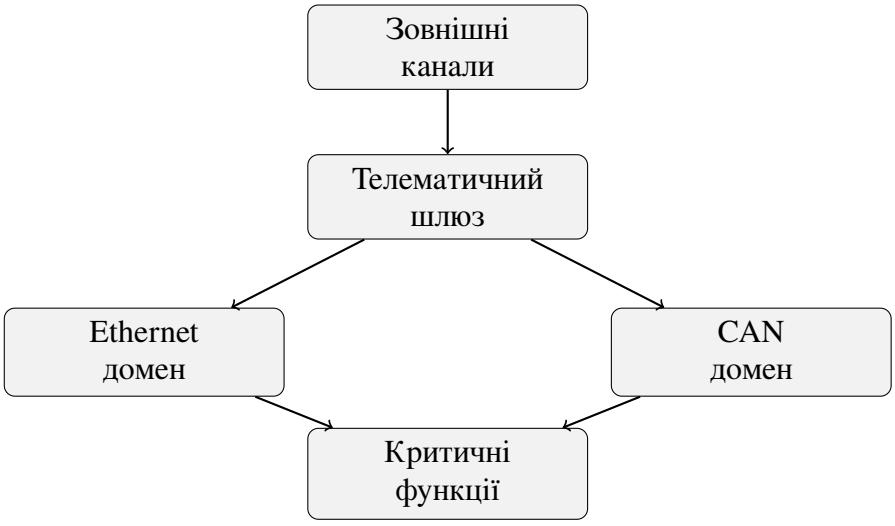

Рис. 5.4: Сегментація автомобільних каналів зв'язку

Бездротові канали потребують захисту через відкритість середовища. Wi-Fi і Bluetooth можуть використовуватися для мультимедіа, діагностики, мобільних застосунків і підключення користувачів. Якщо ці інтерфейси неправильно налаштовані, вони можуть стати початковим вектором атаки. Необхідно обмежувати доступні сервіси, використовувати захищене спарювання, відключати непотрібні профілі, оновлювати стеки протоколів і не допускати прямого переходу з користувацького домену до критичних мереж.

Для V2X важливо поєднувати криптографію й фізичну правдоподібність. Повідомлення з правильним підписом може бути небезпечним, якщо вузол скомпрометований або датчик помилковий. Тому перевірка повинна включати не лише сертифікат, а й координати, швидкість, напрям руху, часову мітку та відповідність дорожній ситуації. Функція довіри до повідомлення може бути описана як:

$$T_m = w_1 C_{cert} + w_2 C_{time} + w_3 C_{geo} + w_4 C_{kin} + w_5 C_{hist}, \tag{5.12}$$

де C_{cert} — довіра до сертифіката, C_{time} — актуальність часу, C_{geo} — географічна релевантність, C_{kin} — кінематична правдоподібність, C_{hist} — історія поведінки вузла.

Захист каналів також вимагає керування пропускною здатністю та затримкою. Надмірний криптографічний або фільтраційний контроль може вплинути на реальний час. Тому для критичних повідомлень потрібно оцінювати:

$$T_{secure} = T_{base} + T_{crypto} + T_{filter} + T_{ids}, \tag{5.13}$$

де T_{base} — базова затримка передавання, T_{crypto} — час криптографічної обробки, T_{filter} — час фільтрації, T_{ids} — час аналізу IDS. Має виконуватися умова $T_{secure} \leq T_{max}$.

Отже, захист CAN, Ethernet і бездротових каналів має будуватися за принципом багаторівневої оборони. Неможливо покладатися лише на один механізм. Потрібні сегментація, криптографія, IDS, контроль доступу, фільтрація, безпечні протоколи, моніторинг і тестування в умовах затримок, завад і деградації.

Табл. 5.5: Приклади правил безпечної сегментації автомобільної мережі

Правило	**Зміст**	**Очікуваний ефект**
Ізоляція мультимедіа	Розважальні сервіси не мають прямого доступу до шасі	Обмеження бічного переміщення
Контроль діагностики	Доступ лише з автентифікацією й журналюванням	Захист від сервісного зловживання
Шлюзова фільтрація	Дозвіл лише потрібних ID і сервісів	Зменшення ін'єкцій і DoS
Захист V2X	Підпис, сертифікат, перевірка правдоподібності	Захист кооперативних повідомлень
Обмеження API	Мінімальні права й перевірка токенів	Захист телематичних сервісів

5.4 Безпечне оновлення програмного забезпечення

Безпечне оновлення програмного забезпечення є критичним методом підтримки кібербезпеки й надійності сучасного автомобільного транспорту. Оновлення дозволяє усувати вразливості, виправляти дефекти, покращувати функції, змінювати конфігурації, оновлювати сертифікати та адаптувати систему до нових вимог. Водночас процес оновлення сам є високоризиковим: підміна пакета, помилка сумісності, переривання встановлення або неправильний відкат можуть призвести до відмови функцій чи компрометації системи [3, 10, 1].

Безпечний процес оновлення повинен відповідати кільком принципам: автентичність джерела, цілісність пакета, сумісність з конфігурацією, контроль версій, захищене передавання, перевірка перед встановленням, можливість відновлення, журналювання та оцінка впливу на безпеку. Для автомобіля особливо важливо, щоб оновлення не порушувало функціональну безпеку й не встановлювалося в небезпечний момент, наприклад під час критичного маневру або в умовах низького заряду живлення.

Перевірка пакета оновлення може бути формалізована як набір умов:

$$Valid(U) = Auth(U) \land Int(U) \land Comp(U, V) \land Safe(S), \tag{5.14}$$

де $Auth(U)$ — перевірка автентичності джерела, $Int(U)$ — цілісність пакета, $Comp(U, V)$ — сумісність з поточною версією V, $Safe(S)$ — безпечний стан

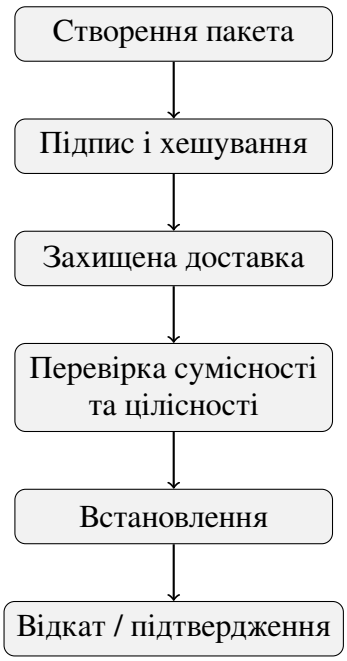

Рис. 5.5: Етапи безпечного оновлення програмного забезпечення

системи для встановлення. Якщо хоча б одна умова не виконується, оновлення має бути відхилене або відкладене.

Табл. 5.6: Ризики оновлення ПЗ та методи контролю

Ризик	**Наслідок**	**Метод контролю**
Підміна пакета	Встановлення шкідливого ПЗ	Цифровий підпис, перевірка сертифіката
Пошкодження пакета	Збій встановлення	Хеш, контроль цілісності, повторне завантаження
Несумісність версій	Втрата функції або помилки інтеграції	Реєстр конфігурацій, попередня перевірка
Переривання оновлення	Непрацездатний ECU або сервіс	A/B-розділи, відкат, контроль живлення
Неврахований вплив	Новий ризик безпеки або надійності	Аналіз впливу, тестування, журналювання

Для оцінювання надійності процесу оновлення можна використати показник:

$$R_{upd} = P_{auth} \cdot P_{int} \cdot P_{comp} \cdot P_{install} \cdot P_{rec}, \tag{5.15}$$

де P_{auth} — імовірність правильної автентифікації, P_{int} — імовірність збереження цілісності, P_{comp} — імовірність сумісності, $P_{install}$ — імовірність успішного встановлення, P_{rec} — імовірність відновлення після збою. Низьке значення будь-якої складової зменшує надійність усього процесу.

Оновлення повинні супроводжуватися аналізом впливу на кібербезпеку, функціональну безпеку та експлуатаційну надійність. Якщо змінюється алгоритм ADAS, потрібно оцінити його поведінку в дорожніх сценаріях. Якщо оновлюється криптографічна бібліотека, потрібно перевірити сумісність сертифікатів. Якщо змінюється телематичний API, потрібно оцінити вплив на мобільні застосунки й серверні сервіси. Керування оновленнями має бути пов'язане з керуванням конфігураціями.

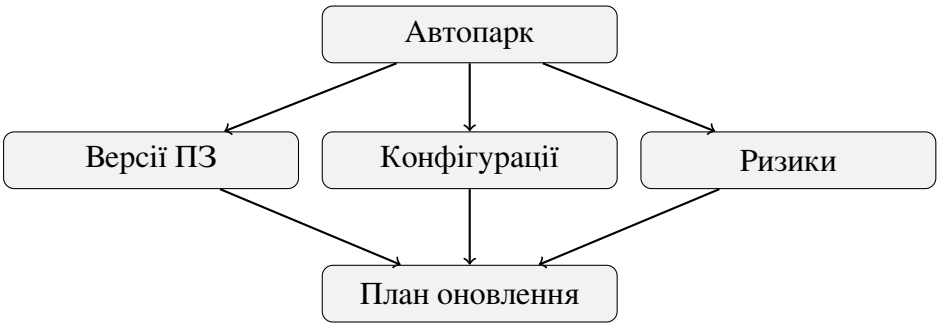

Рис. 5.6: Планування оновлень з урахуванням версій, конфігурацій і ризиків

Важливим є поетапне розгортання оновлень. Для великого автопарку або міської ITS доцільно спочатку оновлювати тестову групу, потім обмежену експлуатаційну групу, після чого масштабувати оновлення. Це дає змогу виявити проблеми до масового впливу. Імовірність системного інциденту при поетапному розгортанні можна зменшити, якщо кожний етап має критерії зупинки:

$$Deploy_{next} = 1 \quad \text{якщо} \quad E_{crit} = 0 \wedge Q_{metrics} \geq Q_{min}. \tag{5.16}$$

де E_{crit} — кількість критичних помилок, $Q_{metrics}$ — сукупний показник якості після етапу.

Безпечне оновлення також потребує журналювання. Потрібно фіксувати, хто ініціював оновлення, яка версія встановлена, коли виконано перевірку, який був результат, чи застосовувався відкат, які помилки виникли та як вони усунуті. Такі журнали важливі для аудиту, розслідування інцидентів і підтвердження нормативної відповідності.

Отже, безпечне оновлення програмного забезпечення є одним із центральних методів кіберзахисту ITS. Воно забезпечує актуальність захисту, але саме потребує суворого контролю. Надійний процес оновлення має поєднувати

криптографію, керування конфігураціями, тестування, аналіз впливу, поетапне розгортання, відкат і аудит.

5.5 Керування доступом і захист телематичних платформ

Телематичні платформи є одним із головних цифрових вузлів автомобільного транспорту. Вони забезпечують віддалену діагностику, моніторинг автопарку, навігацію, оновлення, страхові сервіси, мобільні застосунки, збір телематичних даних, інтеграцію з центрами керування та взаємодію з користувачами. Компрометація телематичної платформи може призвести до витоку даних, несанкціонованих команд, порушення оновлень, відстеження транспортних засобів або поширення атаки на інші компоненти ITS [52, 1, 9, 11].

Управління доступом має відповідати принципам мінімальних привілеїв, розподілу ролей, багатофакторної автентифікації, контролю сесій, журналювання й регулярного перегляду прав. У телематичних системах можуть існувати різні ролі: водій, власник, оператор автопарку, сервісна станція, виробник, адміністратор платформи, розробник API, орган управління або страховий партнер. Кожна роль повинна мати лише ті права, які потрібні для виконання функції.

Табл. 5.7: Приклад рольової моделі доступу до телематичної платформи

Роль	**Дозволені дії**	**Обмеження**
Водій	Перегляд власних поїздок, налаштування застосунку	Немає доступу до чужих авто
Оператор автопарку	Моніторинг транспорту, звіти, маршрути	Без зміни критичного ПЗ
Сервісна станція	Діагностика й сервісні операції	Тимчасовий доступ із журналюванням
Виробник	Оновлення, відкликання, технічна підтримка	Контроль процедур і підписів
Адміністратор	Керування платформою	MFA, поділ обов'язків, аудит

Модель контролю доступу можна подати як функцію:

$$Access(u, a, r, t) = Policy(Role(u), Perm(a), Risk(r), Context(t)), \quad (5.17)$$

де u — користувач або сервіс, a — запитувана дія, r — поточний рівень

ризику, t — контекст, наприклад місце, час, пристрій або стан автомобіля. Така модель показує, що доступ не повинен залежати лише від ролі; він має враховувати контекст і ризик.

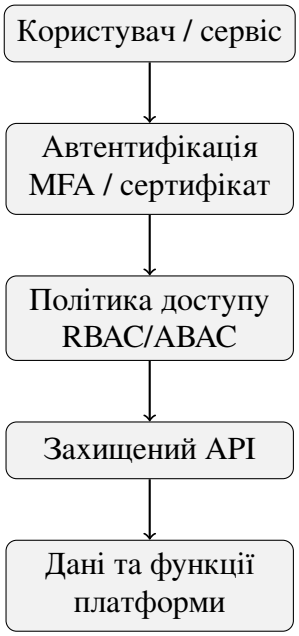

Рис. 5.7: Контур управління доступом до телематичної платформи

Для захисту API телематичної платформи необхідні автентифікація сервісів, обмеження швидкості запитів, перевірка токенів, контроль походження, валідація параметрів, журналювання, сегментація середовищ і регулярне тестування. API часто є слабким місцем, оскільки через нього взаємодіють мобільні застосунки, веб-портали, автомобілі, партнери й внутрішні сервіси. Помилка авторизації може дозволити доступ до чужого транспортного засобу або даних.

Ризик доступу можна оцінити як:

$$R_{access} = P_{comp} \cdot Priv \cdot Impact \cdot Exposure, \tag{5.18}$$

де P_{comp} — імовірність компрометації облікового запису або токена, $Priv$ — рівень привілеїв, $Impact$ — наслідки дії, $Exposure$ — ступінь відкритості інтерфейсу. Зменшення будь-якого множника знижує ризик: MFA зменшує P_{comp}, мінімальні привілеї — $Priv$, сегментація — $Impact$, обмеження API — $Exposure$.

Телематичні платформи повинні захищати не лише команди, а й дані. Геолокація, історія маршрутів, стиль водіння, технічний стан, ідентифіка-

тори пристроїв і платіжні дані можуть бути персональними або комерційно чутливими. Тому платформа повинна реалізовувати мінімізацію даних, псевдонімізацію, шифрування, контроль строків зберігання, управління згодою, розмежування доступу й механізми аудиту [52, 53, 54].

Табл. 5.8: Контрольні заходи для захисту телематичних платформ

Напрям	**Заходи**	**Ефект**
Ідентичність	MFA, сертифікати, ротація токенів	Менше захоплень акаунтів
Авторизація	RBAC/ABAC, мінімальні привілеї	Обмеження шкоди
API	Обмеження частоти запитів, валідація, журналювання	Захист від зловживань
Дані	Шифрування, псевдонімізація, строки зберігання	Захист приватності
Операції	SIEM/SOC, резервні копії, реагування	Виявлення та відновлення

Захист телематичних платформ має включати безперервний моніторинг. Ознаками інциденту можуть бути незвичні географічні входи, масові запити до API, спроби доступу до багатьох автомобілів, аномальна кількість помилок авторизації, нетипове завантаження даних або спроби виконати сервісні команди поза регламентом. Для таких подій потрібні автоматизовані правила кореляції та сценарії реагування.

Індекс підозрілості сесії можна подати як:

$$S_{sess} = \alpha G + \beta V + \gamma F + \delta P + \epsilon H, \tag{5.19}$$

де G — географічна нетиповість, V — обсяг запитів, F — частота помилок, P — рівень привілеїв, H — історичне відхилення від профілю. Якщо S_{sess} перевищує поріг, платформа може вимагати повторну автентифікацію, обмежити дію або повідомити SOC.

Отже, управління доступом і захист телематичних платформ є критичним компонентом кібербезпеки ITS. Цей напрям поєднує ідентичність, авторизацію, API-безпеку, захист даних, моніторинг, реагування та правову відповідність. Без нього навіть добре захищений автомобіль може залишатися вразливим через зовнішні цифрові сервіси.

5.6 Інтегрована архітектура захисту інтелектуальних транспортних систем

Окремі методи кібербезпеки мають найбільшу ефективність тоді, коли вони об'єднані в інтегровану архітектуру захисту. Така архітектура повинна охоплювати рівень транспортного засобу, комунікацій, інфраструктури, центру керування, телематичної платформи та даних. Вона має визначати, які активи захищаються, які загрози враховуються, які механізми застосовуються, як події журналюються, хто реагує на інцидент і як оцінюється залишковий ризик [1, 11, 16, 12].

Принцип багаторівневого захисту означає, що відмова одного механізму не повинна призводити до повної компрометації. Якщо атакувальник обходить автентифікацію користувача, його права мають бути обмежені. Якщо він надсилає підписане, але неправдиве V2X-повідомлення, перевірка правдоподібності має зменшити ризик. Якщо компрометовано телематичний сервіс, сегментація має перешкоджати переходу до критичних автомобільних доменів.

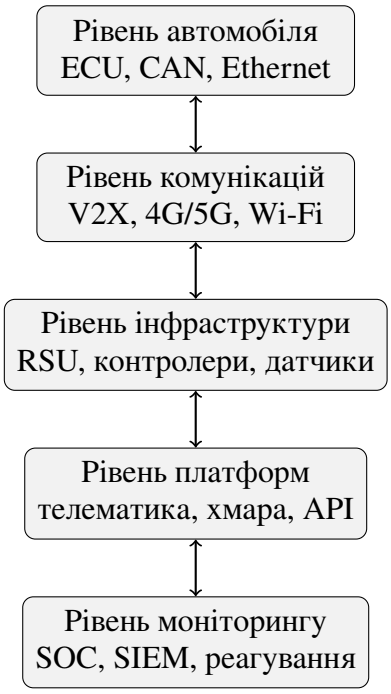

Рис. 5.8: Багаторівнева архітектура кіберзахисту ITS

Інтегральну ефективність захисту можна подати як:

$$E_{total} = 1 - \prod_{i=1}^{n}(1 - E_i), \tag{5.20}$$

де E_i — ефективність i-го незалежного захисного рівня. Якщо рівні не є

незалежними, реальна ефективність буде нижчою, тому потрібно уникати спільних точок відмови: одного ключа, одного адміністратора, одного сервера або одного незахищеного каналу.

Табл. 5.9: Відповідність захисних методів рівням ITS

Рівень	**Методи**	**Ключова мета**
Автомобіль	SecOC, IDS, шлюзи, безпечне завантаження, діагностичний контроль	Захист критичних функцій
V2X	PKI, підписи, псевдоніми, довірчі моделі	Достовірний обмін
Інфраструктура	Сегментація, фізичний захист, резервування	Стійкість керування рухом
Платформи	IAM, безпека API, шифрування, SIEM	Захист сервісів і даних
Операції	SOC, реагування, аудит, навчання	Безперервне управління ризиком

Архітектура захисту повинна підтримувати принцип безпечної деградації. Якщо не працює V2X, автомобіль не повинен втрачати базову безпеку. Якщо недоступна хмарна платформа, локальні функції мають зберігатися. Якщо IDS виявляє аномалію, реакція повинна знижувати ризик, а не створювати нову небезпеку. Це вимагає узгодження кібербезпеки з функціональною безпекою та експлуатаційною надійністю [2, 4, 1].

Для управління залишковим ризиком можна використовувати критерій:

$$R_{res} = R_{init} - \sum_{i=1}^{n} \Delta R_i + R_{complexity}, \tag{5.21}$$

де R_{init} — початковий ризик, ΔR_i — зменшення ризику від заходу, $R_{complexity}$ — додатковий ризик через складність, помилки конфігурації або експлуатаційні обмеження. Ця формула нагадує, що надмірно складний захист може створювати власні ризики.

Інтегрована архітектура також потребує процедур реагування. Повинні бути визначені події, які вважаються інцидентами, порядок ескалації, відповідальні особи, допустимий час реагування, способи ізоляції, критерії відновлення та вимоги до звітності. Для транспортних систем важливо, щоб реагування враховувало не лише IT-сервіси, а й дорожню ситуацію, безпеку користувачів

і роботу екстрених служб.

5.7 Оцінювання ефективності та аудит кібербезпеки

Методи кібербезпеки повинні регулярно оцінюватися. Наявність політик, криптографії або IDS не гарантує фактичного захисту, якщо вони неправильно налаштовані, не оновлюються або не використовуються під час реагування. Оцінювання ефективності включає технічні тести, аудит конфігурацій, аналіз журналів, перевірку прав доступу, тестування резервного відновлення, навчання персоналу й аналіз інцидентів.

Для ITS важливо оцінювати не лише кількість заблокованих атак, а й вплив захисних заходів на безпеку руху та надійність. Наприклад, криптографія не повинна створювати неприпустимих затримок; IDS не повинна генерувати надмірну кількість хибних попереджень; оновлення не повинні порушувати функціональну безпеку; політики доступу не повинні блокувати аварійні процедури.

Табл. 5.10: Метрики оцінювання кіберзахисту ITS

Метрика	**Зміст**	**Призначення**
MTTD	Середній час виявлення інциденту	Оцінка моніторингу
MTTR	Середній час реагування/відновлення	Оцінка операційної готовності
Частка хибнопозитивних спрацювань	Частка хибних попереджень	Якість IDS/SOC
Затримка встановлення виправлень	Час від випуску до встановлення оновлення	Ризик відомих вразливостей
Частка перегляду прав доступу	Частка переглянутих прав доступу	Контроль привілеїв

Середній час виявлення та реагування можна подати як:

$$MTTD = \frac{1}{n}\sum_{i=1}^{n}(t_{detect,i} - t_{start,i}), \tag{5.22}$$

$$MTTR = \frac{1}{n}\sum_{i=1}^{n}(t_{restore,i} - t_{detect,i}). \tag{5.23}$$

Зменшення цих показників є одним із головних завдань операційної кібербезпеки.

Аудит кіберзахисту має охоплювати документи, архітектуру, технічні налаштування й фактичні журнали. Документи показують, що повинно бути; архітектура показує, як система задумана; конфігурації показують, як вона налаштована; журнали показують, як вона реально працює. Розбіжності між цими рівнями часто є джерелом ризику.

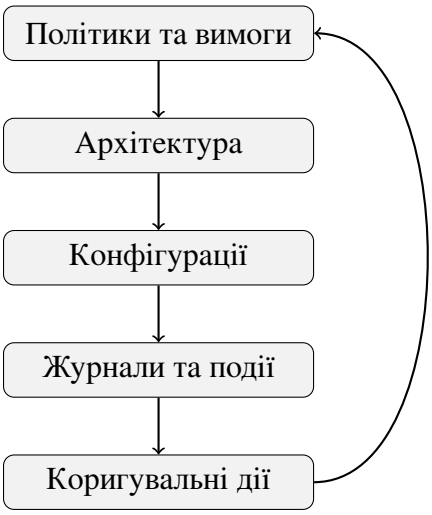

Рис. 5.9: Цикл аудиту й удосконалення кіберзахисту ITS

Загальний рівень зрілості кіберзахисту ITS можна описати індексом:

$$M_{sec} = w_1 C_{asset} + w_2 C_{access} + w_3 C_{crypto} + w_4 C_{monitor} + w_5 C_{response} + w_6 C_{update}, \tag{5.24}$$

де C_{asset} — інвентаризація активів, C_{access} — управління доступом, C_{crypto} — криптографічний захист, $C_{monitor}$ — моніторинг, $C_{response}$ — реагування, C_{update} — керування оновленнями. Значення ваг w_i визначаються критичністю конкретної ITS.

Для великих транспортних систем доцільно проводити навчання та кіберучення. Вони мають перевіряти не лише технічну реакцію, а й координацію між операторами, службами безпеки, дорожніми службами, виробниками, постачальниками зв'язку та органами влади. Сценарії можуть включати компрометацію V2X-вузла, програма-вимагач центру керування, масову помилку оновлення, витік телематичних даних або атаку на світлофорний коридор.

Отже, оцінювання ефективності й аудит є необхідними для підтримки кібербезпеки ITS у часі. Захист, який не перевіряється, поступово деградує

через зміни конфігурацій, нові вразливості, людські помилки та застарівання технологій. Безперервний аудит перетворює кібербезпеку з одноразового проєкту на керований процес.

5.8 Практичні сценарії впровадження захисту та карта контролів

Практичне впровадження кібербезпеки в ITS доцільно починати не з вибору окремого програмного продукту, а з побудови карти контролів. Карта контролів показує, які активи існують у системі, які загрози для них актуальні, які захисні механізми вже застосовуються, хто відповідає за їх підтримку та які прогалини залишаються. Для автомобільного транспорту така карта має охоплювати транспортний засіб, внутрішні мережі, телематичний модуль, V2X-інтерфейси, дорожню інфраструктуру, центр керування, хмарні платформи, мобільні застосунки й персональні дані [1, 11, 12, 37].

Першим сценарієм є захист підключеного транспортного засобу. У цьому випадку базовими контролями є безпечне завантаження, контроль цілісності програмного забезпечення, сегментація доменів, захист діагностичного доступу, IDS на шлюзі, журналювання безпекових подій і безпечне оновлення. Особливу увагу потрібно приділяти переходам між доменами: мультимедійний або користувацький домен не повинен мати прямого доступу до критичних функцій шасі. Якщо такий доступ потрібний для сервісу, він має проходити через контрольований шлюз із фільтрацією, автентифікацією та обмеженням команд.

Другим сценарієм є захист V2X-коридору. Тут важливими є PKI, перевірка сертифікатів, цифровий підпис повідомлень, псевдонімізація, контроль часу, географічна релевантність, захист RSU, моніторинг радіоканалу та механізми відкликання. Крім того, оператор дороги повинен мати процедуру реагування на підозрілі V2X-події: перевірку через інфраструктурні датчики, тимчасове зниження довіри до вузла, повідомлення центру керування та, за потреби, відкликання сертифіката [16, 17, 20, 21].

Третім сценарієм є захист телематичної платформи автопарку. Для нього критичними є управління ідентичностями, багатофакторна автентифікація операторів, розмежування ролей, захист API, шифрування даних, журналювання запитів, контроль масового експорту, моніторинг аномальних сесій, резервне копіювання та план реагування на витік даних. У цьому сценарії

кібербезпека тісно пов'язана із захистом персональних даних, оскільки телематична платформа може містити маршрути, стиль водіння, графіки роботи й технічний стан транспортних засобів [52, 53, 54].

Табл. 5.11: Карта контролів кібербезпеки для типових сценаріїв ITS

Сценарій	**Ключові контролі**	**Показники перевірки**
Підключений автомобіль	Безпечне завантаження, IDS, сегментація, контроль діагностики	Кількість заблокованих команд, час виявлення, стан журналів
V2X-коридор	PKI, підпис, псевдоніми, перевірка правдоподібності	Частка валідних повідомлень, затримка перевірки, відкликання
Телематична платформа	IAM, MFA, безпека API, шифрування, SIEM	Аномальні сесії, перегляд прав, час реагування
Центр керування	Сегментація, резервування, SOC, аудит конфігурацій	MTTD, MTTR, доступність сервісів, відновлення
Дані користувачів	Мінімізація, псевдонімізація, строки зберігання	Обсяг даних, запити доступу, аудит передачі третім сторонам

Для вибору оптимального набору контролів можна використовувати співвідношення між зниженням ризику та вартістю впровадження:

$$K_{eff,i} = \frac{\Delta R_i}{C_i + O_i}, \tag{5.25}$$

де ΔR_i — очікуване зниження ризику від i-го контролю, C_i — вартість впровадження, O_i — витрати на експлуатацію. Контролі з високим K_{eff} доцільно впроваджувати першочергово, якщо вони не створюють неприйнятної затримки або конфлікту з функціональною безпекою.

Карта контролів повинна містити також оцінку залишкових прогалин. Наприклад, якщо V2X-повідомлення підписуються, але відсутня перевірка фізичної правдоподібності, зберігається ризик прийняття повідомлень від скомпрометованого вузла. Якщо телематична платформа використовує MFA, але не обмежує права сервісних облікових записів, залишається ризик надмірного доступу. Якщо оновлення підписуються, але немає механізму відкату, залишається ризик втрати функції після помилки встановлення.

Для формалізації прогалин можна використати показник покриття кон-

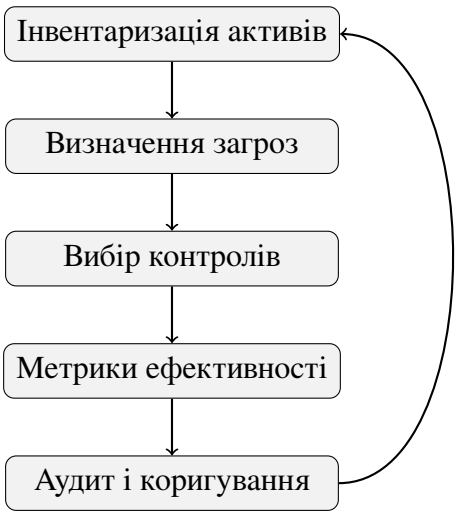

Рис. 5.10: Процес побудови та підтримки карти контролів кібербезпеки ITS

тролями:

$$C_{cov} = \frac{\sum_{j=1}^{m} a_j w_j}{\sum_{j=1}^{m} w_j}, \tag{5.26}$$

де $a_j = 1$, якщо вимога j покрита контролем, і $a_j = 0$, якщо не покрита, а w_j — критичність вимоги. Якщо C_{cov} низький для критичного домену, впровадження ITS не повинно переходити до промислової експлуатації без додаткових заходів.

Табл. 5.12: Приклад оцінювання покриття захисними контролями

Вимога	**Критичність**	**Покриття**	**Прогалина**
Підпис V2X-повідомлень	Висока	Так	Немає
Відкликання сертифікатів	Висока	Частково	Повільна синхронізація
Відкат оновлень	Висока	Частково	Не для всіх ECU
MFA операторів	Висока	Так	Немає
Псевдонімізація телематики	Середня/висока	Частково	Ризик повторної ідентифікації

Четвертим сценарієм є захист центру керування. Він потребує сегментації мережі, резервних робочих місць, багатофакторної автентифікації, моніторингу операторських дій, резервного копіювання, журналювання команд, сценаріїв ручного керування й регулярних навчань. На відміну від звичайної IT-системи, центр керування має реагувати в реальному часі на дорожні події,

тому захисні процедури не повинні паралізувати оперативну роботу. Баланс між контролем і швидкістю реагування є критичним.

П'ятим сценарієм є захист даних і аналітики. Дані ITS повинні перевірятися на якість, походження, цілісність і відповідність меті оброблення. Якщо аналітична модель отримує недостовірні або атаковані дані, вона може сформувати неправильний прогноз. Тому кібербезпека даних має включати контроль джерел, перевірку аномалій, журналювання перетворень, контроль доступу до навчальних наборів і періодичну перевірку моделей.

Індекс пріоритету впровадження контролю можна подати як:

$$P_{ctrl} = \alpha R + \beta G + \gamma L - \delta C - \epsilon T, \tag{5.27}$$

де R — рівень ризику, G — розмір прогалини, L — нормативна або договірна важливість, C — вартість, T — додаткова затримка або складність. Контролі з найбільшим P_{ctrl} формують першочерговий план кіберзахисту.

Таким чином, практичне впровадження методів кібербезпеки в ITS має спиратися на карту контролів, сценарії застосування й вимірювані показники. Це дозволяє перейти від загального твердження про необхідність захисту до конкретного плану: які активи захищаються, які ризики зменшуються, які контролі впроваджені, які прогалини залишаються та як вони будуть усунуті.

5.9 Узагальнення методів забезпечення кібербезпеки

Методи забезпечення кібербезпеки в ITS утворюють взаємопов'язану систему. Автентифікація й шифрування створюють базову довіру до даних і вузлів. IDS забезпечує виявлення аномалій і атак, які не були заблоковані. Захист CAN, Ethernet і бездротових каналів обмежує технічні вектори компрометації. Безпечне оновлення підтримує актуальність програмного забезпечення та усуває вразливості. Управління доступом і захист телематичних платформ контролюють зовнішні цифрові сервіси. Аудит і моніторинг забезпечують сталість захисту.

Інтегральну модель кіберзахисту можна подати як багатокритеріальну оптимізацію:

$$\min Z = \alpha R_{cyber} + \beta R_{safety} + \gamma C_{cost} + \delta T_{latency} - \mu A_{availability}, \tag{5.28}$$

Табл. 5.13: Узагальнення методів кібербезпеки ITS

Метод	**Що захищає**	**Ключові обмеження**
Криптографія	Повідомлення, оновлення, канали, журнали	Потребує керування ключами
IDS	Автомобільні мережі, платформи, події	Ризик хибних спрацювань
Сегментація	Домени автомобіля та інфраструктури	Потребує точної архітектури
Безпечні оновлення	ПЗ, сертифікати, конфігурації	Ризик несумісності
IAM/безпека API	Телематика, сервіси, користувачі	Потребує постійного аудиту
SOC/аудит	Операційний захист	Потребує кваліфікованого персоналу

де R_{cyber} — кіберризик, R_{safety} — ризик для безпеки руху, C_{cost} — витрати, $T_{latency}$ — додаткова затримка від захисту, $A_{availability}$ — доступність сервісів. Ця модель показує, що захист має бути збалансованим: надмірне ускладнення може зменшити доступність або збільшити затримку.

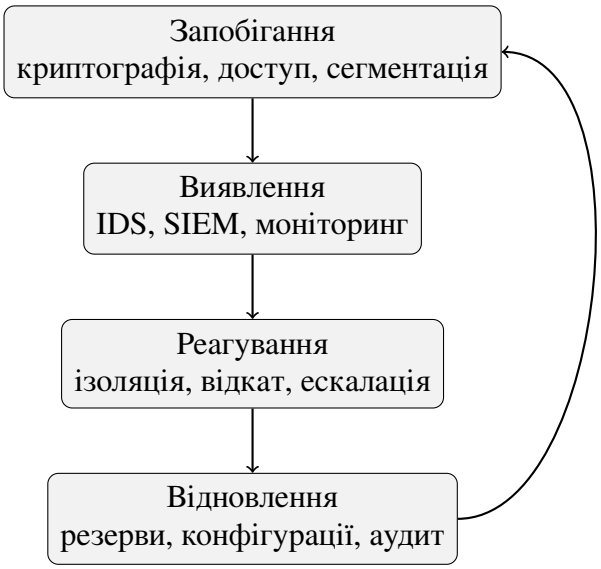

Рис. 5.11: Цикл забезпечення кібербезпеки ITS

Кінцевою метою є не абсолютне усунення всіх кіберризиків, а досягнення прийнятного залишкового ризику за збереження безпеки руху, надійності й експлуатаційної придатності. Для цього методи захисту повинні бути технічно сумісними, нормативно обґрунтованими, організаційно підтриманими та регулярно перевірятися. ITS є динамічною системою, тому кібербезпека має

бути безперервним процесом, а не одноразовою конфігурацією.

Отже, розділ показує, що забезпечення кібербезпеки в інтелектуальних транспортних системах потребує поєднання криптографії, IDS, мережевого захисту, безпечних оновлень, управління доступом, захисту телематики, моніторингу й аудиту. Саме інтегроване застосування цих методів створює основу для стійкого, безпечного та надійного автомобільного транспорту в цифровому середовищі.

6 Підвищення надійності автомобільного транспорту в інтелектуальних транспортних системах

Підвищення надійності автомобільного транспорту в інтелектуальних транспортних системах є практичним продовженням аналізу кібербезпеки, функціональної безпеки та експлуатаційної стійкості. Якщо попередні розділи визначали структуру ITS, кіберзагрози, природу цифрових відмов і методи захисту, то цей розділ зосереджується на інженерних і організаційних засобах підвищення надійності. У сучасному автомобільному транспорті надійність формується не лише якістю механічних вузлів, а й стабільністю програмного забезпечення, якістю даних, доступністю каналів зв'язку, справністю датчиків, стійкістю центрів керування та здатністю системи швидко відновлюватися після відмов або атак [2, 4, 3, 6].

Надійність ITS має розглядатися як властивість розподіленої кіберфізичної системи. Така система включає транспортні засоби, дорожню інфраструктуру, V2X-вузли, телематичні платформи, центри керування, цифрові сервіси, операторів і користувачів. Відмова одного компонента може залишитися локальною, але може й поширитися на інші рівні: деградація датчика призводить до хибного повідомлення, хибне повідомлення впливає на алгоритм керування, алгоритм формує неправильне рішення, а транспортна мережа отримує затримки або ризики безпеки. Тому підвищення надійності потребує резервування, діагностики, прогнозування, моніторингу, штучного інтелекту, відмовостійких архітектур і керованих процедур реагування [58, 59, 60, 56].

У цьому розділі розглянуто п'ять ключових напрямів: резервування критичних компонентів; діагностика та прогнозування технічного стану; моніторинг транспортних засобів у реальному часі; використання штучного інтелекту для виявлення аномалій; забезпечення відмовостійкості систем керування. Кожний напрям має власні методи, показники, обмеження й вимоги до інтеграції з кібербезпекою та функціональною безпекою.

6.1 Резервування критичних компонентів

Резервування є одним із базових методів підвищення надійності транспортних систем. Його сутність полягає у введенні додаткових компонентів, каналів, функцій або процедур, які можуть підтримати працездатність системи у разі відмови основного елемента. Для автомобільного транспорту в ITS резервування застосовується на різних рівнях: датчики транспортного засобу, електронні блоки керування, джерела живлення, канали зв'язку, сервери центру керування, дорожні контролери, бази даних, хмарні сервіси та операторські процедури. Мета резервування полягає не лише у продовженні роботи, а й у збереженні безпечного й контрольованого стану [2, 4, 78].

Резервування може бути апаратним, програмним, інформаційним, функціональним і організаційним. Апаратне резервування передбачає дублювання фізичних компонентів: датчиків, блоків, серверів, каналів живлення. Програмне резервування передбачає альтернативні алгоритми, незалежні реалізації, контрольні обчислення або можливість відкату версії. Інформаційне резервування використовує кілька джерел даних для підтвердження стану. Функціональне резервування означає, що одна функція тимчасово виконується іншим компонентом або на нижчому рівні. Організаційне резервування включає змінних операторів, резервні процедури й альтернативні маршрути реагування.

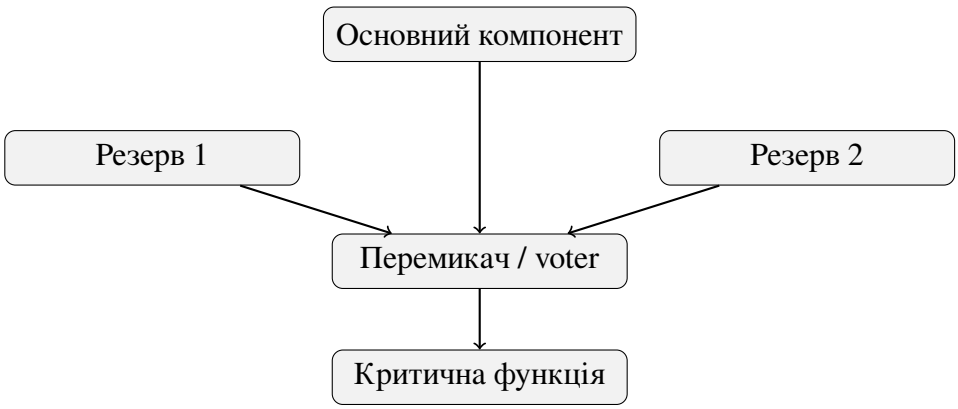

Рис. 6.1: Загальна схема резервування критичної функції

Для паралельного резервування, коли достатньо працездатності хоча б одного з n незалежних компонентів, імовірність виконання функції дорівнює:

$$P_{par} = 1 - \prod_{i=1}^{n}(1 - P_i), \tag{6.1}$$

де P_i — імовірність працездатності i-го компонента. Якщо компоненти однакові й мають імовірність працездатності P, формула спрощується:

$$P_{par} = 1 - (1 - P)^n. \tag{6.2}$$

Це показує, що навіть два або три резервні канали можуть істотно підвищити надійність, якщо їх відмови незалежні.

Для послідовної структури, де відмова будь-якого елемента призводить до втрати функції, імовірність працездатності становить:

$$P_{ser} = \prod_{i=1}^{n} P_i. \tag{6.3}$$

Тому в ITS потрібно уникати зайвих послідовних залежностей у критичних функціях. Наприклад, якщо попередження водія залежить одночасно від датчика, телематичної платформи, хмарного сервера й мобільного застосунку, відмова будь-якої ланки знижує готовність. Для критичних функцій доцільно залишати локальну автономність автомобіля та інфраструктури.

Табл. 6.1: Види резервування в автомобільному транспорті та ITS

Вид резервування	**Приклад**	**Очікуваний ефект**
Апаратне	Дублювання датчиків, серверів, каналів живлення	Зменшення ризику одиничної відмови
Програмне	Альтернативний алгоритм, відкат, незалежна реалізація	Зниження наслідків дефектів ПЗ
Інформаційне	Порівняння GNSS, IMU, даних коліс і V2X	Підвищення достовірності стану
Комунікаційне	V2X + 4G/5G + локальний канал	Доступність повідомлень при втраті мережі
Організаційне	Резервні оператори, аварійні регламенти	Скорочення часу відновлення

У транспортних засобах важливим є різнорідне резервування датчиків. Камера, радар, лідар, ультразвуковий датчик, GNSS і інерційний модуль мають різні фізичні принципи роботи та різні типи відмов. Камера може втратити якість у тумані або темряві, радар краще працює в погану погоду, але має інші обмеження, GNSS може бути недоступним у міській забудові або піддаватися

спуфінгу. Різнорідне резервування зменшує ризик спільної відмови, хоча не усуває його повністю [45, 46, 72, 79].

Для системи з голосуванням “два з трьох” і однаковою імовірністю працездатності P імовірність правильного рішення можна подати як:

$$P_{2oo3} = 3P^2(1 - P) + P^3. \tag{6.4}$$

Ця схема корисна для критичних функцій, оскільки дає змогу відкинути один помилковий канал. Проте вона вимагає перевірки незалежності каналів і захисту від спільних причин, наприклад однакової помилки програмної обробки або однакового джерела живлення.

Резервування каналів зв’язку особливо важливе для ITS. Якщо V2X-канал недоступний через завади, повідомлення може бути передане через стільникову мережу або локальний інфраструктурний вузол. Якщо хмарний сервіс недоступний, локальний контролер повинен продовжувати роботу за резервним планом. Якщо центр керування втрачає зв’язок із групою перехресть, кожне перехрестя повинно мати автономний безпечний режим. Таке резервування знижує залежність від єдиної точки відмови [8, 26, 27].

Ефективність резервування залежить від часу перемикання. Якщо резервний компонент існує, але активується надто повільно, критична функція може бути втрачена. Умова придатності резерву може бути подана як:

$$T_{detect} + T_{switch} + T_{stabilize} \leq T_{max}, \tag{6.5}$$

де T_{detect} — час виявлення відмови, T_{switch} — час перемикання, $T_{stabilize}$ — час стабілізації роботи резерву, T_{max} — допустимий час переривання функції.

Резервування має й обмеження. Воно збільшує складність, вартість, енергоспоживання, кількість інтерфейсів і площу атаки. Якщо резервні компоненти неправильно синхронізовані або мають різні версії програмного забезпечення, вони можуть самі стати джерелом відмов. Тому резервування повинно супроводжуватися керуванням конфігураціями, тестуванням, моніторингом і процедурами перевірки працездатності резерву.

Періодичне тестування резерву можна описати через імовірність прихованої відмови. Якщо резерв перевіряється з інтервалом T_{test}, а інтенсивність його відмови λ_b, то наближена імовірність прихованої відмови між тестами

Табл. 6.2: Критерії вибору резервування для ITS

Критерій	**Пояснення**	**Приклад**
Критичність функції	Вплив відмови на безпеку руху	Гальмування, світлофорний план, V2X-попередження
Час реакції	Допустима затримка перемикання	Мілісекунди для автомобіля, секунди для сервісу
Незалежність резерву	Відсутність спільних причин відмови	Інший датчик, інше живлення, інший канал
Вартість	Витрати на обладнання та супровід	Резервний сервер або дублювання RSU
Кіберризик	Можливість компрометації резерву	Окремі ключі, сегментація, аудит

дорівнює:

$$P_{hidden} \approx \lambda_b \frac{T_{test}}{2}. \tag{6.6}$$

Зменшення інтервалу тестування знижує ризик прихованої недоступності резерву, але збільшує експлуатаційні витрати.

Отже, резервування критичних компонентів є необхідним, але не самодостатнім методом підвищення надійності. Його ефективність визначається незалежністю резервів, швидкістю перемикання, регулярним тестуванням, кіберзахистом, керуванням конфігураціями та здатністю системи переходити в безпечний деградаційний режим.

6.2 Діагностика та прогнозування технічного стану

Діагностика та прогнозування технічного стану забезпечують перехід від реактивного ремонту до проактивного управління надійністю. У реактивній моделі несправність усувається після відмови. У планово-попереджувальній моделі обслуговування виконується через фіксовані інтервали. У прогнозній моделі рішення приймається на основі фактичного стану компонента, тенденцій деградації, режимів експлуатації та статистики відмов. Для цифровізованого автомобільного транспорту саме прогнозна модель є найбільш перспективною [58, 59, 60].

Діагностика в ITS спирається на дані від транспортних засобів, датчиків, електронних блоків, телематичних платформ, дорожньої інфраструктури та

центрів керування. До діагностичних параметрів належать коди несправностей, температура, напруга, струм, вібрація, рівень шуму сенсорів, кількість перезапусків, помилки пам'яті, затримки зв'язку, втрати пакетів, стан сертифікатів, версії програмного забезпечення й журнали подій. Поєднання цих даних дає змогу оцінювати не лише факт відмови, а й наближення до відмови.

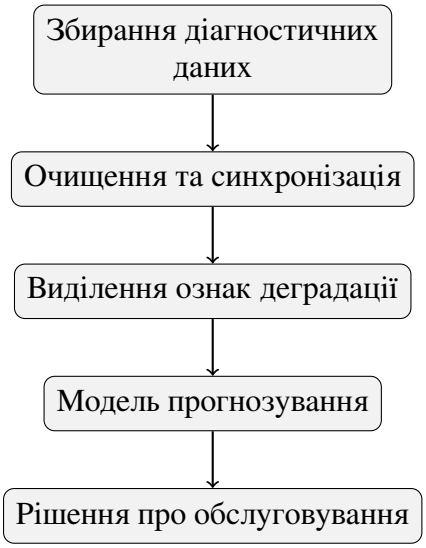

Рис. 6.2: Процес діагностики та прогнозування технічного стану

Для опису деградації компонента можна використати функцію стану $h(t)$, де $h = 1$ відповідає повністю справному стану, а $h = 0$ — граничній відмові. Просте лінійне наближення має вигляд:

$$h(t) = 1 - \frac{d(t)}{d_{crit}}, \tag{6.7}$$

де $d(t)$ — накопичена деградація, d_{crit} — критичний рівень. Якщо деградація зростає зі швидкістю v_d, залишковий ресурс можна оцінити як:

$$RUL = \frac{d_{crit} - d(t)}{v_d}. \tag{6.8}$$

На практиці деградація часто нелінійна, тому використовують статистичні, регресійні, байєсівські та нейромережеві моделі.

Індекс технічного стану компонента можна подати як зважену суму нормованих ознак:

$$H_c = 1 - \sum_{i=1}^{m} w_i \frac{x_i - x_i^{nom}}{x_i^{crit} - x_i^{nom}}, \tag{6.9}$$

Табл. 6.3: Джерела даних для прогнозування технічного стану

Джерело	**Приклади параметрів**	**Призначення**
ECU	Коди помилок, температура, перезапуски	Діагностика електроніки
Датчики	Шум, дрейф, пропуски, калібрування	Виявлення деградації сприйняття
Комунікації	Затримка, втрати пакетів, рівень сигналу	Оцінка доступності сервісів
Телематика	Пробіг, режим руху, навантаження	Прогноз ресурсу агрегатів
Інфраструктура	Стан контролерів, живлення, мережа	Надійність дорожніх компонентів

де x_i — поточне значення ознаки, x_i^{nom} — номінальне значення, x_i^{crit} — критичне значення, w_i — вага ознаки. Якщо H_c зменшується нижче порогу, компонент потребує обслуговування або заміни.

Прогнозування технічного стану може застосовуватися не лише до автомобіля, а й до інфраструктури ITS. Світлофорні контролери, RSU, камери, дорожні датчики, сервери й мережеве обладнання мають власні ознаки деградації. Наприклад, часті втрати зв'язку з RSU можуть свідчити про проблеми живлення, антени або мережевої конфігурації. Зростання кількості помилок відеоаналітики може вказувати на забруднення камери або зміну умов освітлення.

Для класифікації стану можна використовувати множину станів:

$$S = \{S_0, S_1, S_2, S_3\}, \tag{6.10}$$

де S_0 — справний стан, S_1 — рання деградація, S_2 — передвідмовний стан, S_3 — відмова. Перехід між станами можна описати марковською моделлю з матрицею переходів:

$$\Pi = \begin{bmatrix} p_{00} & p_{01} & 0 & 0 \\ 0 & p_{11} & p_{12} & 0 \\ 0 & 0 & p_{22} & p_{23} \\ p_{30} & 0 & 0 & p_{33} \end{bmatrix}. \tag{6.11}$$

Елемент p_{30} може описувати відновлення після ремонту.

Важливою умовою прогнозування є якість даних. Якщо діагностичні

Табл. 6.4: Методи прогнозування технічного стану

Метод	**Переваги**	**Обмеження**
Пороговий контроль	Простота, зрозумілість, швидкість	Погано враховує складні тренди
Статистичні моделі	Оцінка ймовірностей і довірчих інтервалів	Потребують припущень про розподіли
Марковські моделі	Опис станів деградації	Потребують даних переходів
Машинне навчання	Виявлення нелінійних залежностей	Потребує якісних даних і валідації
Фізичні моделі	Пояснюваність і зв'язок з механізмом відмови	Складність побудови для комплексних систем

дані неповні, несинхронізовані, шумні або містять кібераномалії, модель може сформувати неправильний прогноз. Тому перед прогнозуванням потрібні фільтрація, нормалізація, перевірка часових міток, виявлення пропусків і перевірка достовірності джерел. Кібербезпека даних стає частиною прогнозної надійності.

Ефект прогнозного обслуговування можна оцінити через зменшення непланових простоїв:

$$E_{pm} = \frac{T_{down}^{base} - T_{down}^{pred}}{T_{down}^{base}} \cdot 100\%, \tag{6.12}$$

де T_{down}^{base} — простій при базовій стратегії, T_{down}^{pred} — простій при прогнозному обслуговуванні. Для автопарків і критичних транспортних сервісів цей показник може бути одним із головних аргументів на користь цифрової діагностики.

Отже, діагностика та прогнозування технічного стану є центральним інструментом підвищення надійності в ITS. Вони дозволяють виявляти деградацію до відмови, планувати обслуговування, зменшувати простої, підвищувати безпеку й оптимізувати ресурси. Однак їх ефективність залежить від якості даних, правильності моделей, кіберзахисту джерел і готовності організації реагувати на прогнози.

6.3 Моніторинг транспортних засобів у реальному часі

Моніторинг транспортних засобів у реальному часі забезпечує оперативне спостереження за станом автомобілів, маршрутами, технічними параметрами, подіями, безпековими попередженнями та якістю сервісів. У контексті ITS моніторинг є не лише диспетчерською функцією, а й основою для прогнозування, реагування на інциденти, виявлення аномалій, управління автопарком, підтримки V2X-сервісів і забезпечення надійності транспортної мережі [32, 35, 36, 61].

Система моніторингу в реальному часі зазвичай включає бортові датчики, телематичний блок, канали зв'язку, платформу оброблення даних, базу подій, модуль аналітики, інтерфейс оператора та механізми реагування. Дані можуть надходити з різною частотою: координати й швидкість — часто, діагностичні параметри — за подіями або інтервалами, журнали безпеки — при спрацюванні правил, оновлення стану сервісів — періодично. Завдання системи полягає в тому, щоб не лише зібрати дані, а й швидко перетворити їх на корисну інформацію.

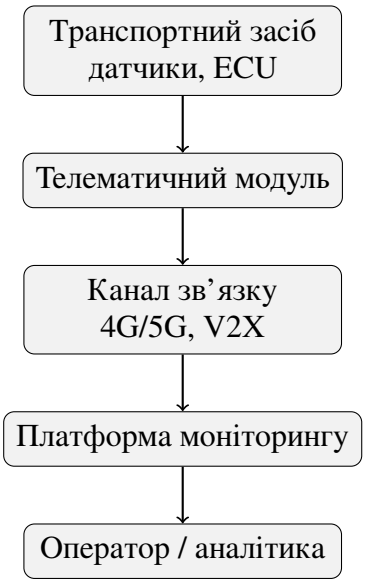

Рис. 6.3: Архітектура моніторингу транспортного засобу в реальному часі

Ключовим параметром є затримка моніторингу:

$$T_{mon} = T_{sense} + T_{edge} + T_{comm} + T_{cloud} + T_{vis}, \tag{6.13}$$

де T_{sense} — час вимірювання, T_{edge} — попередня обробка на борту або периферійному вузлі, T_{comm} — передавання, T_{cloud} — серверна обробка, T_{vis} —

відображення оператору або передавання в інший сервіс. Для критичних подій має виконуватися умова:

$$T_{mon} \leq T_{crit}. \tag{6.14}$$

Табл. 6.5: Параметри моніторингу транспортних засобів у реальному часі

Група параметрів	**Приклади**	**Призначення**
Рух	Координати, швидкість, прискорення, курс	Контроль маршруту й безпеки
Технічний стан	DTC, температура, напруга, помилки ECU	Діагностика та прогнозування
Комунікації	Рівень сигналу, затримка, втрати пакетів	Оцінка доступності сервісів
Кіберподії	Помилки автентифікації, IDS-події, зміни конфігурації	Виявлення атак і зловживань
Експлуатація	Пробіг, витрата енергії, режим роботи	Управління автопарком

Для оцінювання повноти моніторингу можна використати показник:

$$C_{mon} = \frac{N_{received}}{N_{expected}}, \tag{6.15}$$

де $N_{received}$ — кількість отриманих повідомлень або параметрів, $N_{expected}$ — очікувана кількість за період. Якщо C_{mon} знижується, це може свідчити про втрату зв'язку, відмову телематичного модуля, перевантаження платформи або кібератаку.

Реальний час не завжди означає миттєвість. Для різних сервісів допустимі різні затримки. Попередження про аварійну подію потребує секунд або менше, контроль маршруту автопарку може працювати з інтервалом у десятки секунд, технічна діагностика може передаватися рідше, а аналітика ресурсу може виконуватися пакетно. Тому система моніторингу повинна класифікувати дані за критичністю й пріоритетом.

Моніторинг у реальному часі має бути захищеним. Дані повинні передаватися через автентифіковані та зашифровані канали, а платформа повинна перевіряти походження повідомлень. Якщо атакувальник може підмінити телематичні дані, оператор отримає хибну картину. Якщо атакувальник може відстежувати дані, порушується приватність. Тому моніторинг потребує кри-

Табл. 6.6: Класи критичності даних моніторингу

Клас	**Приклади даних**	**Вимоги**
Критичні	Аварійна подія, відмова гальм, V2X-попередження	Мінімальна затримка, пріоритет, підтвердження
Високі	Втрата зв'язку, помилки ECU, небезпечний стиль руху	Швидке повідомлення оператору
Середні	Маршрут, регулярність, технічні тренди	Періодична передача й аналітика
Низькі	Статистичні звіти, історичні дані	Пакетна обробка

птографії, контролю доступу, журналювання й виявлення аномалій [52, 53, 1].

Для фільтрації потокових даних можна використовувати експоненційне згладжування:

$$\hat{x}_t = \alpha x_t + (1 - \alpha)\hat{x}_{t-1}, \tag{6.16}$$

де x_t — поточне вимірювання, $\hat{x}_t$ — згладжена оцінка, α — коефіцієнт згладжування. Такий підхід допомагає зменшити шум, але для критичних подій потрібно не приховати різкі зміни, а правильно їх класифікувати.

Моніторинг також підтримує управління автопарком. Оператор може бачити стан кожного транспортного засобу, оцінювати ризик відмови, планувати обслуговування, контролювати регулярність, зменшувати простої та реагувати на аварійні події. Для громадського транспорту це впливає на дотримання графіків, для вантажного — на логістику, для спеціального — на готовність до реагування.

Отже, моніторинг транспортних засобів у реальному часі є основою оперативного підвищення надійності. Він забезпечує дані для діагностики, прогнозування, кіберзахисту, диспетчеризації та відновлення. Його ефективність залежить від затримки, повноти, якості, захищеності та здатності операторів і алгоритмів використовувати отриману інформацію.

6.4 Використання штучного інтелекту для виявлення аномалій

Штучний інтелект і машинне навчання відіграють дедалі більшу роль у виявленні аномалій автомобільного транспорту в ITS. Аномалією може бути технічна деградація, кібератака, нетипова поведінка водія, несправність

датчика, підроблене повідомлення, нестабільний канал зв'язку, відхилення транспортного потоку або помилка програмної функції. Традиційні порогові правила корисні, але часто недостатні для складних нелінійних залежностей. Методи ШІ дають змогу аналізувати великі обсяги даних і знаходити приховані закономірності [44, 47, 48, 56].

Виявлення аномалій може бути контрольованим, неконтрольованим або напівконтрольованим. Контрольовані методи потребують розмічених прикладів нормальної та аномальної поведінки. Неконтрольовані методи будують модель нормальності й шукають відхилення без явних міток. Напівконтрольовані методи використовують обмежену кількість міток або лише нормальні дані. Для автомобільних систем часто актуальні неконтрольовані та напівконтрольовані підходи, оскільки реальні атаки й відмови трапляються рідше, ніж нормальні режими.

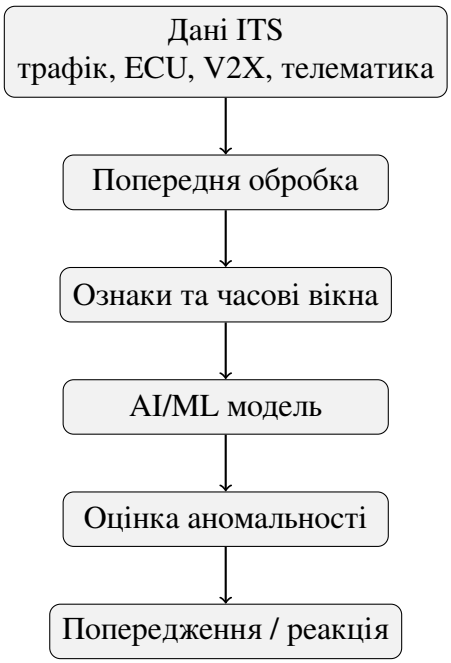

Рис. 6.4: Конвеєр ШІ-виявлення аномалій в ITS

Для формального опису аномальності можна використати функцію оцінки:

$$A(x) = \|x - \hat{x}\|, \tag{6.17}$$

де x — фактичний вектор ознак, $\hat{x}$ — очікуваний або реконструйований вектор. Якщо $A(x) > \theta$, об'єкт вважається аномальним. В автоенкодерах $\hat{x}$ є реконструкцією вхідних даних, а велика помилка реконструкції свідчить про нетиповість.

Для часових рядів корисною є прогнозна аномальність:

$$A_t = |x_t - \hat{x}_t|, \tag{6.18}$$

де $\hat{x}_t$ — прогноз моделі на момент t. Якщо фактичне значення істотно відрізняється від прогнозу, система фіксує аномалію. Такий підхід застосовний до швидкості, температури, затримки зв'язку, кількості CAN-повідомлень, інтенсивності потоку або навантаження сервера.

Табл. 6.7: Методи ШІ для виявлення аномалій в ITS

Метод	**Застосування**	**Обмеження**
Автокодувальник	Аномалії CAN, телематики, сенсорів	Потребує стабільної нормальної вибірки
LSTM/GRU	Часові ряди руху й технічного стану	Складність навчання та пояснення
Ізоляційний ліс	Табличні ознаки й телематика	Чутливість до налаштувань
Графові моделі	Транспортні мережі та взаємодії вузлів	Потребують графової структури
Класифікатори	Відомі типи атак і відмов	Потребують розмічених даних

Для оцінювання моделі ШІ використовують точність, повноту, F1-міру, ROC-AUC, затримку виявлення та стійкість до зміни умов. У транспортних системах важливим є баланс між хибно позитивними й хибно негативними спрацюваннями. Хибно негативне спрацювання може пропустити небезпечну атаку або відмову. Хибно позитивне може перевантажити оператора, створити недовіру до системи або викликати зайве втручання.

Функцію втрат для налаштування порога можна подати як:

$$L(\theta) = c_{FN} FN(\theta) + c_{FP} FP(\theta), \tag{6.19}$$

де c_{FN} і c_{FP} — вартість хибно негативних і хибно позитивних рішень. Для критичних функцій c_{FN} зазвичай значно вище, але надмірне зменшення порога може зробити систему непридатною через велику кількість хибних тривог.

моделі ШІ в ITS повинні бути захищені від атак на дані й моделі. Атакувальник може намагатися впливати на навчальні дані, подавати спеціально сформовані вхідні сигнали, приховувати аномалію або змусити модель помил-

ково класифікувати стан. Тому потрібні перевірка джерел даних, контроль якості навчальних вибірок, моніторинг дрейфуу, тестування на стійкість і обмеження автоматичних дій моделі [81, 44, 56].

Табл. 6.8: Ризики використання ШІ для надійності ITS

Ризик	**Прояв**	**Заходи контролю**
Дрейф даних	Зміна умов руху або сезонності	Перенавчання, моніторинг якості
Отруєння даних	Шкідливі приклади в навчанні	Перевірка джерел, очищення вибірок
Непояснюваність	Оператор не розуміє причину тривоги	ХШІ, журнали ознак, правила
Хибні тривоги	Перевантаження оператора	Налаштування порогів, пріоритезація
Автоматична помилка	Неправильна реакція системи	Людина в контурі, безпечні обмеження

Для транспортних потоків перспективними є графові підходи. Дорожню мережу можна подати графом $G = (V, E)$, де V — вузли, E — дорожні сегменти. Стан мережі описується матрицею ознак X_t. Аномалія може оцінюватися як відхилення фактичного стану від прогнозу графової моделі:

$$A_G(t) = \|X_t - f(G, X_{t-1}, ..., X_{t-k})\| . \tag{6.20}$$

Такий підхід дозволяє враховувати просторові зв'язки: затор або відмова датчика на одному сегменті впливає на сусідні ділянки.

Важливою є пояснюваність AI. Для оператора недостатньо отримати повідомлення "аномалія". Потрібно знати, які ознаки спричинили рішення: різка зміна температури ECU, нетипова частота CAN-кадрів, втрата V2X-повідомлень, неможлива траєкторія або відхилення від історичного профілю. Пояснюваність підвищує довіру та допомагає правильно реагувати.

Отже, штучний інтелект є потужним інструментом підвищення надійності ITS, але його потрібно використовувати обережно. моделі ШІ повинні бути валідувані, захищені, пояснювані, інтегровані з правилами безпеки та підконтрольні операційним процедурам. Найбільший ефект досягається тоді, коли ШІ доповнює діагностику, IDS, моніторинг і прогнозне обслуговування, а не замінює їх повністю.

6.5 Забезпечення відмовостійкості систем керування

Відмовостійкість систем керування означає здатність продовжувати виконання критичних функцій або переходити в безпечний стан у разі відмови компонентів, помилок програмного забезпечення, втрати зв'язку, деградації даних або кібератаки. Для ITS це стосується як бортових систем автомобіля, так і дорожньої інфраструктури, центрів керування та цифрових сервісів. Відмовостійкість є вищим рівнем надійності: система не лише рідко відмовляє, а й здатна контролювати наслідки відмов [2, 4, 78].

Системи керування автомобільним транспортом можуть працювати на локальному, коридорному, мережевому та стратегічному рівнях. Локальний рівень включає автомобіль і окремий контролер перехрестя. Коридорний рівень координує групу об'єктів. Мережевий рівень управляє міською або регіональною ITS. Стратегічний рівень визначає політики, пріоритети та планування. Відмовостійкість має бути забезпечена на кожному рівні, оскільки відмова локального компонента може вплинути на мережу, а відмова центру керування не повинна паралізувати локальні функції.

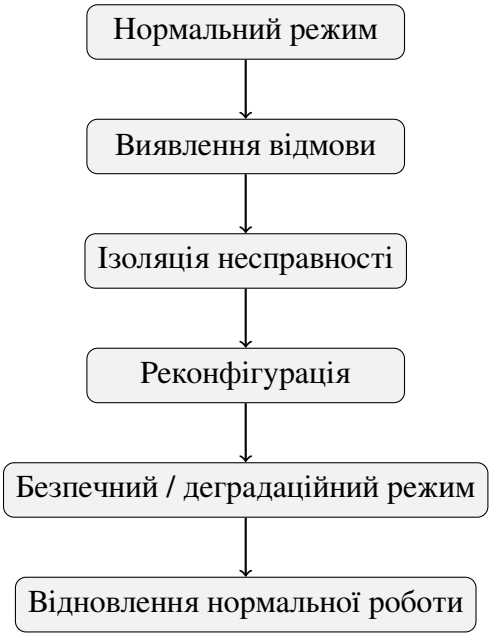

Рис. 6.5: Логіка відмовостійкого керування

Відмовостійке керування включає виявлення відмови, ізоляцію несправного компонента, оцінювання доступних ресурсів, реконфігурацію керування, перехід у деградаційний режим і відновлення. Формально керуючий вплив

можна подати як функцію стану та доступних ресурсів:

$$u(t) = \pi(x(t), r(t), q(t)), \tag{6.21}$$

де $x(t)$ — стан транспортної системи, $r(t)$ — доступні ресурси після відмови, $q(t)$ — якість даних. Якщо $r(t)$ або $q(t)$ знижуються, політика керування π повинна змінюватися.

Для системи керування важливо визначити мінімально прийнятний функціональний рівень:

$$F(t) \geq F_{min}. \tag{6.22}$$

Якщо фактична функціональна спроможність $F(t)$ нижча за F_{min}, система повинна перейти в безпечний стан, обмежити функцію або передати керування людині. Для автомобіля це може бути мінімально ризиковий маневр, для світлофора — локальний план, для центру керування — аварійна процедура.

Табл. 6.9: Деградаційні режими систем керування ITS

Відмова	**Деградаційний режим**	**Мета**
Втрата датчика авто	Використання резервних сенсорів, обмеження ADAS	Збереження безпеки руху
Втрата V2X	Локальне сприйняття та хмарний канал за наявності	Зменшення залежності від V2X
Відмова світлофорного зв'язку	Автономний локальний план	Уникнення хаосу на перехресті
Недоступність центру	Локальна координація або ручний режим	Підтримка базового керування
Деградація даних	Блокування автоматичних рішень, перевірка оператором	Запобігання хибним діям

Для відмовостійкого керування важлива ізоляція відмови. Якщо система не може визначити, який компонент несправний, вона може неправильно відключити справний канал або продовжити довіряти помилковому. Імовірність правильного відновлення можна подати як:

$$P_{rec} = P_{det} \cdot P_{iso} \cdot P_{reconf} \cdot P_{stable}, \tag{6.23}$$

де P_{det} — імовірність виявлення, P_{iso} — імовірність правильної ізоляції, P_{reconf} — імовірність успішної реконфігурації, P_{stable} — імовірність стабільної роботи після реконфігурації.

Відмовостійкість має враховувати кіберзагрози. Якщо система автоматично перемикається на резервний канал, атакувальник може спробувати спричинити відмову основного каналу й змусити систему перейти на менш захищений резерв. Якщо деградаційний режим має слабшу автентифікацію, він може стати вектором атаки. Тому резервні й деградаційні режими повинні мати не нижчий, а контрольований рівень кіберзахисту [1, 11, 40].

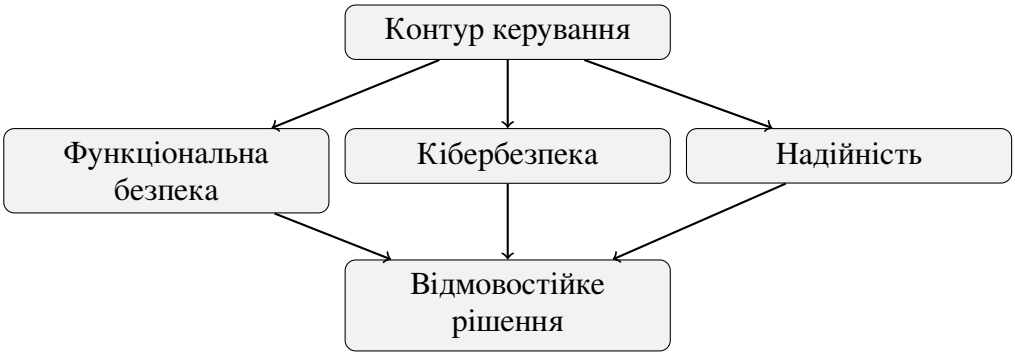

Рис. 6.6: Узгодження безпеки, кібербезпеки та надійності у відмовостійкому керуванні

У центрах керування відмовостійкість досягається резервними серверами, дублюванням баз даних, резервними каналами зв'язку, аварійними робочими місцями, локальними режимами інфраструктури та процедурами ручного керування. Важливо регулярно перевіряти, чи може центр перейти на резервний майданчик, чи актуальні резервні копії, чи оператори знають процедури, чи не втрачено доступ до критичних конфігурацій.

Показник стійкості керування можна визначити як:

$$S_c = \frac{T_{max} - T_{loss}}{T_{max}} \cdot Q_{deg}, \tag{6.24}$$

де T_{loss} — час втрати або деградації керування, T_{max} — максимально допустимий час, Q_{deg} — якість деградаційного режиму. Якщо S_c близький до одиниці, система швидко зберігає прийнятну функціональність.

Отже, забезпечення відмовостійкості систем керування є ключовим елементом підвищення надійності ITS. Воно потребує резервування, діагностики, ізоляції відмов, реконфігурації, безпечних деградаційних режимів, кіберзахи-

сту резервів і регулярного тестування. Лише така система здатна підтримувати безпечну мобільність у реальних умовах відмов, атак і невизначеності.

6.6 Інтегрована програма підвищення надійності інтелектуальних транспортних систем

Окремі методи підвищення надійності дають найбільший ефект тоді, коли вони об'єднані в інтегровану програму. Така програма повинна включати інвентаризацію активів, класифікацію критичних функцій, аналіз відмов, аналіз кіберзагроз, визначення показників надійності, впровадження резервування, організацію моніторингу, прогнозне обслуговування, ШІ-аналітику, відмовостійке керування та регулярний аудит. Без інтеграції ці заходи можуть існувати окремо й не давати системного ефекту.

Табл. 6.10: Елементи інтегрованої програми підвищення надійності ITS

Елемент	**Зміст**	**Результат**
Активи	Перелік автомобілів, ECU, датчиків, RSU, сервісів	База для аналізу ризику
Критичність	Визначення функцій із впливом на безпеку	Пріоритети резервування
Моніторинг	Потоки даних, журнали, телематика, SOC	Оперативна спостережуваність
Прогнозування	RUL, деградація, ШІ-аналітика	Планове обслуговування
Відмовостійкість	Деградаційні режими й реконфігурація	Збереження керованості
Аудит	Перевірка показників і процедур	Постійне вдосконалення

Інтегральний показник програми можна подати як:

$$I_R = w_1 R_d + w_2 M_r + w_3 P_m + w_4 A_i + w_5 F_t + w_6 C_s, \tag{6.25}$$

де R_d — рівень резервування, M_r — якість моніторингу, P_m — зрілість прогнозного обслуговування, A_i — ефективність ШІ-аналітики, F_t — відмовостійкість керування, C_s — кіберстійкість. Ваги w_i визначаються типом транспортної системи та критичністю функцій.

Впровадження програми має бути поетапним. На першому етапі ство-

рюється інвентаризація та базові показники. На другому — впроваджуються моніторинг і діагностика. На третьому — реалізується резервування критичних компонентів. На четвертому — додаються прогнозні моделі й ШІ-виявлення аномалій. На п'ятому — перевіряються деградаційні режими та відмовостійке керування. На шостому — програма переходить у цикл постійного вдосконалення.

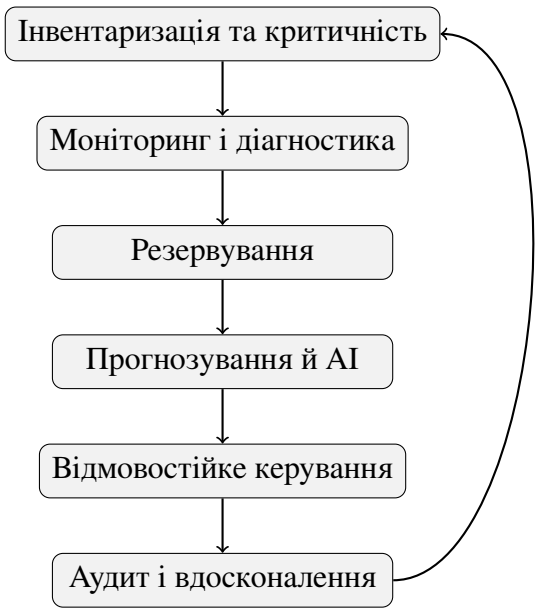

Рис. 6.7: Етапи інтегрованої програми підвищення надійності ITS

Економічну доцільність програми можна оцінити через баланс витрат і знижених втрат:

$$B = \sum_{t=1}^{T} \frac{\Delta C_t - C_{prog,t}}{(1+r)^t}, \tag{6.26}$$

де ΔC_t — зменшення втрат у період t, $C_{prog,t}$ — витрати на програму, r — коефіцієнт дисконтування. Якщо $B > 0$, програма має позитивний економічний ефект. Проте для критичних систем безпекова цінність може бути важливішою за прямий економічний результат.

6.7 Показники рівня обслуговування, ключові показники ефективності та оцінювання готовності транспортних сервісів

Для практичного підвищення надійності ITS важливо перейти від загальних тверджень до вимірюваних показників. У великих транспортних системах надійність повинна фіксуватися у вигляді цільових рівнів сервісу, або SLA.

Такі рівні можуть визначати доступність телематичної платформи, допустиму затримку V2X-повідомлень, час відновлення центру керування, повноту даних моніторингу, допустиму частку відмов датчиків і час реагування на критичні події. Без формальних показників складно довести, що надійність справді підвищується.

SLA для автомобільного транспорту має враховувати критичність функцій. Наприклад, сервіс аварійного попередження потребує вищої доступності та меншої затримки, ніж історичний звіт про пробіг. Сервіс керування світлофорним коридором потребує резервних сценаріїв, тоді як сервіс інформаційної аналітики може працювати з більшими затримками. Тому показники мають бути диференційованими за класами критичності.

Табл. 6.11: Приклади SLA/KPI для підвищення надійності ITS

Показник	**Зміст**	**Приклад цільового значення**
Доступність сервісу	Частка часу працездатності	$A \geq 0.995$ для критичних сервісів
Затримка повідомлення	Час від події до отримання	$T \leq T_{crit}$ для попереджень
Повнота даних	Частка отриманих телематичних записів	$C_{mon} \geq 0.98$
Час виявлення	Інтервал до фіксації інциденту	$MTTD$ у межах регламенту
Час відновлення	Інтервал до повернення функції	$MTTR \leq T_{max}$
Частка прогнозних ремонтів	Обслуговування до відмови	Зростання частки планових втручань

Доступність сервісу за період спостереження можна оцінити як:

$$A_s = 1 - \frac{T_{down}}{T_{obs}}, \tag{6.27}$$

де T_{down} — сумарний час недоступності, T_{obs} — загальний час спостереження. Якщо сервіс має кілька критичних компонентів, доцільно оцінювати не лише загальну доступність, а й внесок кожного компонента:

$$T_{down} = \sum_{i=1}^{n} T_{down,i} + T_{dep}, \tag{6.28}$$

де T_{dep} — додатковий час простою через залежності між компонентами.

Для моніторингу виконання SLA можна використовувати інтегральний індекс:

$$SLA_{idx} = w_1 A_s + w_2(1 - \frac{T_{lat}}{T_{max}}) + w_3 C_{mon} + w_4(1 - \frac{MTTR}{T_{rec}}), \qquad (6.29)$$

де T_{lat} — фактична затримка, T_{max} — допустима затримка, T_{rec} — нормативний час відновлення. Якщо SLA_{idx} опускається нижче порога, потрібне управлінське втручання.

Рис. 6.8: Цикл управління SLA/KPI надійності ITS

KPI повинні бути пов'язані з конкретними відповідальними суб'єктами. Якщо доступність V2X-сервісу низька, відповідальність може належати оператору дороги, постачальнику зв'язку, власнику RSU або центру сертифікації. Якщо високий MTTR для світлофорного контролера, проблема може бути у відсутності запасних частин, регламентів або навченого персоналу. Тому KPI мають бути не лише технічними, а й управлінськими.

6.8 Матриця критичності компонентів і планування обслуговування

Для підвищення надійності необхідно визначити, які компоненти є найкритичнішими. Не всі елементи ITS потребують однакового рівня резервування, моніторингу чи прогнозної діагностики. Критичність визначається впливом відмови на безпеку руху, масштабом наслідків, частотою використання, часом відновлення, наявністю резерву та кіберризиком. Матриця критичності допомагає розподіляти ресурси раціонально.

Табл. 6.12: Матриця критичності компонентів ITS

Компонент	**Критичність**	**Тип відмови**	**Пріоритет заходів**
Гальмівний ECU	Критична	Неправильна команда або недоступність	Резервування, самодіагностика, тестування
GNSS/IMU	Висока	Помилкова локалізація	Сенсорне злиття, перевірка правдоподібності
RSU	Висока	Втрата або підміна V2I	PKI, резервний канал, моніторинг
Світлофорний контролер	Критична	Неправильний режим фаз	Локальний план, резерв живлення, аудит
Телематична платформа	Висока	Недоступність або витік даних	IAM, резервування, SIEM, резервне копіювання
Мобільний застосунок	Середня	Недоступність сервісу	Контроль API, оновлення, підтримка

Критичність можна оцінити чисельно:

$$K_c = \alpha S + \beta M + \gamma E + \delta T_r + \epsilon C_y - \zeta R_b, \tag{6.30}$$

де S — тяжкість наслідків, M — масштаб впливу, E — експозиція, T_r — час відновлення, C_y — кіберризик, R_b — наявність резерву. Компоненти з найбільшим K_c повинні мати найвищий пріоритет у плані обслуговування.

Планування обслуговування може бути сформульоване як задача оптимізації:

$$\min \sum_{i=1}^{n} (C_{maint,i} + C_{fail,i} P_{fail,i}), \tag{6.31}$$

за умов:

$$A_i \geq A_i^{min}, \qquad R_i \leq R_i^{max}. \tag{6.32}$$

Тобто потрібно мінімізувати сумарні витрати на обслуговування та очікувані втрати від відмов, зберігаючи мінімальну доступність і максимальний допустимий ризик.

Матриця критичності повинна регулярно оновлюватися. Після зміни

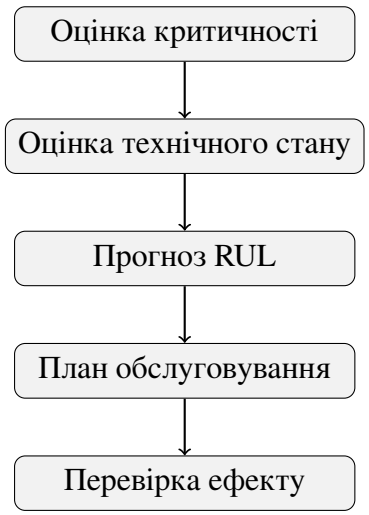

Рис. 6.9: Планування обслуговування на основі критичності та RUL

архітектури, додавання нового V2X-сервісу, оновлення програмного забезпечення, появи нової вразливості або зміни транспортного навантаження критичність компонентів може змінитися. Наприклад, компонент, який був допоміжним у традиційній системі, може стати критичним після впровадження автоматизованого керування.

6.9 Надійність даних і керування якістю інформаційних потоків

У цифровізованій ITS надійність технічних компонентів неможлива без надійності даних. Дані є основою для діагностики, прогнозування, ШІ-аналітики, маршрутизації, V2X-попереджень і керування рухом. Якщо дані неповні, застарілі, помилкові або підроблені, навіть справні технічні компоненти можуть сформувати неправильне рішення. Тому керування якістю даних є окремим напрямом підвищення надійності [32, 34, 61].

Якість даних включає повноту, точність, своєчасність, узгодженість, достовірність, просторову деталізацію та простежуваність походження. У транспортних системах особливо важливі своєчасність і узгодженість. Дані, які надійшли із запізненням, можуть бути непридатними для керування. Дані, що суперечать іншим джерелам, потребують перевірки перед використанням.

Інтегральний показник якості даних можна подати як:

$$Q_D = w_1 C + w_2 A + w_3 T + w_4 S + w_5 V + w_6 P, \tag{6.33}$$

де C — повнота, A — точність, T — своєчасність, S — узгодженість, V

Табл. 6.13: Параметри якості даних для надійності ITS

Параметр	**Зміст**	**Наслідок низької якості**
Повнота	Наявність усіх потрібних даних	Неповна картина стану
Точність	Близькість до реального значення	Неправильне рішення
Своєчасність	Актуальність у момент використання	Запізніле реагування
Узгодженість	Несуперечність між джерелами	Конфлікт алгоритмів
Достовірність	Перевірене походження й цілісність	Ризик атаки або помилки

— перевіреність, P — простежуваність. Якщо $Q_D < Q_{min}$, дані не повинні використовуватися для критичного керування без додаткової перевірки.

Для узгодження даних із кількох джерел можна використовувати зважене злиття:

$$\hat{x} = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}, \tag{6.34}$$

де x_i — оцінка від i-го джерела, w_i — вага довіри до цього джерела. Вага може залежати від історичної точності, стану датчика, затримки, сертифіката або контексту.

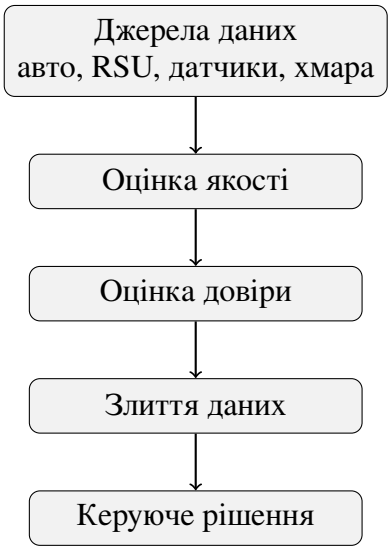

Рис. 6.10: Керування якістю даних у контурі надійності ITS

Надійність даних також залежить від кібербезпеки. Підроблені або змінені дані можуть виглядати як технічна помилка, а технічна помилка може

бути сприйнята як кібератака. Тому системи якості даних повинні взаємодіяти з IDS, криптографічною перевіркою та журналюванням. Для критичних потоків потрібно зберігати походження даних, версію алгоритму оброблення й часові мітки.

6.10 Організаційні процедури реагування та відновлення

Технічні методи підвищення надійності не будуть ефективними без організаційних процедур. Реальна транспортна система працює в умовах обмеженого часу, розподіленої відповідальності, змінного навантаження та взаємодії багатьох суб'єктів. Тому потрібно заздалегідь визначити, хто виявляє відмову, хто приймає рішення, хто виконує перемикання, хто повідомляє користувачів, хто відповідає за відновлення та хто аналізує причини.

Процедури реагування повинні бути сценарними. Для втрати зв'язку з транспортним засобом один сценарій; для відмови світлофорного контролера — інший; для деградації телематичної платформи — третій; для масової помилки оновлення — четвертий; для кібератаки на центр керування — п'ятий. Кожний сценарій має містити тригери, ролі, послідовність дій, допустимий час, резервні засоби й критерії завершення.

Табл. 6.14: Сценарії реагування на відмови в ITS

Сценарій	**Перші дії**	**Критерій відновлення**
Втрата V2X-вузла	Перевірка живлення, каналу, сертифіката	Стабільна передача й валідні повідомлення
Відмова світлофора	Перехід на локальний план, виїзд бригади	Повернення координованого режиму
Деградація датчика авто	Перевірка резервних джерел, обмеження функції	Підтверджена справність або заміна
Недоступність платформи	Перемикання на резерв, повідомлення операторів	Відновлення SLA й журналів
Масова помилка оновлення	Зупинка розгортання, відкат, аналіз впливу	Стабільна версія й закриття інциденту

Час реагування можна розкласти на етапи:

$$T_{resp} = T_{detect} + T_{decide} + T_{dispatch} + T_{repair} + T_{verify}, \tag{6.35}$$

де T_{detect} — виявлення, T_{decide} — прийняття рішення, $T_{dispatch}$ — направлення

ресурсу, T_{repair} — ремонт або відновлення, T_{verify} — перевірка. Зменшення будь-якого етапу підвищує загальну відновлюваність.

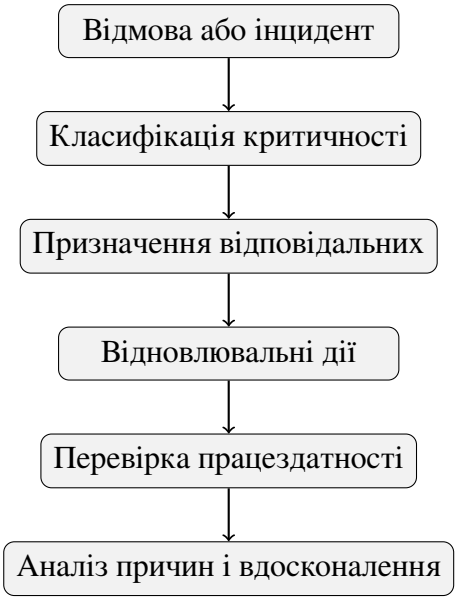

Рис. 6.11: Організаційний цикл реагування на відмови ITS

Після відновлення необхідно виконувати аналіз першопричин. Якщо причина не усунута, відмова повториться. Аналіз має охоплювати технічну причину, програмну причину, людський фактор, організаційну прогалину, кіберризик і недоліки моніторингу. Результатом має бути коригувальна дія: оновлення регламенту, зміна конфігурації, додаткове резервування, навчання персоналу або перегляд SLA.

6.11 Верифікація, випробування та навчання персоналу

Підвищення надійності має бути підтверджене випробуваннями. Недостатньо описати резервування або деградаційний режим у документації; потрібно перевірити, що він працює в реальних або наближених до реальних умовах. Випробування повинні включати відмову датчика, втрату зв'язку, відмову живлення, помилку оновлення, перевантаження платформи, кібераномалію та людську помилку. Для автоматизованих функцій важливі сценарні й симуляційні тести [75, 76, 77].

Покриття випробувань можна оцінити як:

$$C_{test} = \frac{N_{scen}^{tested}}{N_{scen}^{required}}, \tag{6.36}$$

Табл. 6.15: Види випробувань для підтвердження надійності ITS

Випробування	**Мета**	**Приклад**
Функціональне	Перевірка заданої функції	Коректність локального плану світлофора
Відмовне	Перевірка реакції на відмову	Втрата основного каналу зв'язку
Навантажувальне	Оцінка роботи під піком	Масовий потік телематики
Кіберстійкість	Перевірка при атаці або аномалії	Підроблені V2X-повідомлення
Відновлення	Перевірка резервів і відкату	Відновлення після помилки оновлення
Навчальне	Перевірка персоналу	Тренування центру керування

де N_{scen}^{tested} — кількість перевірених сценаріїв, $N_{scen}^{required}$ — кількість обов'язкових сценаріїв. Для критичних систем значення C_{test} має бути близьким до одиниці, але важлива не лише кількість сценаріїв, а й їх якість.

Навчання персоналу є складовою надійності. Оператор, який не розуміє деградаційного режиму або неправильно інтерпретує попередження, може посилити наслідки технічної відмови. Тому персонал повинен регулярно проходити тренування з реагування на відмови, кіберінциденти, втрату зв'язку, недоступність даних і аварійні транспортні події. Навчання має включати не лише інструкції, а й практичні сценарії.

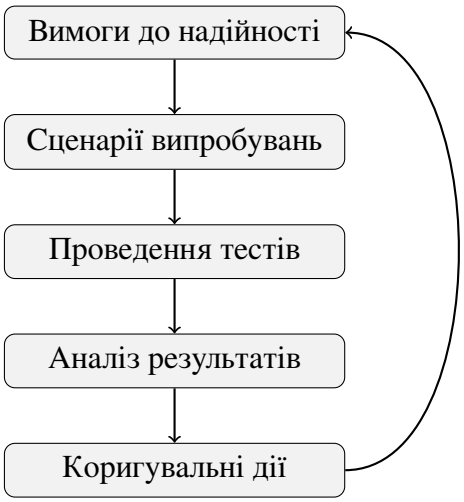

Рис. 6.12: Цикл верифікації надійності ITS

Отже, верифікація, випробування та навчання персоналу закривають цикл підвищення надійності. Вони показують, чи працюють резерви, чи пра-

вильні прогнози, чи здатна система відновитися, чи готові оператори діяти в умовах невизначеності. Без регулярних випробувань надійність залишається припущенням, а не підтвердженою властивістю.

6.12 Дорожня карта впровадження заходів підвищення надійності

Для реального впровадження заходів підвищення надійності потрібна дорожня карта. Вона визначає послідовність дій, відповідальних суб'єктів, ресурси, строки, контрольні показники та критерії завершення етапів. Без дорожньої карти резервування, моніторинг, ШІ-аналітика й відмовостійке керування можуть залишитися окремими проєктами, які не створюють єдиного ефекту для транспортної системи.

Перший етап дорожньої карти — базовий аудит. Він включає інвентаризацію транспортних засобів, датчиків, ECU, комунікаційних модулів, RSU, серверів, каналів зв'язку, програмних версій і експлуатаційних процедур. На цьому етапі визначаються критичні функції, поточні показники доступності, типові відмови, середній час відновлення та наявні резерви. Без цього неможливо обґрунтовано визначити пріоритети.

Другий етап — створення системи моніторингу й діагностики. Його завдання полягає у забезпеченні видимості стану компонентів. Якщо система не бачить власного стану, вона не може прогнозувати відмови або реагувати вчасно. На цьому етапі впроваджуються телематичні потоки, журнали, панелі операторів, контроль якості даних і базові правила попередження.

Третій етап — резервування та деградаційні режими. Для критичних компонентів визначаються резерви, перевіряється незалежність, налаштовуються правила перемикання, створюються локальні плани роботи та аварійні регламенти. Особливу увагу потрібно приділяти перевірці резерву, оскільки неперевірений резерв може виявитися недоступним саме під час відмови.

Четвертий етап — прогнозне обслуговування й ШІ-аналітика. На основі зібраних даних будуються моделі деградації, оцінювання RUL, виявлення аномалій і пріоритезації технічного обслуговування. На цьому етапі важливо не передавати ШІ-моделям неконтрольовані повноваження, а використовувати їх як інструмент підтримки рішень з пояснюваними результатами.

П'ятий етап — верифікація, навчання й постійне вдосконалення. Він включає регулярні випробування, навчання персоналу, кібернавчання, ана-

ліз інцидентів, перегляд SLA/KPI та оновлення матриці критичності. Саме цей етап перетворює підвищення надійності на безперервний процес, а не одноразове впровадження.

Табл. 6.16: Дорожня карта підвищення надійності автомобільного транспорту в ITS

Етап	**Основні дії**	**Критерій завершення**
Аудит	Інвентаризація, критичність, базові KPI	Повний реєстр активів і ризиків
Моніторинг	Телематика, журнали, якість даних	Видимість критичних станів
Резервування	Дублювання, локальні режими, перемикання	Перевірений резерв і сценарії деградації
Прогнозування	RUL, ШІ-аналітика, планування ТО	Планове попередження відмов
Верифікація	Тести, навчання, аудит, вдосконалення	Підтверджене виконання SLA

Пріоритет виконання етапів можна визначити через індекс готовності:

$$G_{road} = \frac{A_{assets} + A_{data} + A_{staff} + A_{budget} + A_{risk}}{5}, \tag{6.37}$$

де A_{assets} — готовність інвентаризації, A_{data} — готовність даних, A_{staff} — готовність персоналу, A_{budget} — ресурсна готовність, A_{risk} — зрілість аналізу ризиків. Якщо G_{road} низький, складні ШІ-рішення або масштабне резервування можуть бути передчасними.

Ризик невиконання дорожньої карти можна оцінити як:

$$R_{impl} = P_{delay} I_{delay} + P_{budget} I_{budget} + P_{data} I_{data} + P_{staff} I_{staff}, \tag{6.38}$$

де $P_{delay}, P_{budget}, P_{data}, P_{staff}$ — імовірності затримки, нестачі бюджету, низької якості даних і нестачі персоналу, а I — відповідні наслідки. Ця формула показує, що надійність залежить не лише від технічних рішень, а й від управління впровадженням.

Дорожня карта повинна завершуватися не статичним документом, а циклом удосконалення. Після кожного інциденту, тесту або зміни архітектури потрібно переглядати критичність, SLA, резервування, моделі прогнозування та процедури реагування. Такий підхід забезпечує адаптацію ITS до нових

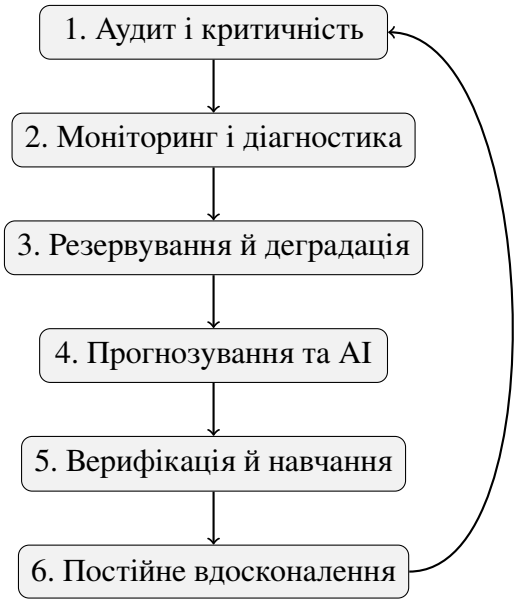

Рис. 6.13: Дорожня карта впровадження заходів підвищення надійності

Табл. 6.17: Ризики впровадження програми підвищення надійності та способи зниження

Ризик	**Прояв**	**Спосіб зниження**
Низька якість даних	Помилкові прогнози й аномалії	Валідація, очищення, контроль джерел
Недостатнє фінансування	Неповне резервування або моніторинг	Пріоритезація за критичністю
Опір персоналу	Формальне виконання процедур	Навчання й участь операторів
Несумісність систем	Проблеми інтеграції компонентів	Відкриті інтерфейси, тестування
Кіберризики резервів	Компрометація запасних каналів	Однаковий рівень захисту резерву

транспортних, технологічних і кібербезпекових умов.

6.13 Узагальнення підходів до підвищення надійності

Підвищення надійності автомобільного транспорту в ITS потребує системного підходу. Резервування зменшує ризик одиничних відмов; діагностика й прогнозування дозволяють діяти до відмови; моніторинг у реальному часі забезпечує спостережуваність; штучний інтелект виявляє складні аномалії; відмовостійке керування підтримує безпечну функціональність у деградаційних режимах. Разом ці методи формують основу стійкого автомобільного транспорту.

Табл. 6.18: Узагальнення методів підвищення надійності автомобільного транспорту в ITS

Метод	**Основна функція**	**Ключовий ризик**
Резервування	Збереження функції після відмови	Спільні причини відмов і складність
Діагностика	Виявлення несправностей і деградації	Неповні або недостовірні дані
Прогнозування	Оцінка залишкового ресурсу	Помилка моделі або дрейф даних
Моніторинг	Оперативна спостережуваність	Затримки, втрата зв'язку, кіберризики
ШІ-аналітика	Виявлення складних аномалій	Непояснюваність і хибні тривоги
Відмовостійке керування	Безпечна деградація й відновлення	Неправильна реконфігурація

Загальний ефект підвищення надійності можна оцінити як:

$$E_R = \frac{R_{base} - R_{new}}{R_{base}} \cdot 100\%, \tag{6.39}$$

де R_{base} — базовий рівень ризику відмов і деградації, R_{new} — рівень після впровадження заходів. Для практичного застосування цей показник доцільно деталізувати за компонентами: транспортні засоби, інфраструктура, зв'язок, дані, центри керування та організаційні процеси.

Надійність не повинна розглядатися окремо від кібербезпеки. Резервний канал може бути вразливим; діагностичні дані можуть бути підроблені; модель

ШІ може бути атакована; моніторинг може порушувати приватність; деградаційний режим може мати слабші механізми захисту. Тому кожний метод підвищення надійності повинен проходити оцінку кіберризику та функціональної безпеки [1, 2, 4, 11].

Підсумовуючи, підвищення надійності автомобільного транспорту в ITS є безперервним процесом, що поєднує технічні рішення, програмні механізми, дані, штучний інтелект, кібербезпеку й організаційні процедури. Його кінцева мета полягає у забезпеченні такої транспортної системи, яка здатна працювати безпечно, передбачувано й стійко навіть за умов відмов, атак, неповних даних і змінного транспортного середовища.

7 Інтегрована стратегія розвитку кібербезпечних і надійних інтелектуальних транспортних систем

7.1 Передумови формування інтегрованої стратегії

Розвиток інтелектуальних транспортних систем в автомобільному транспорті не може обмежуватися окремим упровадженням датчиків, телематичних платформ, засобів зв'язку або програмних сервісів. Такі елементи створюють цінність лише тоді, коли вони поєднані в керовану архітектуру, де кібербезпека, функціональна безпека, експлуатаційна надійність, захист даних і нормативна відповідність розглядаються як взаємозалежні складові. Якщо один із цих компонентів залишається поза системним управлінням, загальна ефективність ITS знижується, а ризики переходять із технічного рівня на організаційний і соціальний.

Інтегрована стратегія повинна враховувати специфіку автомобільного транспорту: високу кількість учасників, різнорідність транспортних засобів, тривалий життєвий цикл, залежність від дорожньої інфраструктури, використання бездротових каналів зв'язку та постійне накопичення телематичних даних. Саме тому стратегічне управління ITS має спиратися не лише на технічні стандарти, а й на процедури прийняття рішень, аудит, навчання персоналу, сценарне планування та механізми швидкого відновлення після інцидентів.

Ключовим принципом такої стратегії є перехід від реактивної моделі до проактивної. Реактивна модель передбачає усунення наслідків після появи відмови або атаки. Проактивна модель орієнтується на прогнозування, раннє виявлення аномалій, оцінювання залишкового ризику й постійне вдосконалення контролів. Для автомобільного транспорту це особливо важливо, оскільки навіть локальний збій у цифровому сервісі може вплинути на безпеку руху, пропускну здатність мережі, довіру користувачів і економічну ефективність перевезень.

7.2 Цільова архітектура управління кіберстійкістю інтелектуальних транспортних систем

Цільова архітектура управління кіберстійкістю ITS має охоплювати п'ять взаємопов'язаних рівнів: рівень транспортного засобу, рівень дорожньої інфраструктури, рівень комунікацій, рівень центрів керування та рівень організаційного управління. На рівні транспортного засобу пріоритетними є захист електронних блоків керування, бортових мереж, діагностичних інтерфейсів, датчиків і програмних оновлень. На рівні інфраструктури важливими є захист світлофорних об'єктів, дорожніх сенсорів, камер, станцій V2X і периферійних обчислювальних вузлів.

Комунікаційний рівень повинен забезпечувати автентифікацію повідомлень, цілісність даних, керування сертифікатами, шифрування критичних потоків і захист від підміни або повторного передавання повідомлень. Центри керування мають виконувати функції моніторингу, кореляції подій, диспетчерського реагування, резервного керування та аналітичної підтримки рішень. Організаційний рівень об'єднує політики, регламенти, відповідальність, аудит, навчання та взаємодію з регуляторами, постачальниками й операторами.

Узагальнений рівень кіберстійкості ITS можна подати як інтегральний показник:

$$R_{ITS} = w_1 R_v + w_2 R_i + w_3 R_c + w_4 R_o + w_5 R_m, \tag{7.1}$$

де R_v — стійкість транспортних засобів, R_i — стійкість інфраструктури, R_c — стійкість комунікацій, R_o — організаційна готовність, R_m — здатність до моніторингу та відновлення, $w_1, \ldots, w_5$ — вагові коефіцієнти. Такий підхід дозволяє не зводити оцінювання до одного технічного компонента, а порівнювати різні сценарії розвитку ITS за сукупним ефектом.

7.3 Модель поетапного впровадження інтегрованої стратегії

Практичне впровадження інтегрованої стратегії доцільно здійснювати поетапно. Перший етап полягає в інвентаризації активів, потоків даних, програмного забезпечення, каналів зв'язку, зовнішніх інтеграцій і критичних функцій. Без такого опису неможливо коректно визначити межі системи та відповідальність за ризики. Другий етап передбачає класифікацію активів за критичністю, впливом на безпеку руху, залежністю від персональних даних і

складністю відновлення.

Третій етап охоплює моделювання загроз і ризиків. Для кожного критичного активу необхідно визначити можливі сценарії атаки або відмови, наслідки, імовірність, наявні контролі та залишковий ризик. Четвертий етап передбачає розроблення портфеля заходів: технічних, організаційних, нормативних і навчальних. П'ятий етап полягає у впровадженні моніторингу, регулярному тестуванні, аудиті та перегляді стратегії за результатами інцидентів, змін технологій і появи нових вимог.

Табл. 7.1: Етапи впровадження інтегрованої стратегії ITS

Етап	**Основний зміст**	**Очікуваний результат**
1	Інвентаризація активів і потоків даних	Карта системи та меж відповідальності
2	Класифікація критичності	Пріоритети захисту й резервування
3	Моделювання загроз і відмов	Реєстр ризиків і сценаріїв інцидентів
4	Вибір і впровадження контролів	Узгоджений портфель заходів
5	Моніторинг, аудит і вдосконалення	Цикл постійного підвищення стійкості

Ефективність етапного впровадження можна оцінювати через показник зрілості:

$$M_{ITS} = \frac{1}{n} \sum_{k=1}^{n} m_k, \tag{7.2}$$

де m_k — рівень зрілості окремого процесу: управління активами, кіберризиками, оновленнями, інцидентами, доступом, даними, аудитом або навчанням. Значення M_{ITS} доцільно використовувати не як формальний рейтинг, а як інструмент планування наступних кроків.

7.4 Практичні рекомендації для операторів і органів управління

Для операторів автомобільного транспорту першочерговим завданням є створення єдиного реєстру цифрових активів. До нього мають входити транспортні засоби, бортові пристрої, програмні версії, канали зв'язку, облікові записи, постачальники, телематичні сервіси та критичні API. Такий реєстр по-

винен оновлюватися не епізодично, а в межах регулярного процесу управління конфігураціями.

Другим практичним завданням є запровадження регламенту безпечних оновлень. Оновлення програмного забезпечення має проходити перевірку цілісності, тестування сумісності, контроль версій, оцінювання впливу на безпеку та можливість повернення до попереднього стану. Для транспортних систем це не лише питання кібербезпеки, а й питання експлуатаційної надійності, оскільки помилка оновлення може створити масовий збій у роботі сервісу.

Третім завданням є побудова центру моніторингу подій ITS або інтеграція транспортних систем із наявним центром кіберзахисту. Такий центр повинен збирати події з транспортних засобів, інфраструктури, серверів, мережевих пристроїв і прикладних сервісів. Важливо, щоб моніторинг не обмежувався фіксацією технічних помилок, а дозволяв виявляти нетипові шаблони поведінки, зокрема масові відмови датчиків, аномальні команди, різке зростання затримок або підозрілу активність облікових записів.

Для органів управління транспортом важливими є вимоги до сумісності, відкритості інтерфейсів, мінімального рівня кіберзахисту, захисту персональних даних і готовності до аудиту. У договорах із постачальниками ITS-рішень доцільно передбачати вимоги до документації, журналювання, оновлень, повідомлення про вразливості, строків реагування та передачі даних у стандартизованих форматах. Це зменшує залежність від одного постачальника й підвищує керованість життєвого циклу системи.

7.5 Узагальнені висновки монографії

Проведене дослідження показує, що інтелектуальні транспортні системи є базовим напрямом розвитку автомобільного транспорту, але їх ефективність залежить від здатності забезпечити кібербезпеку, функціональну безпеку, експлуатаційну надійність і нормативну відповідність у єдиній системі управління. Цифровізація підвищує продуктивність перевезень, якість інформаційних сервісів і можливості диспетчеризації, однак одночасно створює нові залежності від програмного забезпечення, каналів зв'язку, даних і постачальників.

У монографії обґрунтовано, що кіберзагрози для автомобільного транспорту мають системний характер. Вони можуть впливати на бортові мережі, V2X-комунікації, дорожню інфраструктуру, центри керування, телематичні

платформи та персональні дані. Тому захист ITS повинен будуватися за принципом багаторівневої оборони, де технічні засоби доповнюються організаційними процедурами, аудитом, резервуванням і навчанням персоналу.

Надійність автомобільного транспорту в умовах цифровізації визначається не лише технічним станом механічних компонентів, а й стабільністю датчиків, електронних блоків керування, програмного забезпечення, інформаційних потоків і центрів оброблення даних. Це потребує переходу до прогнозної діагностики, цифрових двійників, моніторингу в реальному часі та ризик-орієнтованого планування технічного обслуговування.

Нормативно-правове та стандартизаційне забезпечення формує основу довіри до ITS. Міжнародні стандарти ISO, UNECE, ETSI та IEEE, а також вимоги до захисту даних і українське законодавство мають застосовуватися не фрагментарно, а як взаємопов'язана система. Для України особливого значення набуває поетапна гармонізація з європейськими підходами, розвиток національних профілів стандартів, підготовка експертів і проведення пілотних проєктів.

Отже, стратегічний розвиток кібербезпечних і надійних ITS повинен ґрунтуватися на інтеграції архітектури, ризик-менеджменту, нормативної відповідності, моніторингу, відновлення та постійного вдосконалення. Такий підхід дозволяє підвищити безпеку руху, стійкість транспортних сервісів, довіру користувачів і готовність автомобільного транспорту до подальшої цифрової трансформації.

8 Нормативно-правове та стандартизаційне забезпечення

Нормативно-правове та стандартизаційне забезпечення є основою безпечного розвитку автомобільного транспорту в інтелектуальних транспортних системах. Технологічні рішення ITS не можуть ефективно функціонувати без узгоджених вимог до архітектури, кібербезпеки, функціональної безпеки, оновлення програмного забезпечення, захисту даних, сертифікації, управління ризиками та відповідальності учасників. Стандарти визначають технічні й процесні вимоги, а нормативно-правові акти встановлюють обов'язкові правила, права, обов'язки та механізми контролю. Для автомобільного транспорту, що стає підключеним, програмно-визначеним і залежним від даних, така нормативна рамка є не формальністю, а умовою безпечної експлуатації [1, 2, 3, 9, 10].

Складність нормативного забезпечення полягає в тому, що ITS поєднує кілька сфер регулювання: автомобільну безпеку, кібербезпеку, телекомунікації, захист персональних даних, дорожній рух, стандартизацію, технічне регулювання, цифрові сервіси та міжнародну сумісність. Один і той самий компонент, наприклад V2X-модуль, одночасно підпадає під вимоги комунікаційної архітектури, криптографічної безпеки, захисту приватності, функціональної безпеки та експлуатаційної надійності. Тому стандарти повинні застосовуватися не ізольовано, а як узгоджена система [5, 6, 7, 8, 13].

Для України питання гармонізації стандартів має особливе значення через необхідність модернізації транспортної інфраструктури, інтеграції з європейськими підходами, підвищення кіберстійкості та розвитку цифрових сервісів мобільності. Гармонізація не означає механічне копіювання документів. Вона потребує адаптації вимог до національної правової системи, інституційних можливостей, стану інфраструктури, ринку транспортних послуг і процедур технічного регулювання [28, 29, 12, 5].

8.1 Міжнародні стандарти кібербезпеки автомобільного транспорту

Міжнародні стандарти кібербезпеки автомобільного транспорту формують процесну, технічну та організаційну основу захисту підключених транс-

портних засобів і ITS. Найважливішими документами є ISO/SAE 21434, UN Regulation No. 155, ISO 24089, UN Regulation No. 156, рамка кібербезпеки NIST 2.0, рекомендації ENISA, стандарти ETSI та IEEE для ITS/V2X-комунікацій. Кожен із цих документів має власну сферу застосування, але разом вони формують систему вимог до життєвого циклу кібербезпеки [1, 9, 3, 10, 11, 12].

ISO/SAE 21434 визначає підхід до інженерії кібербезпеки дорожніх транспортних засобів. Його логіка базується на управлінні ризиками протягом життєвого циклу: від концепції та розроблення до виробництва, експлуатації, обслуговування та виведення з експлуатації. Стандарт не обмежується технічними контролями; він вимагає процесів, ролей, відповідальності, аналізу загроз, оцінювання ризиків, формування вимог кібербезпеки, верифікації, валідації та моніторингу після випуску [1].

UN Regulation No. 155 встановлює вимоги до кібербезпеки та системи управління кібербезпекою транспортного засобу. Його значення полягає в тому, що кібербезпека стає частиною процедур схвалення типу транспортних засобів. Виробник повинен продемонструвати наявність система управління кібербезпекою, здатність ідентифікувати ризики, впроваджувати заходи, моніторити загрози та реагувати на інциденти. Це перетворює кібербезпеку з добровільної практики на регуляторну вимогу [9].

рамка кібербезпеки NIST 2.0 корисний для ITS як загальна рамка управління кіберризиками. Він структурує діяльність навколо функцій управління, ідентифікації, захисту, виявлення, реагування та відновлення. Для транспортної організації це означає, що потрібно не лише впровадити захисні засоби, а й мати управління, інвентаризацію активів, процедури виявлення, реагування та відновлення. Така логіка добре поєднується з потребами центрів керування, операторів автопарків і постачальників телематичних сервісів [11].

ETSI TS 102 940 і ETSI TS 103 097 визначають архітектурні та форматні аспекти безпеки ITS-комунікацій. Вони важливі для C-ITS, оскільки описують безпекові заголовки, сертифікати, підписи та механізми довіри для повідомлень. IEEE 1609.2 і IEEE 1609.2.1 виконують споріднену роль у середовищі WAVE, визначаючи безпекові сервіси й інтерфейси керування сертифікатами [16, 17, 20, 21].

Взаємодію стандартів можна подати як покриття вимог. Нехай $S = \{s_1, s_2, \ldots, s_n\}$ — множина стандартів, а $R = \{r_1, r_2, \ldots, r_m\}$ — множина

Табл. 8.1: Ключові міжнародні документи з кібербезпеки автомобільного транспорту

Документ	**Сфера регулювання**	**Практичне значення**
ISO/SAE 21434	Інженерія кібербезпеки автомобіля	Процеси TARA, вимоги, верифікація, життєвий цикл
UN R155	Кібербезпека та CSMS для схвалення типу	Регуляторний контроль виробника
ISO 24089	Інженерія оновлення ПЗ	Керування OTA/оновленнями та конфігураціями
UN R156	SUMS і оновлення ПЗ	Нормативне підтвердження керованого оновлення
NIST CSF 2.0	Загальна рамка кіберризиків	Ідентифікація, захист, виявлення, реагування, відновлення, управління
ETSI/IEEE V2X	Безпека ITS-комунікацій	Сертифікати, підписи, заголовки, мережеві сервіси

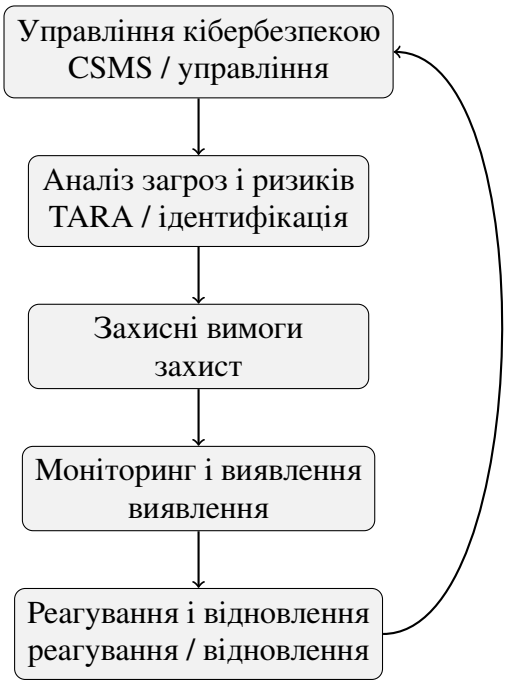

Рис. 8.1: Узагальнений цикл нормативного управління кібербезпекою автомобільного транспорту

вимог кібербезпеки. Тоді матриця покриття має вигляд:

$$A = [a_{ij}], \qquad a_{ij} = \begin{cases} 1, & \text{стандарт } s_i \text{ покриває вимогу } r_j, \\ 0, & \text{інакше.} \end{cases} \tag{8.1}$$

Інтегральне покриття вимог можна оцінити як:

$$C_R = \frac{\sum_{j=1}^{m} \max_i a_{ij} w_j}{\sum_{j=1}^{m} w_j}, \tag{8.2}$$

де w_j — критичність вимоги. Якщо $C_R < 1$, залишаються прогалини, які потрібно закривати додатковими політиками або національними нормативами.

Табл. 8.2: Співвідношення стандартів і життєвого циклу кібербезпеки

Етап	**Нормативна опора**	**Ключовий результат**
Концепція	ISO/SAE 21434, NIST CSF	Область застосування та активи
Аналіз ризику	ISO/SAE 21434, SAE J3061, SAHARA	TARA, класифікація загроз
Проєктування	ISO/SAE 21434, ETSI, IEEE	Вимоги, архітектура, криптографія
Оновлення	ISO 24089, UN R156	Керований процес ПЗ
Експлуатація	UN R155, NIST CSF, ENISA	Моніторинг, інциденти, відновлення

Важливо, що стандарти не замінюють інженерне мислення. Виконання вимог ISO/SAE 21434 або UN R155 не гарантує абсолютної відсутності ризику. Воно забезпечує структурований процес, у межах якого ризики ідентифікуються, оцінюються, зменшуються та контролюються. Тому нормативна відповідність повинна розглядатися як мінімальна умова, а не як межа розвитку кібербезпеки.

8.2 Функціональна безпека та міжнародний стандарт 26262

ISO 26262 є базовим міжнародним стандартом функціональної безпеки дорожніх транспортних засобів. Він зосереджений на небезпеках, що виникають через відмови електричних та електронних систем. Для цифровізованого автомобільного транспорту цей стандарт залишається фундаментальним,

оскільки більшість критичних функцій — гальмування, кермування, стабілізація, енергетичне керування, ADAS — залежать від електроніки та програмного забезпечення [2].

Функціональна безпека відрізняється від загальної надійності тим, що її центральним об'єктом є небезпечна відмова. Компонент може бути ненадійним, але не створювати значної небезпеки; і навпаки, рідкісна відмова критичної функції може бути неприпустимою. ISO 26262 вводить систематичний підхід до ідентифікації небезпек, оцінювання ризику, визначення рівень повноти автомобільної безпеки (ASIL), формування цілей безпеки, технічних вимог і перевірки їх виконання.

Рис. 8.2: Логіка функціональної безпеки за ISO 26262

Оцінювання ASIL базується на трьох параметрах: тяжкість наслідків S, експозиція E і керованість C. Узагальнену функцію ризику можна подати як:

$$R_{ASIL} = f(S, E, C). \tag{8.3}$$

Для навчального аналізу зручно використовувати числову апроксимацію:

$$R_s = w_S S + w_E E + w_C C, \tag{8.4}$$

де w_S, w_E, w_C — вагові коефіцієнти. Чим вищі тяжкість, експозиція та складність керування ситуацією, тим вищий рівень вимог до безпеки.

Для ITS важливим є те, що функціональна безпека автомобіля взаємодіє

Табл. 8.3: Ключові поняття ISO 26262 для автомобільного транспорту

Поняття	**Зміст**	**Практичне значення**
Елемент аналізу	Система або функція, що аналізується	Межі аналізу безпеки
Небезпека	Потенційне джерело шкоди	Початок HARA
Небезпечна подія	Небезпека в конкретному сценарії	Оцінка ризику
ASIL	Рівень цілісності безпеки	Глибина вимог і перевірок
Ціль безпеки	Ціль безпеки високого рівня	Основа технічних вимог
Механізм безпеки	Механізм зниження ризику	Діагностика, резервування, безпечний стан

з інфраструктурою та цифровими сервісами. Якщо автомобіль отримує дані від V2X, карти або хмарного сервісу, потрібно визначити, чи є ці дані частиною функції безпеки. Якщо так, їх достовірність, затримка, доступність і цілісність мають бути включені в аналіз. Інакше функція може формально відповідати ISO 26262 на рівні автомобіля, але залишатися небезпечною в реальному ITS-середовищі.

ISO 21448 доповнює ISO 26262, фокусуючись на безпеці передбачуваної функціональності. Це важливо для систем сприйняття та автоматизованого водіння, де небезпечна поведінка може виникнути без класичної відмови. Наприклад, камера може бути справною, але неправильно класифікувати об'єкт у складних умовах. Тому ISO 26262, ISO 21448 та кібербезпека мають застосовуватися разом [4, 75, 76, 71].

Табл. 8.4: Співвідношення ISO 26262, ISO 21448 та кібербезпеки

Сфера	**Типова причина ризику**	**Приклад**
ISO 26262	Випадкова або систематична відмова E/E	Відмова ECU гальмування
ISO 21448	Небезпечна поведінка без відмови	Помилкове сприйняття дорожньої сцени
ISO/SAE 21434	Навмисна атака або зловмисна зміна	Підміна V2X або прошивки
Експлуатаційна надійність	Деградація сервісу або компонента	Втрата зв'язку з центром керування

Для оцінювання достатності механізмів безпеки можна використати показник діагностичного покриття:

$$DC = \frac{\lambda_{detected}}{\lambda_{total}}, \tag{8.5}$$

де $\lambda_{detected}$ — інтенсивність відмов, які виявляються механізмами діагностики, λ_{total} — загальна інтенсивність релевантних відмов. Високе діагностичне покриття зменшує ризик небезпечних прихованих відмов.

Впровадження ISO 26262 у контексті ITS потребує розширення меж аналізу. Потрібно враховувати не лише автомобіль, а й взаємодію з дорожньою інфраструктурою, оновленнями, даними й операторами. Наприклад, якщо функція адаптивного руху залежить від даних інфраструктури, межі item можуть включати інтерфейс V2I або вимоги до достовірності зовнішніх повідомлень.

8.3 Кібербезпека транспортних засобів та міжнародний стандарт 21434

ISO/SAE 21434 є центральним стандартом кібербезпеки автомобільної галузі. Його значення полягає в тому, що він вводить інженерію кібербезпеки як структурований процес, пов'язаний з життєвим циклом транспортного засобу. Стандарт охоплює організаційне управління, проєктне управління, розподілену розробку, безперервну діяльність, концепцію, розроблення продукту, виробництво, експлуатацію, обслуговування та виведення з експлуатації [1].

Ключовим елементом ISO/SAE 21434 є TARA — аналіз загроз і оцінювання ризиків. TARA дає змогу визначати активи, сценарії загроз, шляхи атак, вплив, ймовірність, рівень ризику та вимоги кібербезпеки. Для ITS TARA має враховувати не лише автомобільні активи, а й V2X-вузли, телематичні платформи, оновлення, дорожню інфраструктуру, сертифікати, дані користувачів і центри керування [64, 73, 64].

Ризик у TARA можна представити як функцію впливу та здійсненності атаки:

$$R_{cyber} = F(Impact, AttackFeasibility). \tag{8.6}$$

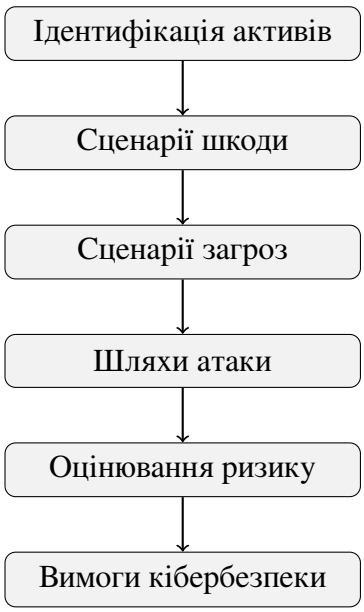

Рис. 8.3: Узагальнений процес TARA за логікою ISO/SAE 21434

Для кількісної ілюстрації можна використати модель:

$$R_{cyber} = I \cdot AF, \tag{8.7}$$

де I — інтегральний вплив на безпеку, експлуатацію, фінанси та приватність, AF — здійсненність атаки. Здійсненність може залежати від часу, знань, доступу, обладнання та вікна можливості:

$$AF = w_t T + w_k K + w_a A + w_e E + w_o O. \tag{8.8}$$

ISO/SAE 21434 тісно пов'язаний з UN Regulation No. 155. Якщо стандарт описує інженерний процес, то UN R155 робить наявність CSMS регуляторною вимогою. Виробник повинен довести, що здатний управляти кіберризиками не лише під час розроблення, а й після випуску транспортного засобу. Це особливо важливо для OTA-оновлень, нових вразливостей і довгого життєвого циклу автомобіля [9, 3, 10].

Важливим питанням є узгодження ISO/SAE 21434 з ISO 26262. Кіберзахисний механізм не повинен створювати нову небезпеку, а функціонально безпечна система не повинна залишатися вразливою до навмисних атак. Наприклад, автентифікація повідомлень має бути достатньо швидкою, щоб не порушити часові вимоги; аварійний доступ має бути контрольованим, щоб не стати вектором атаки; деградаційний режим має бути і безпечним, і захищеним.

Табл. 8.5: Елементи TARA для автомобільного транспорту в ITS

Елемент	**Зміст**	**Приклад**
Актив	Те, що має цінність і потребує захисту	ECU, V2X-ключ, телематичні дані
Сценарій шкоди	Небажаний наслідок	Небезпечний маневр, витік маршруту
Сценарій загрози	Потенційна дія атакувальника	Підроблення повідомлення
Шлях атаки	Послідовність кроків	Компрометація API та команда авто
Ризик	Поєднання впливу і здійсненності	Пріоритет захисту
Вимога	Захисна ціль або контроль	Підпис, IDS, сегментація

Табл. 8.6: Зіставлення ISO/SAE 21434 та UN Regulation No. 155

Критерій	**ISO/SAE 21434**	**UN R155**
Тип документа	Стандарт інженерії кібербезпеки	Регуляторна вимога схвалення типу
Фокус	Процеси, TARA, вимоги, життєвий цикл	CSMS, управління ризиками, доказ відповідності
Суб'єкт	Організація та проєкти розроблення	Виробник транспортного засобу
Результат	Вимоги й артефакти кібербезпеки	Підтвердження керованості кіберризику
Експлуатація	Моніторинг і підтримка	Обов'язковий контроль після випуску

Індекс узгодженості функціональної та кібербезпеки можна подати як:

$$C_{SS} = \frac{N_{linked}}{N_{safety} + N_{security} - N_{overlap}}, \tag{8.9}$$

де N_{linked} — кількість вимог, що мають простежений зв'язок між безпекою та кібербезпекою, N_{safety} і $N_{security}$ — загальна кількість відповідних вимог, $N_{overlap}$ — перетин. Низьке значення C_{SS} свідчить про ризик розриву між аналізами.

Для ITS ISO/SAE 21434 повинен застосовуватися ширше, ніж лише до автомобіля. Хоча стандарт орієнтований на дорожніх транспортних засобів, його принципи корисні для телематичних платформ, V2X-сервісів, центрів керування й дорожніх вузлів. Активи, загрози, вимоги, верифікація та моніторинг потрібні на всіх рівнях ITS, інакше слабка ланка інфраструктури може знизити безпеку всього транспортного середовища.

8.4 Вимоги до захисту даних у транспортних системах

Захист даних у транспортних системах є нормативно-правовим питанням, яке безпосередньо пов'язане з кібербезпекою, приватністю, довірою користувачів і законністю цифрових сервісів. ITS обробляє геолокацію, маршрути, час поїздок, стиль водіння, технічний стан, ідентифікатори пристроїв, відео, платежі, дані мобільних застосунків і журнали подій. Частина цих даних є персональними або може стати персональною після поєднання з іншими наборами [53, 52, 54].

Європейський підхід до захисту персональних даних базується на принципах законності, справедливості, прозорості, обмеження мети, мінімізації даних, точності, обмеження строку зберігання, цілісності, конфіденційності та підзвітності. Для підключених транспортних засобів ці принципи означають, що оператор або виробник повинен чітко пояснювати, які дані збираються, навіщо, на якій правовій підставі, як довго зберігаються, кому передаються та як користувач може реалізувати свої права [53, 52].

Ризик повторної ідентифікації в ITS є високим через унікальність маршрутів. Навіть якщо ім'я користувача видалено, регулярні координати можуть показати місце проживання, роботи або звичні маршрути. Тому анонімізація транспортних даних є складною, а в багатьох випадках доцільніше гово-

Табл. 8.7: Принципи захисту даних та їх застосування в ITS

Принцип	**Зміст**	**Приклад в ITS**
Мінімізація	Збирати лише необхідні дані	Не зберігати точну геолокацію без потреби
Обмеження мети	Дані лише для заявленої цілі	Діагностика не повинна автоматично ставати маркетингом
Прозорість	Зрозуміла інформація користувачу	Політика телематичного застосунку
Точність	Актуальні та правильні дані	Виправлення помилкових записів
Безпека	Захист від доступу, зміни, втрати	Шифрування, IAM, аудит
Підзвітність	Доказ виконання вимог	Журнали, DPIA, договори з підрядниками

рити про псевдонімізацію та зменшення ризику, а не про повне усунення ідентифікації.

Формально ризик приватності можна подати як:

$$R_p = P_{id} \cdot I_p, \tag{8.10}$$

де P_{id} — імовірність ідентифікації або повторної ідентифікації, I_p — наслідки для особи. Імовірність ідентифікації зростає зі збільшенням кількості квазіідентифікаторів:

$$P_{id} = 1 - \prod_{i=1}^{n} (1 - q_i), \tag{8.11}$$

де q_i — внесок окремої ознаки, наприклад місця, часу, пристрою або поведінкового шаблону.

Акт ЄС про дані додає до теми даних ще один вимір: доступ до даних і справедливе використання. Для підключених транспортних засобів це означає потребу балансувати між інтересами користувача, виробника, сервісної організації, постачальника цифрового сервісу та суспільними потребами. Доступ до даних має бути прозорим, контрольованим і безпечним, щоб не створювати нові ризики приватності чи кібербезпеки [54].

Українське законодавство про захист персональних даних і кібербезпеку створює національну рамку, у якій мають розвиватися ITS-сервіси. Закон

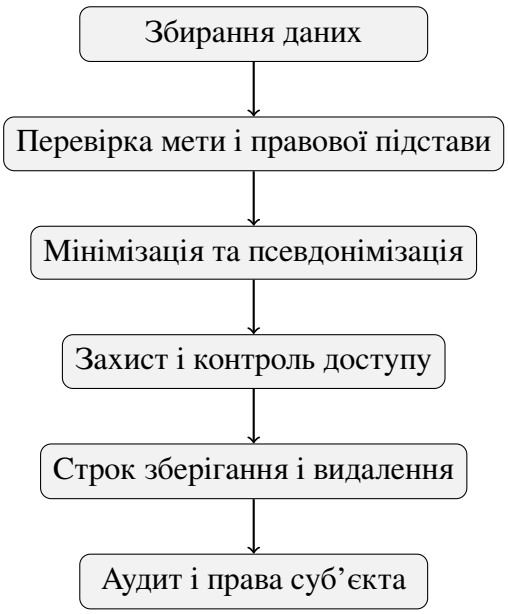

Рис. 8.4: Життєвий цикл захисту даних у транспортній системі

України "Про захист персональних даних" визначає базові вимоги до оброблення персональних даних, а Закон України "Про основні засади забезпечення кібербезпеки України" встановлює загальні засади кібербезпеки та захисту критичної інфраструктури [53, 12]. Для транспортних систем важливо поєднати ці вимоги з європейськими й міжнародними стандартами.

Табл. 8.8: Категорії транспортних даних і нормативні вимоги

Дані	**Ризик**	**Вимога захисту**
Геолокація	Відстеження особи	Мінімізація, псевдонімізація, строк зберігання
Стиль водіння	Профілювання та дискримінація	Прозорість, правова підстава, обмеження мети
Діагностика	Комерційна чутливість	Контроль доступу, договори з сервісами
V2X-псевдоніми	Повторна ідентифікація	Ротація, політика сертифікатів
Відео/аудіо	Дані третіх осіб	DPIA, обмеження доступу, маскування

Для оцінювання відповідності захисту даних можна використати індекс:

$$D_{comp} = w_1 L + w_2 M + w_3 T + w_4 S + w_5 A + w_6 R, \tag{8.12}$$

де L — правова підстава, M — мінімізація, T — прозорість, S — безпека, A — аудит, R — реалізація прав суб'єкта. Низьке значення будь-якого компонента вказує на потребу в коригувальних заходах.

Отже, вимоги до захисту даних у транспортних системах мають бути інтегровані в архітектуру ITS з самого початку. Захист даних не може бути доданий після запуску сервісу, оскільки структура збирання, зберігання, доступу та обміну визначається на етапі проєктування. Для довіри користувачів приватність є такою ж важливою, як функціональна безпека чи кіберстійкість.

8.5 Перспективи гармонізації стандартів в Україні

Гармонізація стандартів в Україні є необхідною умовою розвитку сучасного автомобільного транспорту в ITS. Вона має забезпечити сумісність із європейськими підходами, підвищити безпеку транспортних сервісів, створити прозорі вимоги для виробників і операторів, підтримати цифровізацію інфраструктури та зменшити ризики фрагментарного впровадження несумісних рішень. Водночас гармонізація потребує не лише перекладу стандартів, а й створення інституційної спроможності їх застосовувати [28, 29, 5, 29].

Першим напрямом є нормативне наближення до європейської рамки ITS. Директива (ЄС) 2023/2661 оновлює підхід до розгортання ITS у дорожньому транспорті та взаємодії з іншими видами транспорту. Для України це важливо з погляду сумісності сервісів, доступності даних, стандартних інтерфейсів і розвитку цифрової мобільності. Гармонізація має включати не лише загальні принципи, а й технічні профілі даних, вимоги до якості та безпеки сервісів [28, 29].

Другим напрямом є впровадження автомобільних стандартів кібербезпеки та оновлень. ISO/SAE 21434, ISO 24089, UN R155 і UN R156 повинні стати орієнтирами для виробників, імпортерів, сервісних організацій, операторів автопарків і регуляторів. Навіть якщо не всі вимоги можуть бути негайно зроблені обов'язковими, їх доцільно використовувати як основу для технічних умов, тендерних вимог, сертифікаційних процедур і внутрішніх політик [1, 3, 9, 10].

Гармонізацію можна описати як процес зменшення розриву між націо-

Табл. 8.9: Напрями гармонізації стандартів ITS в Україні

Напрям	**Міжнародна основа**	**Очікуваний результат**
Архітектура ITS	ISO 14813-1, ISO 21217, ETSI EN 302 665	Сумісність сервісів і компонентів
Кібербезпека авто	ISO/SAE 21434, UN R155	Керований життєвий цикл кіберризиків
Оновлення ПЗ	ISO 24089, UN R156	Безпечні OTA та контроль версій
V2X-комунікації	ETSI, IEEE, 3GPP	Довіра, сертифікати, гібридний зв'язок
Дані й приватність	GDPR, EDPB, Акт про дані, українське право	Захист користувачів і прозорий обмін

нальними вимогами N та міжнародною цільовою рамкою I:

$$G_h = 1 - \frac{\|I - N\|}{\|I\|}. \tag{8.13}$$

Якщо G_h наближається до одиниці, рівень гармонізації високий. На практиці $\|I - N\|$ означає не математичну норму документів, а кількість і критичність розбіжностей у вимогах, процедурах, термінах, ролях і механізмах контролю.

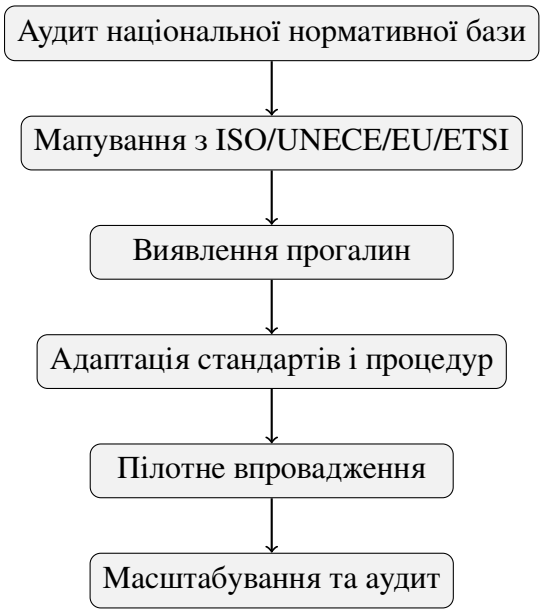

Рис. 8.5: Послідовність гармонізації стандартів ITS в Україні

Третім напрямом є підготовка кадрів і інституцій. Стандарти не працюють без фахівців, здатних їх застосовувати. Потрібні експерти з автомобільної

кібербезпеки, функціональної безпеки, ITS-архітектури, захисту даних, сертифікації, аудиту та управління інцидентами. Освітні програми, професійна сертифікація й навчання операторів мають стати частиною гармонізації.

Четвертим напрямом є пілотні проєкти. Доцільно починати з транспортних коридорів, міських центрів керування, автопарків громадського транспорту або логістичних систем, де можна перевірити стандартизовані інтерфейси, вимоги до даних, кібербезпеку, SLA та процедури реагування. Результати пілотів повинні використовуватися для уточнення національних профілів стандартів.

Табл. 8.10: Етапи впровадження гармонізованих вимог в Україні

Етап	**Зміст**	**Результат**
1	Інвентаризація законодавства, стандартів і практик	Карта поточного стану
2	Вибір пріоритетних міжнародних стандартів	Цільова нормативна рамка
3	Розроблення національних профілів і методик	Практичні вимоги для впровадження
4	Пілотні ITS-проєкти та аудит	Перевірка застосовності
5	Масштабування, навчання, сертифікація	Системне впровадження
6	Постійний перегляд відповідно до нових стандартів	Актуальність і сумісність

Для оцінювання готовності до гармонізації можна використати індекс:

$$H_U = w_1 L + w_2 S + w_3 I + w_4 P + w_5 E + w_6 A, \tag{8.14}$$

де L — готовність законодавства, S — наявність стандартів, I — інституційна спроможність, P — пілотні проєкти, E — експертний потенціал, A — механізми аудиту. Низький компонент показує, де потрібні першочергові дії.

П'ятим напрямом є узгодження захисту даних. Українські ITS-сервіси мають бути сумісними з європейськими очікуваннями щодо приватності, прозорості й доступу до даних. Це важливо для міжнародних перевезень, інтеграції цифрових сервісів, участі європейських постачальників і довіри користувачів. Гармонізація повинна включати не лише правові норми, а й технічні заходи: псевдонімізацію, контроль доступу, аудит, строки зберігання

та безпечні API.

8.6 Інтегрована модель нормативної відповідності інтелектуальних транспортних систем

Оскільки ITS охоплює багато стандартів і правових актів, потрібна інтегрована модель нормативної відповідності. Така модель дозволяє пов'язати вимоги до кібербезпеки, функціональної безпеки, оновлень, V2X, захисту даних і експлуатаційної надійності в єдину систему управління. Без інтеграції організація може виконувати окремі вимоги, але залишати прогалини на стиках між сферами.

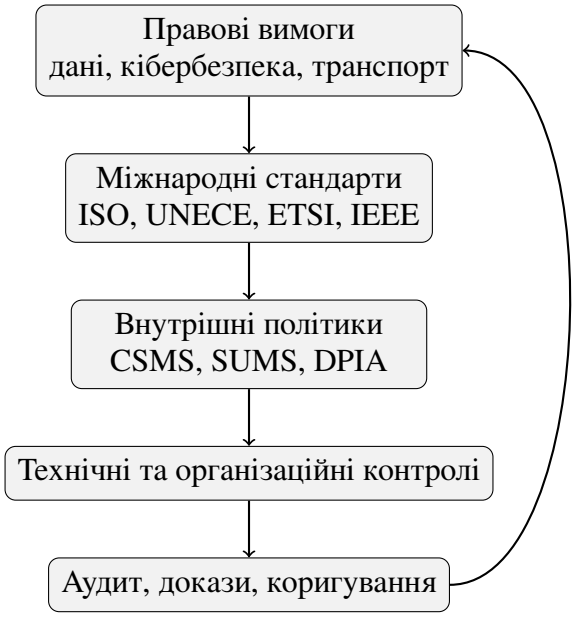

Рис. 8.6: Інтегрована модель нормативної відповідності ITS

Нормативна відповідність може бути оцінена за матрицею вимог і доказів. Нехай R_j — вимога, E_j — наявний доказ виконання, K_j — критичність. Тоді рівень відповідності можна подати як:

$$C_{norm} = \frac{\sum_{j=1}^{m} K_j E_j}{\sum_{j=1}^{m} K_j}, \qquad E_j \in [0,1]. \tag{8.15}$$

Якщо доказ частковий, E_j може мати проміжне значення. Такий підхід корисний для аудиту, тендерних вимог і підготовки до сертифікації.

Важливою складовою є доказова база. Організація повинна не лише стверджувати, що вимоги виконані, а й мати документи, журнали, результати

Табл. 8.11: Приклад матриці нормативної відповідності ITS

Група вимог	**Нормативна основа**	**Доказ виконання**
CSMS	ISO/SAE 21434, UN R155	Політика, TARA, журнал інцидентів
SUMS	ISO 24089, UN R156	Реєстр версій, підпис оновлень, відкат
V2X-безпека	ETSI TS 102 940, ETSI TS 103 097, IEEE 1609.2	Сертифікати, підписи, перевірка повідомлень
Функціональна безпека	ISO 26262, ISO 21448	HARA, ASIL, тестування, обґрунтування безпеки
Захист даних	GDPR, EDPB, Акт про дані, українське право	DPIA, політики доступу, журнали, строки зберігання

тестів, звіти аудиту, записи оновлень, реєстр активів і процедури реагування. У транспортних системах доказова база має бути достатньою для технічного аудиту, розслідування інциденту та підтвердження відповідності перед регулятором або замовником.

Інтегрована модель також повинна враховувати оновлення стандартів. Нормативне середовище змінюється: оновлюються ISO-документи, розвиваються європейські акти, змінюються підходи до даних і кібербезпеки. Тому відповідність не може бути одноразовою. Потрібен процес моніторингу змін і перегляду вимог:

$$T_{review} \leq T_{change} + T_{impact} + T_{update}, \tag{8.16}$$

де T_{change} — час виявлення зміни стандарту, T_{impact} — оцінка впливу, T_{update} — впровадження змін у політики й контролі.

8.7 Дорожня карта стандартизації та висновки до розділу

Дорожня карта стандартизації ITS повинна поєднувати міжнародні вимоги, національну правову базу, інституційну спроможність і практичні пілотні проєкти. Її мета — створити передбачуване середовище, у якому автомобільний транспорт може цифровізуватися без втрати безпеки, приватності й надійності. Така дорожня карта має бути поетапною, оскільки одночасне впровадження всіх стандартів може перевищити можливості організацій.

Табл. 8.12: Дорожня карта стандартизаційного забезпечення ITS

Етап	**Основні дії**	**Результат**
1	Визначення базових стандартів ISO, UNECE, ETSI, IEEE	Цільова нормативна архітектура
2	Мапування з українським законодавством	Виявлення прогалин
3	Розроблення національних профілів ITS	Практичні вимоги до проєктів
4	Пілоти з кібербезпеки, V2X, даних і оновлень	Перевірені методики
5	Сертифікація, аудит і навчання персоналу	Спроможність застосування
6	Постійний перегляд і оновлення	Актуальна відповідність

Узагальнений пріоритет стандартизаційного заходу можна визначити як:

$$P_s = \alpha R + \beta I + \gamma U + \delta E - \eta C, \tag{8.17}$$

де R — рівень ризику, який зменшує захід, I — вплив на сумісність, U — актуальність для України, E — європейська інтеграційна значущість, C — складність впровадження. Це дозволяє визначати, які стандарти впроваджувати першочергово.

Рис. 8.7: Цикл стандартизаційного розвитку ITS

Підсумовуючи, нормативно-правове та стандартизаційне забезпечення

є необхідною умовою розвитку кібербезпечного й надійного автомобільного транспорту в ITS. ISO 26262 формує основу функціональної безпеки; ISO/SAE 21434 — основу кібербезпеки; ISO 24089 і UN R156 — основу керованого оновлення; UN R155 — регуляторний вимір кібербезпеки; ETSI та IEEE — основу довіри у V2X; GDPR, EDPB, Акт про дані і українське законодавство — основу захисту даних. Гармонізація цих вимог в Україні має здійснюватися поетапно, з урахуванням технічної сумісності, інституційної спроможності, кіберстійкості та європейської інтеграції.

9 Перспективи розвитку кібербезпечного та надійного автомобільного транспорту

Перспективи розвитку автомобільного транспорту в середовищі інтелектуальних транспортних систем визначаються одночасним ускладненням транспортних засобів, дорожньої інфраструктури, комунікаційних мереж, хмарних сервісів, алгоритмів штучного інтелекту та нормативних вимог. Якщо попередні етапи цифровізації переважно додавали до автомобіля окремі електронні функції, то наступний етап формує повноцінну мережеву кіберфізичну екосистему. У ній автономний транспортний засіб, V2X-вузол, периферійний сервер, центр керування, цифровий сертифікат, телематична платформа й користувацький застосунок працюють як взаємозалежні елементи єдиного сервісу мобільності [5, 6, 28, 29, 43, 44].

Головна особливість майбутнього розвитку полягає в тому, що кібербезпека та надійність перестають бути допоміжними вимогами. Вони стають умовою масштабування автономного руху, кооперативних сервісів, 5G/6G-комунікацій, хмарно-периферійної обробки даних, блокчейн-реєстрів і цифрових сертифікатів. Чим більше функцій автомобіля залежить від даних і зовнішніх сервісів, тим вищими стають вимоги до автентичності, доступності, цілісності, часової синхронізації, відмовостійкості та контрольованості оновлень [1, 2, 3, 9, 10, 11, 12].

Для стратегічного аналізу майбутню готовність автомобільного транспорту до безпечної цифрової трансформації доцільно подати інтегральним показником:

$$P_{future} = \alpha A + \beta C + \gamma E + \delta D + \eta R + \theta G, \tag{9.1}$$

де A — рівень автономності та валідації автоматизованих функцій, C — якість комунікацій 5G/6G і V2X, E — зрілість периферійно-хмарних архітектури, D — захищеність даних і цифрової ідентичності, R — експлуатаційна надійність, G — нормативна та організаційна готовність. Такий показник підкреслює, що майбутній розвиток не може оцінюватися тільки за технологічним рівнем

автомобіля.

9.1 Розвиток автономних транспортних засобів

Автономні транспортні засоби є одним із найскладніших напрямів розвитку автомобільного транспорту, оскільки вони поєднують сенсорні системи, алгоритми сприйняття, машинне навчання, планування траєкторії, керування приводами, цифрові карти, V2X-комунікації та взаємодію з людиною. Перехід від систем допомоги водієві до високих рівнів автоматизації означає, що транспортний засіб повинен самостійно виявляти об'єкти, прогнозувати поведінку учасників руху, приймати рішення в умовах невизначеності й переходити в безпечний стан у разі деградації функцій [43, 44, 45, 46, 47, 48].

З погляду надійності автономний автомобіль є багатоканальною системою, у якій помилка одного компонента не повинна призводити до неконтрольованої поведінки. Камери мають високу інформативність, але залежать від освітлення та погодних умов. Радари краще працюють у складній видимості, але мають обмеження в класифікації об'єктів. Лідари формують точну просторову картину, але можуть бути чутливими до забруднення, опадів і вартості. Тому майбутня архітектура автономного транспорту має спиратися на сенсорне злиття, діагностику деградації та резервування критичних функцій [31, 45, 46, 79, 80].

Найважливішою методичною проблемою автономного транспорту є валідація. Кількість можливих дорожніх сценаріїв надзвичайно велика, тому неможливо перевірити систему лише традиційними дорожніми випробуваннями. Потрібне поєднання реальних тестів, симуляції, апаратно-програмних стендів, цифрових двійників, сценарного аналізу та післяексплуатаційного моніторингу. Особливу увагу необхідно приділяти рідкісним, але небезпечним сценаріям: нестандартній поведінці пішоходів, частково перекритій розмітці, помилковим дорожнім знакам, тимчасовим ремонтним зонам, аварійним транспортним засобам і конфліктам між локальним сприйняттям та V2X-даними [75, 76, 77, 72, 4].

Для формалізації готовності автономної функції можна використати індекс:

$$A_{ready} = w_1 S_f + w_2 V_s + w_3 D_g + w_4 R_b + w_5 M_o - w_6 U_n, \tag{9.2}$$

Табл. 9.1: Ключові напрями розвитку автономних транспортних засобів

Напрям	**Технологічний зміст**	**Вимоги до безпеки й надійності**
Сенсорне злиття	Камери, радари, лідари, GNSS, IMU	Виявлення деградації, узгодження даних, резервування
ШІ-сприйняття	Класифікація об'єктів, сегментація, прогноз руху	Валідація моделей, контроль невизначеності, ODD
Планування руху	Траєкторії, маневри, взаємодія з учасниками	Безпечні обмеження, пояснюваність, режим збереження працездатності після відмови
V2X-підтримка	Кооперативне сприйняття, попередження, сигнали RSU	Автентифікація, затримка, захист від підміни
Оновлення ПЗ	OTA, моделі ШІ, карти, конфігурації	ISO 24089, відкат, контроль версій, журнали

де S_f — повнота сенсорного покриття, V_s — обсяг сценарної валідації, D_g — здатність виявляти деградацію, R_b — рівень резервування, M_o — якість моніторингу після випуску, U_n — невизначеність поведінки моделі ШІ. Якщо U_n зростає, система повинна обмежувати операційний дизайн або переходити в більш консервативний режим.

Кібербезпека автономних транспортних засобів має безпосередній зв'язок із функціональною безпекою. Атака на датчик, карту, модель машинного навчання, канал V2X або механізм оновлення може проявитися як неправильне рішення системи керування. Наприклад, підміна об'єкта на вході камери, спотворення координат GNSS, повторне відтворення V2X-повідомлення або компрометація OTA-оновлення можуть створити небезпечну ситуацію без класичної механічної відмови [70, 62, 63, 38, 39, 40].

Майбутня архітектура автономного транспорту повинна використовувати принципи багаторівневого захисту. На фізичному рівні потрібні стійкі датчики та діагностика. На рівні даних — перевірка достовірності, часових міток і джерел. На рівні ШІ — контроль невизначеності та виявлення позарозподільних ситуацій. На рівні керування — обмеження команд і безпечний відмовний режим/режим збереження працездатності після відмови режими.

Рис. 9.1: Функціональна архітектура автономного транспортного засобу

На рівні організації — CSMS, SUMS, аудит, оновлення та аналіз інцидентів [1, 2, 3, 9, 10, 81, 82].

Табл. 9.2: Сценарії ризику автономного автомобіля та захисні механізми

Сценарій	**Можливий наслідок**	**Перспективний контроль**
Підміна даних датчика	Хибне сприйняття перешкоди або її відсутності	Сенсорне злиття, перевірка фізичної правдоподібності
Атака на модель ШІ	Неправильна класифікація об'єкта	змагальне тестування, виявлення позарозподільних сценаріїв, контроль довіри
Компрометація карти	Помилковий маневр або обмеження швидкості	Підпис карт, версійність, порівняння з локальним сприйняттям
Повторне передавання V2X	Неправильне попередження або маневр	Часові мітки, сертифікати, перевірка контексту
Помилка OTA	Масова деградація функції	A/B-оновлення, відкат, поетапне розгортання

Надійність автономного автомобіля можна оцінювати через імовірність безпечного завершення поїздки:

$$P_{safe} = \prod_{i=1}^{n}(1 - p_i) \cdot P_{detect} \cdot P_{fallback}, \tag{9.3}$$

де p_i — імовірність критичної відмови компонента i, P_{detect} — імовірність своєчасного виявлення деградації, $P_{fallback}$ — імовірність успішного переходу до безпечного або резервного режиму. Така модель показує, що навіть наявність відмови не обов'язково призводить до небезпечного стану, якщо система має ефективне виявлення та резервний режим.

У перспективі автономні транспортні засоби будуть дедалі більше інтегровані з інфраструктурою. Кооперативне сприйняття, цифрові коридори, розумні перехрестя, високоточні карти та периферійні сервіси дозволять зменшити невизначеність локального сприйняття. Однак це створить нову залежність: безпечність автономного руху частково залежатиме від зовнішніх даних. Тому майбутні автономні системи повинні бути не лише підключеними, а й здатними безпечно деградувати в автономний локальний режим у разі втрати довіри до інфраструктури [6, 14, 15, 33, 26, 27].

Додаткові сценарії розвитку автономності та експлуатаційної готовності

Подальший розвиток автономного транспорту буде залежати від здатності виробників і операторів доводити безпечність не лише окремої функції, а й усього операційного середовища. Для цього необхідно формувати паспорти ODD, у яких фіксуються допустимі типи доріг, швидкісні діапазони, погодні умови, видимість, якість розмітки, наявність цифрової карти, рівень V2X-покриття та вимоги до водія або дистанційного оператора. Якщо хоча б один параметр виходить за допустимі межі, автономна функція повинна знижувати рівень автоматизації або переходити в мінімально ризиковий стан [4, 75, 76, 77].

Важливою перспективою є поєднання автономного автомобіля з цифровим двійником транспортної мережі. Цифровий двійник може моделювати дорожню ситуацію, прогнозувати конфліктні точки, оцінювати ризик маневру та порівнювати поведінку транспортного засобу з очікуваною поведінкою потоку. Проте цифровий двійник не повинен бути єдиним джерелом істини: автономний транспортний засіб має перевіряти зовнішні рекомендації через локальне сприйняття та контекстну логіку [5, 6, 34, 35, 36].

Табл. 9.3: Параметри ODD для перспективного автономного транспорту

Параметр ODD	**Що контролюється**	**Дія при виході за межі**
Тип дороги	Автомагістраль, місто, сільська дорога	Обмеження швидкості або вимкнення функції
Погодні умови	Дощ, сніг, туман, заслiплення	Підвищення дистанції, запит ручного режиму
Якість розмітки	Видимість смуг і знаків	Перехід до карти/V2X або безпечний стан
V2X-покриття	Доступність RSU, CAM/DENM, затримка	Локальний режим без кооперативних рішень
Стан датчиків	Забруднення, деградація, відмова	Резервний канал або мінімально ризиковий маневр

Ризик виходу автономної функції за межі ODD можна подати як:

$$R_{ODD} = \sum_{i=1}^{n} \pi_i z_i c_i, \tag{9.4}$$

де π_i — імовірність порушення параметра i, z_i — індикатор фактичного виходу за допустиму межу, c_i — критичність параметра для безпечного руху. Якщо R_{ODD} перевищує поріг, система повинна ініціювати деградацію функції.

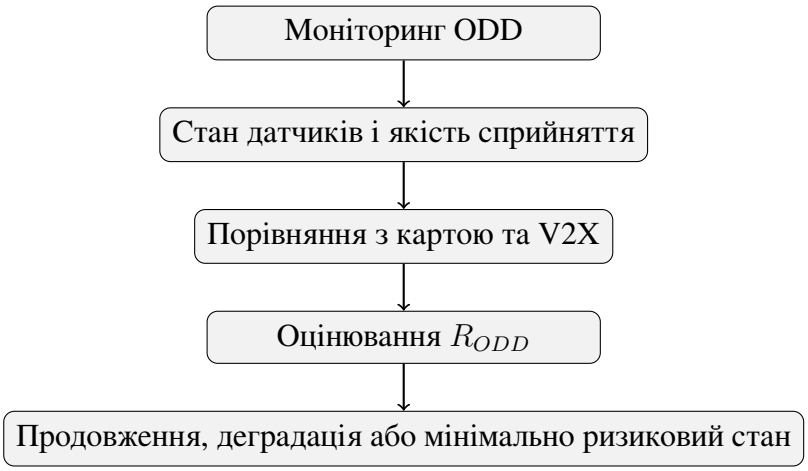

Рис. 9.2: Контур контролю ODD автономного транспортного засобу

Перспективною є також експлуатаційна сертифікація автономних функцій після випуску. Оскільки програмне забезпечення, карти та моделі ШІ оновлюються протягом життєвого циклу, одноразове підтвердження безпечності на етапі виробництва стає недостатнім. Потрібна модель безперервного підтвердження функціональної та кібербезпеки, у якій кожне оновлення про-

ходить оцінку впливу на HARA, TARA, ODD, валідаційні сценарії та дані післяексплуатаційного моніторингу [2, 1, 3, 9, 10, 71].

9.2 Інтеграція мобільних мереж нового покоління, хмарних сервісів та периферійних обчислень

Інтеграція 5G/6G, хмарних сервісів і периферійні обчислення визначатиме наступний етап розвитку ITS. Якщо традиційні транспортні системи переважно передавали дані до централізованого центру керування, то майбутні системи будуть розподіленими. Частина оброблення відбуватиметься в автомобілі, частина — на периферійному вузлі біля дороги або базової станції, частина — у хмарній платформі, а стратегічна аналітика — у міських або регіональних центрах даних. Така архітектура зменшує затримку, але ускладнює кібербезпеку, надійність і керування конфігураціями [24, 25, 26, 27, 6, 61].

5G створює передумови для сервісів із низькою затримкою, високою пропускною здатністю та мережевим сегментуванням. Для ITS це важливо для кооперативного сприйняття, передавання відео з інфраструктури, пріоритезації екстреного транспорту, дистанційної діагностики, оновлень і підтримки автономних функцій. 6G у перспективі може додати ще вищу щільність підключень, інтеграцію комунікацій і сенсингу, орієнтовані на ШІ мережі та наднизькі затримки. Однак кожне з цих покращень збільшує залежність транспорту від телекомунікаційної інфраструктури [33, 24, 25, 26, 23].

Затримку сервісу ITS можна описати як суму компонентів:

$$L_{tot} = L_{veh} + L_{radio} + L_{edge} + L_{backhaul} + L_{cloud} + L_{proc}, \tag{9.5}$$

де L_{veh} — затримка бортової обробки, L_{radio} — затримка радіоканалу, L_{edge} — затримка периферійного вузла, $L_{backhaul}$ — затримка транспортної мережі, L_{cloud} — затримка хмари, L_{proc} — затримка прикладної обробки. Для критичних функцій слід виконувати умову:

$$L_{tot} \leq L_{max}^{safety}. \tag{9.6}$$

Якщо ця умова не виконується, функція не повинна залежати від віддаленого сервісу або має перейти в локальний режим.

Табл. 9.4: Ролі хмари, периферійні обчислення і бортових обчислень в ITS

Рівень	**Типові функції**	**Ключові вимоги**
Бортовий рівень	Реальний час, локальне сприйняття, керування	Мінімальна затримка, безпечний відмовний режим, ізоляція
Периферійний рівень	Кооперативне сприйняття, локальна аналітика, кеш карт	Низька затримка, резервування, фізичний захист
Хмара	Навчання моделей, глобальна аналітика, оновлення	Масштабованість, IAM, журналювання, резервне копіювання
Центр керування	Диспетчеризація, політики, реагування	SLA, SIEM, інтеграція з операторами
Користувацький рівень	Мобільні застосунки, оплата, інформування	Приватність, захист API, доступність

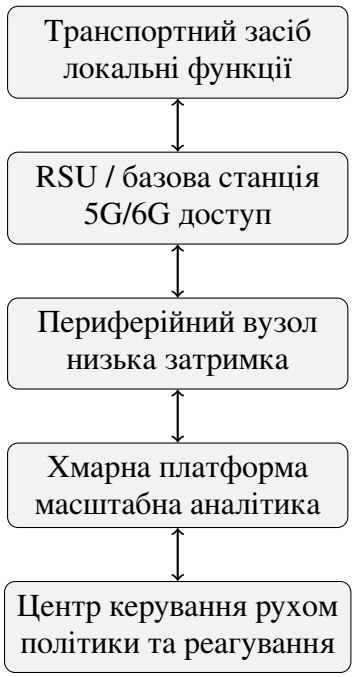

Рис. 9.3: Хмарно-периферійна архітектура ITS із 5G/6G-комунікаціями

Кібербезпека хмарно-периферійної ITS має охоплювати автентифікацію пристроїв, захист API, сегментацію мережі, контроль доступу, журналювання, виявлення аномалій, ізоляцію контейнерів, безпечне розгортання сервісів і керування секретами. Периферійні вузли є особливо чутливими, оскільки вони часто розміщені ближче до дороги, мають фізичні ризики та можуть обслуговувати критичні локальні функції. Компрометація периферійного вузла може вплинути на багато транспортних засобів у певній зоні [11, 12, 55, 56, 57, 81].

Табл. 9.5: Кіберризики 5G/6G та периферійно-хмарних архітектури ITS

Ризик	**Прояв у транспорті**	**Захисний підхід**
Компрометація API	Несанкціоновані команди або витік даних	OAuth/IAM, обмеження частоти запитів, аудит API
Атака на периферійний вузол	Локальне порушення сервісів коридору	нульова довіра, безпечне завантаження, фізичний захист
Збій мережевого зрізу	Втрата якості критичного сервісу	SLA, моніторинг QoS, резервний режим
DDoS на хмару	Недоступність телематики або оновлень	CDN, фільтрація, резервні регіони
Помилка оркестрації	Масове некоректне розгортання сервісу	Канаркове розгортання, відкат, аудит інфраструктури як коду

Надійність розподіленої ITS можна оцінити через доступність багаторівневої архітектури:

$$A_{svc} = 1 - \prod_{k=1}^{m}(1 - A_k), \tag{9.7}$$

де A_k — доступність альтернативного шляху або сервісного рівня. Якщо сервіс може виконуватися локально, на периферії і в хмарі, загальна доступність зростає, але лише за умови незалежності відмов і коректного перемикання. Тому архітектура повинна передбачати не тільки резерви, а й перевірені механізми аварійного перемикання.

Для управління ресурсами периферійно-хмарних у транспортній системі доцільно мінімізувати функцію вартості:

$$J = \lambda_1 L_{tot} + \lambda_2 C_{comp} + \lambda_3 R_{cyb} + \lambda_4 E_{energy} - \lambda_5 Q_{svc}, \tag{9.8}$$

де C_{comp} — вартість обчислювальних ресурсів, R_{cyb} — кіберризик, E_{energy} — енергоспоживання, Q_{svc} — якість транспортного сервісу. Така постановка показує, що найшвидше рішення не завжди є оптимальним, якщо воно створює надмірний ризик або витрати.

Рис. 9.4: Моніторинг кіберстійкості розподіленої периферійно-хмарних ITS

Інтеграція 5G/6G і периферійні обчислення також посилює значення керування даними. Частина даних може оброблятися локально, без передавання в хмару, що зменшує ризики приватності та затримку. Водночас локальна обробка ускладнює аудит, контроль доступу та єдину політику зберігання. Тому майбутні ITS повинні використовувати федеративні архітектури даних, політики мінімізації, псевдонімізацію та механізми контрольованого обміну даними [53, 52, 54, 32, 61].

Додаткові напрями розвитку 5G/6G та периферійної інфраструктури

У перспективі 6G може перетворити дорожню інфраструктуру на сенсорно-комунікаційне середовище, де мережа не лише передає дані, а й допомагає визначати положення об'єктів, оцінювати щільність потоку, прогнозувати ризики та підтримувати кооперативні маневри. Для автомобільного транспорту це означає нову роль оператора зв'язку: він стає учасником забезпечення транспортної безпеки, а не лише постачальником каналу передачі даних [24, 25, 26, 27, 33].

Ключовим питанням буде гарантування якості сервісу. Якщо автономна або кооперативна функція залежить від мережі, необхідно визначити мінімаль-

ні значення затримки, втрат пакетів, доступності, географічного покриття та часу відновлення. Ці показники мають бути зафіксовані в SLA між оператором ITS, оператором зв'язку та власником сервісу. Без формалізованого SLA транспортна система не може довести, що її зовнішні залежності перебувають під контролем.

Табл. 9.6: Показники SLA для 5G/6G-сервісів автомобільної ITS

Показник	**Значення для ITS**	**Механізм контролю**
Затримка	Кооперативні попередження, периферійні рішення	Моніторинг RTT, локальний резервний режим
Доступність	Безперервність сервісів руху	Резервні канали, багатоканальний доступ
Втрати пакетів	Достовірність телеметрії та V2X	QoS-класи, повторна передача для некритичних даних
Покриття	Коридори автономного руху	Карти покриття, геозони ODD
Час відновлення	Реакція після збою мережі	MTTR, аварійні процедури, периферійний кеш

Для вибору місця виконання обчислень можна застосувати правило мінімізації ризик-орієнтованої затримки:

$$X^* = \arg \min_{x \in \{veh, edge, cloud\}} \left(L_x + \kappa R_x + \chi C_x \right), \tag{9.9}$$

де L_x — затримка виконання на рівні x, R_x — кіберризик цього рівня, C_x — вартість або ресурсна складність, κ і χ — вагові коефіцієнти. Для критичних для безпеки функцій вага κ повинна бути високою, щоб система не переносила оброблення в дешевший, але менш захищений контур.

Розподілена архітектура також потребує нової моделі відповідальності. Якщо рішення формується частково автомобілем, частково периферійним вузлом і частково хмарною моделлю, необхідно мати трасування: який компонент надав дані, хто виконав обчислення, яка версія моделі використовувалася, який сертифікат підтвердив джерело та який журнал зберіг результат. Без такого трасування неможливо провести технічне розслідування інциденту або довести відповідність вимогам [1, 3, 11, 12, 54].

Рис. 9.5: Ризик-орієнтований вибір рівня обчислень у ITS

9.3 Використання блокчейну та цифрових сертифікатів

Блокчейн і цифрові сертифікати можуть відігравати важливу роль у майбутніх ITS, але їх не слід розглядати як універсальне рішення для всіх проблем кібербезпеки. Найбільш перспективними є сценарії, де потрібні незмінність записів, розподілена довіра, контроль походження даних, аудит подій, керування цифровими ідентичностями, сертифікатами V2X, історією оновлень і доказами відповідності. У таких сценаріях блокчейн може доповнювати PKI та журнали аудиту, але не замінювати криптографічний захист повідомлень і системне управління ризиками [16, 17, 20, 21, 41, 42].

Цифрові сертифікати вже є фундаментом довіри у V2X-комунікаціях. Повідомлення CAM, DENM або інші кооперативні повідомлення мають бути підписані, щоб отримувач міг перевірити їх походження та цілісність. Водночас постійний сертифікат може створити ризик відстеження транспортного засобу. Тому архітектура довіри повинна поєднувати автентичність і приватність через псевдонімні сертифікати, ротацію ключів, політики відкликання та обмеження доступу до зв'язування ідентичностей [14, 15, 17, 20, 40].

Формально довіру до повідомлення ITS можна подати як інтегральний показник:

$$T_m = \alpha V_{sig} + \beta V_{cert} + \gamma F_{fresh} + \delta C_{ctx} + \eta R_{rep}, \tag{9.10}$$

де V_{sig} — результат перевірки підпису, V_{cert} — чинність сертифіката, F_{fresh} — свіжість повідомлення, C_{ctx} — відповідність контексту дорожньої ситуації, R_{rep} — репутаційний або історичний показник джерела. Така модель показує, що криптографічна перевірка є необхідною, але не завжди достатньою: підписане

Табл. 9.7: Перспективні сценарії блокчейну та цифрових сертифікатів в ITS

Сценарій	**Роль технології**	**Обмеження та умови застосування**
V2X-довіра	Сертифікати, підписи, відкликання	Низька затримка, приватність, масштабованість
Журнал оновлень	Незмінний запис версій ПЗ	Не замінює тестування та відкат
Ланцюг постачання	Походження компонентів і SBOM	Потрібна верифікація первинних даних
Доступ до даних	Смарт-контракти для дозволів	Правова сумісність, відкликання згоди
Аудит інцидентів	Незмінні журнали критичних подій	Захист персональних даних, обмеження зберігання

повідомлення також має бути фізично правдоподібним.

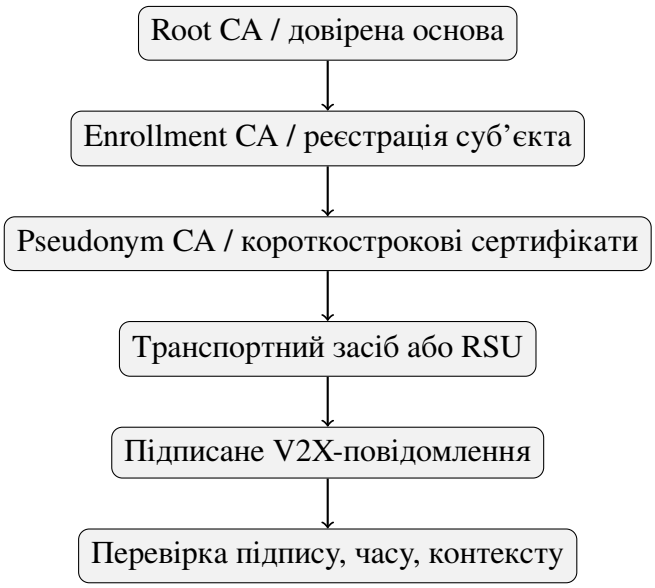

Рис. 9.6: Узагальнена архітектура цифрових сертифікатів для V2X

Блокчейн може бути корисним для незмінного журналу оновлень програмного забезпечення. У такому журналі фіксуються ідентифікатор транспортного засобу або групи, версія пакета, хеш, цифровий підпис, час розгортання, результат перевірки та статус відкату. Це підвищує прозорість SUMS і допомагає розслідувати інциденти. Однак сам блокчейн не гарантує, що оновлення безпечне; він лише фіксує факт і параметри події. Тому його потрібно поєднувати з ISO 24089, UN R156, тестуванням і поетапним розгортанням [3, 10, 50, 51, 49].

Незмінність журналу можна формалізувати через хеш-ланцюг:

$$h_t = H(h_{t-1} \| e_t \| \tau_t), \tag{9.11}$$

де h_t — хеш поточного запису, h_{t-1} — хеш попереднього запису, e_t — подія або метадані оновлення, τ_t — часовий штамп. Якщо будь-який попередній запис змінюється, змінюється весь наступний ланцюг хешів, що полегшує виявлення несанкціонованої модифікації.

Табл. 9.8: Порівняння PKI, централізованого журналу та блокчейн-журналу для ITS

Критерій	**PKI**	**Централізований журнал**	**Блокчейн-журнал**
Автентичність	Висока через сертифікати	Залежить від IAM	Потребує PKI для записів
Незмінність	Не є основною функцією	Залежить від адміністратора	Висока за коректної архітектури
Затримка	Низька для перевірки підпису	Низька	Може бути вищою
Масштабованість	Висока за ієрархії CA	Висока, але централізована	Залежить від консенсусу
Приватність	Потребує псевдонімів	Потребує політик доступу	Потребує обмеження даних у ланцюжку блоків

Важливо не зберігати персональні або деталізовані телематичні дані безпосередньо в блокчейні, якщо це ускладнює реалізацію прав суб'єктів даних, виправлення або видалення. Для ITS доцільніша гібридна модель: у блокчейні зберігаються хеші, докази, ідентифікатори транзакцій і метадані, а самі дані залишаються в контрольованих сховищах із політиками доступу, строками зберігання та аудитом [53, 52, 54, 32].

Для оцінювання доцільності блокчейн-рішення можна використати критерій:

$$B_{use} = \rho_1 N + \rho_2 D + \rho_3 A + \rho_4 M - \rho_5 L - \rho_6 P, \tag{9.12}$$

де N — потреба в незмінності, D — розподіленість довіри, A — потреба в аудиті, M — кількість незалежних учасників, L — допустима затримка, P — ризик приватності. Якщо B_{use} низький, централізований журнал із сильним

контролем доступу може бути кращим за блокчейн.

Рис. 9.7: Гібридна модель блокчейн-аудиту для ITS

У майбутньому цифрові сертифікати, апаратні модулі довіри, HSM, безпечне завантаження, підписані оновлення та журнали доказів мають утворити єдину інфраструктуру довіри. Її завданням буде не лише перевірка повідомлень, а й підтвердження походження програмного забезпечення, компонентів, даних і рішень. Для автомобільного транспорту це особливо важливо через довгий життєвий цикл і велику кількість постачальників [1, 3, 9, 10, 51].

Додаткові моделі довіри, сертифікації та аудиту цифрової ідентичності

Майбутні ITS потребуватимуть не одного, а кількох взаємопов'язаних контурів цифрової ідентичності. Перший контур стосується транспортного засобу як об'єкта, що має сертифікати, ключі, програмні версії та право участі у V2X. Другий контур стосується користувача або водія, який має права доступу до сервісів. Третій контур стосується інфраструктури: RSU, периферійному вузлів, світлофорних контролерів, камер і серверів. Четвертий контур стосується постачальників і сервісних організацій, які отримують тимчасовий доступ для діагностики або оновлення [16, 17, 20, 21, 1].

Довіра до цифрової ідентичності має бути обмеженою в часі та контексті. Сертифікат, який є чинним формально, не повинен автоматично давати доступ до будь-якої функції. Потрібно перевіряти роль суб'єкта, місце, час, стан пристрою, цілісність програмного забезпечення та відповідність запиту політиці. Такий підхід близький до нульової довіри і є особливо важливим для хмарно-периферійних ITS [11, 12, 55, 81].

Табл. 9.9: Контури цифрової ідентичності в перспективній ITS

Контур	**Об'єкти ідентифікації**	**Критичні вимоги**
Транспортний засіб	ECU, телематичний модуль, V2X, OTA-клієнт	Сертифікати, HSM, безпечне завантаження
Користувач	Водій, власник, оператор автопарку	MFA, згода, рольовий доступ
Інфраструктура	RSU, периферійний вузол, світлофор, камера	Захист ключів, фізична безпека, журналювання
Постачальник	Сервіс, діагностика, розробник ПЗ	Тимчасові права, аудит, мінімальні привілеї
Дані	Набори телематики, карти, моделі ШІ	Походження, хеші, політики доступу

Контекстну довіру можна описати показником:

$$T_{ctx} = \nu_1 I_d + \nu_2 S_t + \nu_3 R_l + \nu_4 P_o + \nu_5 H_i, \tag{9.13}$$

де I_d — валідність ідентичності, S_t — стан пристрою, R_l — відповідність ролі, P_o — відповідність політиці доступу, H_i — історія інцидентів або репутація. Доступ до критичних команд має надаватися лише тоді, коли T_{ctx} перевищує заданий поріг.

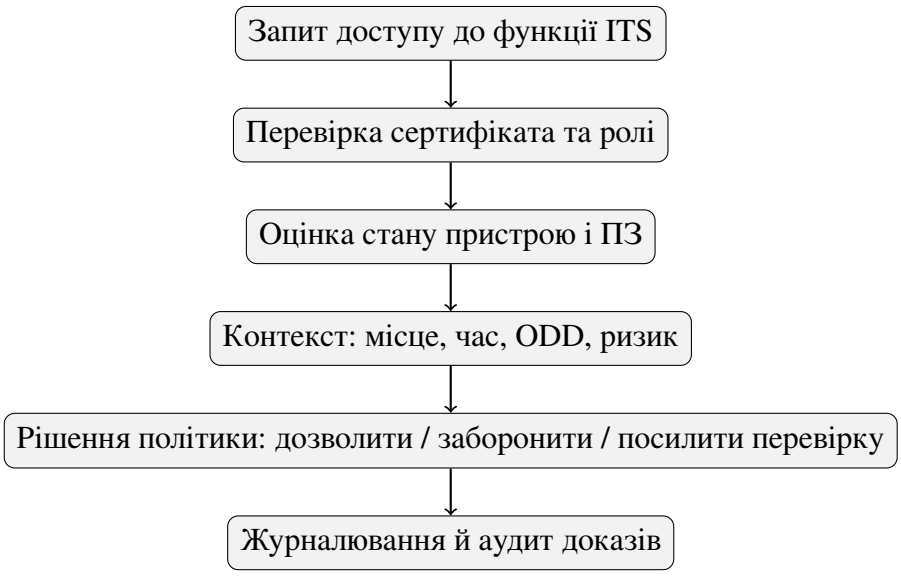

Рис. 9.8: Контекстна перевірка цифрової ідентичності в ITS

Блокчейн-аудит може бути корисним для доказів, але майбутня система повинна підтримувати також відкликання, ротацію, делегування й обмеження прав. Це означає, що незмінність запису має поєднуватися з динамічним

управлінням доступом. У практиці доцільно зберігати в незмінному журналі не персональні дані, а докази: хеш політики, хеш дозволу, ідентифікатор транзакції, час і підпис відповідальної сторони [53, 52, 54, 32].

9.4 Майбутні виклики кібербезпеки в інтелектуальних транспортних системах

Майбутні виклики кібербезпеки в ITS будуть пов'язані не лише зі збільшенням кількості атак, а й зі зміною їх природи. Традиційні атаки на окремий пристрій поступово доповнюються атаками на дані, моделі штучного інтелекту, ланцюги постачання, хмарні середовища, V2X-довіру, оновлення програмного забезпечення та організаційні процеси. У такій ситуації кібербезпека має бути безперервним процесом, а не разовим етапом проєктування [1, 11, 12, 62, 63, 38].

Одним із головних викликів стане масштабованість ризику. Якщо раніше помилка або відмова часто зачіпала один транспортний засіб, то в програмно-визначеному транспорті одна вразливість у спільному компоненті, бібліотеці, OTA-пакеті або хмарному API може вплинути на тисячі автомобілів. Це потребує нових процедур поетапного розгортання, канаркового розгортання, швидкого відкликання, глобального моніторингу та автоматизованого аналізу телеметрії [3, 10, 49, 50, 51].

Табл. 9.10: Майбутні виклики кібербезпеки ITS і стратегічні відповіді

Виклик	**Сутність ризику**	**Стратегічна відповідь**
ШІ-атаки	Змагальні приклади, отруєння даних, дрейф	Валідація даних, виявлення позарозподільних сценаріїв, моніторинг моделей
Ланцюг постачання	Компрометація компонентів або бібліотек	SBOM, аудит постачальників, підпис артефактів
Масові OTA-ризики	Помилка оновлення на великому парку	Поетапне розгортання, відкат, SUMS, телеметрія
V2X-довіра	Підробка або зловживання повідомленнями	PKI, псевдоніми, контекстна перевірка
Хмара й периферія	Компрометація сервісів або API	нульова довіра, SIEM, сегментація, резервування

Ризик майбутньої атаки можна подати як функцію технічної складності

системи, масштабу впливу й готовності захисту:

$$R_{future} = \frac{K_s \cdot M_i \cdot A_p}{C_m \cdot R_o \cdot D_t}, \tag{9.14}$$

де K_s — складність системи, M_i — масштаб потенційного впливу, A_p — привабливість цілі для атакувальника, C_m — зрілість кіберконтролів, R_o — організаційна готовність, D_t — здатність до виявлення та реагування. Формула підкреслює, що навіть складна система може мати прийнятний ризик за умови високої зрілості контролів і швидкого реагування.

Рис. 9.9: Цикл адаптивного управління майбутніми кіберзагрозами ITS

Окремим викликом стане безпека штучного інтелекту. Моделі ШІ використовуються для сприйняття, прогнозування, виявлення аномалій, предиктивного обслуговування та диспетчеризації. Вони можуть деградувати через зміну умов експлуатації, зміщення даних, некоректне навчання або навмисне отруєння наборів даних. Тому майбутні ITS повинні мати процеси MLOps з контролем версій даних, тестами моделей, моніторингом дрейфу, пояснюваністю та процедурами відкликання моделі [44, 47, 48, 56, 80, 81].

Для ШІ-компонента можна визначити індекс довіри:

$$T_{AI} = \mu_1 Q_d + \mu_2 V_m + \mu_3 X_e + \mu_4 M_d + \mu_5 S_c - \mu_6 O_r, \tag{9.15}$$

де Q_d — якість даних, V_m — результати валідації моделі, X_e — пояснюваність, M_d — моніторинг дрейфу, S_c — захищеність середовища навчання й

розгортання, O_r — частка позарозподільних сценаріїв. Якщо T_{AI} падає нижче порогу, модель повинна бути обмежена, перевірена або замінена.

Ланцюг постачання стане ще одним критичним напрямом. Автомобільні системи використовують компоненти багатьох постачальників: мікроконтролери, ОС, проміжне програмне забезпечення, бібліотеки, моделі ШІ, хмарні сервіси, мобільні інструментарії розроблення і інструменти розробки. Компрометація будь-якої ланки може потрапити до кінцевого продукту. Тому потрібні SBOM, підпис артефактів, перевірка залежностей, аудит постачальників і вимоги до розкриття інформації про вразливості [1, 9, 64, 73, 74].

Табл. 9.11: Матриця майбутніх контролів кіберстійкості ITS

Рівень	**Контролі майбутнього**	**Показники ефективності**
Автомобіль	Безпечне завантаження, IDS, сегментація, HSM	Час виявлення, покриття ECU, кількість інцидентів
ШІ/MLOps	Валідація даних, моніторинг дрейфу, відкат моделі	Точність, OOD-рівень, стабільність моделі
V2X	PKI, псевдоніми, контекстна перевірка	Частка відхилених хибних повідомлень
Хмара/периферія	нульова довіра, SIEM, аудит інфраструктури як коду, резервування	SLA, MTTD, MTTR, кількість критичних подій
Організація	CSMS, SUMS, SBOM, навчання, аудит	Зрілість процесів, час закриття вразливостей

Майбутня кібербезпека ITS має бути тісно пов'язана з надійністю. Неможливо вважати транспортний сервіс надійним, якщо він доступний технічно, але вразливий до підміни даних або несанкціонованих команд. Так само неможливо вважати сервіс кібербезпечним, якщо після кожного інциденту він довго відновлюється або не має резервного режиму. Тому перспективною є інтегрована модель кіберстійкості, яка поєднує запобігання, виявлення, реагування, відновлення й навчання [1, 2, 11, 12, 78, 58, 59, 60].

Інтегральний показник кіберстійкості майбутньої ITS можна подати як:

$$CR_{ITS} = \omega_1 P_r + \omega_2 D_e + \omega_3 R_s + \omega_4 R_c + \omega_5 L_n, \tag{9.16}$$

де P_r — здатність запобігати інцидентам, D_e — здатність виявляти, R_s — швидкість реагування, R_c — повнота відновлення, L_n — здатність навчатися

на інцидентах. Саме останній компонент визначає, чи система стає сильнішою після збоїв і атак.

Сценарне планування та підготовка до невідомих загроз

Особливість майбутніх викликів полягає в тому, що частина з них ще не має усталеної класифікації. Нові типи сенсорів, генеративний штучний інтелект, автоматизовані атаки на ланцюги постачання, квантові загрози для криптографії, масове використання цифрових двійників і міжміська інтеграція ITS можуть створити сценарії, які сьогодні важко повністю передбачити. Тому система управління кібербезпекою повинна бути не статичною, а сценарно-адаптивною [12, 11, 1, 64, 82].

Сценарне планування має включати щонайменше чотири групи сценаріїв: технологічні, операційні, організаційні та нормативні. Технологічні сценарії стосуються появи нових вразливостей у 5G/6G, ШІ, V2X або периферійних обчисленнях. Операційні сценарії описують масові відмови, деградацію сервісів, втрату зв'язку або помилки оновлень. Організаційні сценарії охоплюють помилки персоналу, порушення процедур, залежність від постачальника або недостатній аудит. Нормативні сценарії пов'язані зі зміною вимог до даних, сертифікації та міжнародної сумісності.

Табл. 9.12: Сценарне планування майбутніх кіберзагроз ITS

Група сценаріїв	**Приклад**	**Підготовчі заходи**
Технологічні	Атака на модель ШІ або V2X PKI	Перевірки командою атаки, змагальне тестування, оновлення TARA
Операційні	Масовий збій OTA або периферійних вузлів	Відкат, резервування, кризові процедури
Організаційні	Компрометація постачальника	SBOM, аудит, мінімальні привілеї, розкриття інформації про вразливості
Нормативні	Нові вимоги до даних або сертифікації	Аналіз прогалин, оновлення політик, навчання
Соціальні	Втрата довіри користувачів після інциденту	Прозора комунікація, доказова база, компенсаційні дії

Готовність до невідомих загроз можна оцінити через показник адаптив-

ності:

$$A_{cyber} = \sigma_1 I_t + \sigma_2 S_p + \sigma_3 R_t + \sigma_4 F_b + \sigma_5 K_m, \tag{9.17}$$

де I_t — якість розвідки кіберзагроз, S_p — регулярність сценарного планування, R_t — готовність процесів атакувального та захисного тестування, F_b — швидкість зворотного зв'язку після інцидентів, K_m — зрілість знань і навчання персоналу. Високе значення A_{cyber} означає, що організація здатна реагувати навіть на нетипові події.

Рис. 9.10: Цикл сценарної підготовки до майбутніх кіберзагроз ITS

Завершальним елементом є культура безпеки. Навіть найсучасніша архітектура не буде ефективною, якщо організація не має дисципліни оновлень, прозорого повідомлення про вразливості, регулярного навчання, управління доступами та практики аналізу інцидентів. У майбутніх ITS людський фактор не зникає, а змінює форму: оператори, інженери, аналітики, аудитори та постачальники стають частиною кіберфізичного контуру безпеки [1, 9, 11, 12].

Систематизація джерельної бази перспективного розвитку ITS

Для виконання вимоги щодо репрезентативного використання літератури джерельну базу монографії доцільно розглядати як міждисциплінарну систему. Вона охоплює стандарти кібербезпеки, функціональної безпеки, архітектури ITS, V2X-комунікацій, захисту даних, автономного руху, машинного навчання, сенсорного злиття, хмарно-периферійних сервісів, блокчейн-рішень, транспортного моделювання та прикладної організації перевезень. Такий під-

хід важливий тому, що майбутня кіберстійкість автомобільного транспорту не може бути обґрунтована лише однією групою праць: вона формується на перетині технічних, нормативних, інформаційних, експлуатаційних і поведінкових досліджень.

У межах тематичного напряму «нормативно-стандартизаційний контур» використано такі джерела, що формують теоретичну, методичну та прикладну основу відповідних висновків: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36].

У межах тематичного напряму «кібербезпека, V2X та захист автомобільних мереж» використано такі джерела, що формують теоретичну, методичну та прикладну основу відповідних висновків: [37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78].

У межах тематичного напряму «автономність, штучний інтелект, сенсорика та валідація» використано такі джерела, що формують теоретичну, методичну та прикладну основу відповідних висновків: [79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114].

У межах тематичного напряму «хмарні, периферійні, блокчейн- та телематичні сервіси» використано такі джерела, що формують теоретичну, методичну та прикладну основу відповідних висновків: [115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150].

У межах тематичного напряму «транспортне моделювання, пасажирські потоки та системна ефективність» використано такі джерела, що формують теоретичну, методичну та прикладну основу відповідних висновків: [151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190].

Розподіл посилань за тематичними напрямами також зменшує ризик формального цитування, оскільки кожна група джерел пов'язана з конкретним аспектом розвитку ITS: нормативною відповідністю, кіберзахистом, автономністю, цифровою інфраструктурою або транспортною ефективністю. У тексті посилання подано групами не більше ніж по три джерела поспіль, що

забезпечує читабельність і відповідає вимозі щодо структури цитування.

9.5 Висновки до розділу

Перспективи розвитку кібербезпечного та надійного автомобільного транспорту пов'язані з переходом до автономних функцій, розподілених 5G/6G та периферійно-хмарних архітектур, цифрових сертифікатів, блокчейн-аудиту й адаптивного управління кіберзагрозами. Ці напрями створюють значні можливості для підвищення безпеки, ефективності й доступності мобільності, але одночасно збільшують залежність транспорту від програмного забезпечення, даних, комунікацій і постачальників.

Розвиток автономних транспортних засобів потребує поєднання ISO 26262, ISO 21448, ISO/SAE 21434, сценарної валідації, моніторингу моделей ШІ і безпечного оновлення. Інтеграція 5G/6G, хмари та периферійних обчислень має забезпечувати низьку затримку, високу доступність, контроль доступу, захист API та можливість локальної деградації сервісів. Блокчейн і цифрові сертифікати перспективні для довіри, аудиту й походження даних, але повинні застосовуватися вибірково, з урахуванням приватності та затримок.

Отже, майбутня ITS повинна будуватися як адаптивна кіберстійка екосистема. Її розвиток має спиратися на інтеграцію функціональної безпеки, кібербезпеки, експлуатаційної надійності, захисту даних, стандартизації та постійного вдосконалення. Лише такий підхід дозволить масштабувати автономну й підключену мобільність без втрати довіри, керованості та безпеки дорожнього руху [1, 2, 3, 4, 5, 6, 28, 29].

Бібліографія

[1] ISO/SAE 21434:2021. Road vehicles — Cybersecurity engineering. Geneva: International Organization for Standardization, 2021.

[2] ISO 26262:2018. Road vehicles — Functional safety. Parts 1–12. Geneva: International Organization for Standardization, 2018.

[3] ISO 24089:2023. Road vehicles — Software update engineering. Geneva: International Organization for Standardization, 2023.

[4] ISO 21448:2022. Road vehicles — Safety of the intended functionality. Geneva: International Organization for Standardization, 2022.

[5] ISO 14813-1:2024. Intelligent transport systems — Reference model architecture(s) for the ITS sector — Part 1. Geneva: International Organization for Standardization, 2024.

[6] ISO 21217:2024. Intelligent transport systems — Station and communication architecture. Geneva: International Organization for Standardization, 2024.

[7] ISO/TR 21186-1:2021. Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards — Part 1. Geneva: ISO, 2021.

[8] ISO/TR 21186-2:2021. Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards — Part 2: Hybrid communications. Geneva: ISO, 2021.

[9] UN Regulation No. 155. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Geneva: UNECE, 2021.

[10] UN Regulation No. 156. Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system. Geneva: UNECE, 2021.

[11] NIST. The рамка кібербезпеки NIST 2.0. Gaithersburg: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.

[12] ENISA. Good Practices for Security of Smart Cars. Heraklion: European Union Agency for Cybersecurity, 2019.

[13] ETSI EN 302 665 V1.1.1. Intelligent Transport Systems (ITS); Communications Architecture. Sophia Antipolis: ETSI, 2020.

[14] ETSI EN 302 637-2 V1.4.1. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. Sophia Antipolis: ETSI, 2019.

[15] ETSI EN 302 637-3 V1.3.1. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service. Sophia Antipolis: ETSI, 2019.

[16] ETSI TS 102 940 V2.1.1. Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. Sophia Antipolis: ETSI, 2021.

[17] ETSI TS 103 097 V2.1.1. Intelligent Transport Systems (ITS); Security; Security header and certificate formats. Sophia Antipolis: ETSI, 2021.

[18] ETSI TS 103 696 V2.1.1. Intelligent Transport Systems (ITS); Communication Architecture for Multi-Channel Operation (MCO); Release 2. Sophia Antipolis: ETSI, 2021.

[19] ETSI TR 103 439 V2.1.1. Intelligent Transport Systems (ITS); Multi-Channel Operation study; Release 2. Sophia Antipolis: ETSI, 2021.

[20] IEEE Std 1609.2-2016. IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages. New York: IEEE, 2016.

[21] IEEE Std 1609.2.1-2020. IEEE Standard for Wireless Access in Vehicular Environments — Certificate Management Interfaces for End Entities. New York: IEEE, 2020.

[22] IEEE Std 1609.3-2020. IEEE Standard for Wireless Access in Vehicular Environments — Networking Services. New York: IEEE, 2020.

[23] IEEE Std 802.11-2020. IEEE Standard for Information Technology — Telecommunications and information exchange between systems. New York: IEEE, 2021.

[24] 3GPP TR 21.914 V14.0.0. Release 14 Description; Summary of Rel-14 Work Items. Sophia Antipolis: 3GPP, 2017.

[25] 3GPP TR 21.915 V15.0.0. Release 15 Description; Summary of Rel-15 Work Items. Sophia Antipolis: 3GPP, 2019.

[26] 3GPP TS 23.285 V16.7.0. Architecture enhancements for V2X services. Sophia Antipolis: 3GPP, 2020.

[27] 3GPP TS 22.186 V17.0.0. Enhancement of 3GPP support for V2X scenarios. Sophia Antipolis: 3GPP, 2022.

[28] European Parliament and Council. Директива (ЄС) 2023/2661 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in road transport. Brussels: Official Journal of the European Union, 2023.

[29] European Commission. Sustainable and Smart Mobility Strategy — putting European transport on track for the future. Brussels: European Commission, 2020.

[30] U.S. Department of Transportation. Intelligent Transportation Systems Joint Program Office Strategic Plan 2020–2025. Washington: U.S. Department of Transportation, 2020.

[31] Guerrero-Ibáñez J., Zeadally S., Contreras-Castillo J. Sensor technologies for intelligent transportation systems. Sensors. 2018. Vol. 18, No. 4. Article 1212.

[32] Zhang J., Wang F.-Y., Wang K., Lin W.-H., Xu X., Chen C. Data-driven intelligent transportation systems: A survey. IEEE Transactions on Intelligent Transportation Systems. 2018. Vol. 12, No. 4. P. 1624–1639.

[33] Wang J., Shao Y., Ge Y., Yu R. A survey of vehicle to everything (V2X) testing. Sensors. 2019. Vol. 19, No. 2. Article 334.

[34] Zheng Y., Capra L., Wolfson O., Yang H. Urban computing: concepts, methodologies, and applications. ACM Transactions on Intelligent Systems and Technology. 2016. Vol. 5, No. 3. Article 38.

[35] Lv Y., Duan Y., Kang W., Li Z., Wang F.-Y. Traffic flow prediction with big data: a deep learning approach. IEEE Transactions on Intelligent Transportation Systems. 2016. Vol. 16, No. 2. P. 865–873.

[36] Liu Y., Wang Y., Yang X., Zhang L. Short-term travel time prediction by deep learning: a comparison of different LSTM-DNN models. IEEE Transactions on Intelligent Transportation Systems. 2017. Vol. 18, No. 12. P. 3224–3233.

[37] Lamssaggad A., Benamar N., Hafid A. S., Msahli M. A survey on the current security landscape of intelligent transportation systems. IEEE Access. 2021. Vol. 9. P. 9180–9208.

[38] Dibaei M., Zheng X., Jiang K., Abbas R., Liu S., Zhang Y., Xiang Y., Yu S. Attacks and defences on intelligent connected vehicles: a survey. Digital Communications and Networks. 2020. Vol. 6, No. 4. P. 399–421.

[39] Kamel J., Kaiser A., Shami A. A survey on security attacks and defense techniques for connected and autonomous vehicles. Computers & Security. 2021. Vol. 109. Article 102269.

[40] Ghosal A., Conti M. Security issues and challenges in V2X: a survey. Computer Networks. 2020. Vol. 169. Article 107093.

[41] Lu Z., Qu G., Liu Z. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Transactions on Intelligent Transportation Systems. 2019. Vol. 20, No. 2. P. 760–776.

[42] Tangade S., Manvi S. S., Lorenz P. Trust management scheme based on hybrid cryptography for secure communications in VANETs. IEEE Transactions on Vehicular Technology. 2020. Vol. 69, No. 5. P. 5232–5243.

[43] Yurtsever E., Lambert J., Carballo A., Takeda K. A survey of autonomous driving: common practices and emerging technologies. IEEE Access. 2020. Vol. 8. P. 58443–58469.

[44] Ma Y., Wang Z., Yang H., Yang L. Artificial intelligence applications in the development of autonomous vehicles: a survey. IEEE/CAA Journal of Automatica Sinica. 2020. Vol. 7, No. 2. P. 315–329.

[45] Yeong D. J., Velasco-Hernandez G., Barry J., Walsh J. Sensor and sensor fusion technology in autonomous vehicles: a review. Sensors. 2021. Vol. 21, No. 6. Article 2140.

[46] Fayyad J., Jaradat M. A., Gruyer D., Najjaran H. Deep learning sensor fusion for autonomous vehicle perception and localization: a review. Sensors. 2020. Vol. 20, No. 15. Article 4220.

[47] Kuutti S., Bowden R., Jin Y., Barber P., Fallah S. A survey of deep learning applications to autonomous vehicle control. IEEE Transactions on Intelligent Transportation Systems. 2021. Vol. 22, No. 2. P. 712–733.

[48] Grigorescu S., Trasnea B., Cocias T., Macesanu G. A survey of deep learning techniques for autonomous driving. Journal of Field Robotics. 2020. Vol. 37, No. 3. P. 362–386.

[49] Rumez M., Grimm D., Kriesten R., Sax E. An overview of automotive service-oriented architectures and implications for security. SAE International Journal of Transportation Cybersecurity and Privacy. 2020. Vol. 3, No. 1. P. 1–16.

[50] AUTOSAR. Specification of Secure Onboard Communication. AUTOSAR Classic Platform R20-11. Munich: AUTOSAR, 2020.

[51] AUTOSAR. Specification of Crypto Service Manager. AUTOSAR Classic Platform R20-11. Munich: AUTOSAR, 2020.

[52] European Data Protection Board. Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Brussels: EDPB, 2021.

[53] European Parliament and Council. Regulation (EU) 2016/679 — General Data Protection Regulation. Brussels: Official Journal of the European Union, 2016.

[54] European Parliament and Council. Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data — Акт про дані. Brussels: Official Journal of the European Union, 2023.

[55] Loukas G., Vuong T., Heartfield R., Sakellari G., Yoon Y., Gan D. Cloud-based cyber-physical intrusion detection for vehicles using deep learning. IEEE Access. 2018. Vol. 6. P. 3491–3508.

[56] Rajapaksha S., Kalutarage H., Al-Kadri M. O. A survey of deep learning-based intrusion detection in automotive applications. Expert Systems with Applications. 2023. Vol. 233. Article 120972.

[57] Hanselmann M., Strauss T., Dormann K., Ulmer H. CANet: an unsupervised intrusion detection system for high dimensional CAN bus data. IEEE Access. 2020. Vol. 8. P. 58194–58205.

[58] Carvalho T. P. et al. A systematic literature review of machine learning methods applied to predictive maintenance. Computers & Industrial Engineering. 2019. Vol. 137. Article 106024.

[59] Zonta T. et al. Predictive maintenance in the Industry 4.0: a systematic literature review. Computers & Industrial Engineering. 2020. Vol. 150. Article 106889.

[60] Arena F., Collotta M., Luca L., Ruggieri M., Termine F. G. Predictive maintenance in the automotive sector: a literature review. Mathematics. 2022. Vol. 10, No. 15. Article 2603.

[61] Talebkhah M., Sali A., Marjani M., Gordan M., Hashim S. J., Rokhani F. Z. IoT and big data applications in smart cities: recent advances, challenges, and critical issues. IEEE Access. 2021. Vol. 9. P. 55465–55484.

[62] Parkinson S., Ward P., Wilson K., Miller J. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Transactions on Intelligent Transportation Systems. 2017. Vol. 18, No. 11. P. 2898–2915.

[63] Khan S. K., Shiwakoti N., Stasinopoulos P., Chen Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accident Analysis & Prevention. 2020. Vol. 148. Article 105837.

[64] Macher G., Armengaud E., Brenner E., Kreiner C. Threat and risk assessment methodologies in the automotive domain. Procedia Computer Science. 2016. Vol. 83. P. 1288–1294.

[65] Young C., Zambreno J., Olufowobi H., Bloom G. Survey of automotive Controller Area Network intrusion detection systems. IEEE Design & Test. 2019. Vol. 36, No. 6. P. 48–55.

[66] Lokman S.-F., Othman A. T., Abu-Bakar M.-H. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP Journal on Wireless Communications and Networking. 2019. Article 184.

[67] Al-Jarrah O. Y., Maple C., Dianati M., Oxtoby D., Mouzakitis A. Intrusion detection systems for intra-vehicle networks: a review. IEEE Access. 2019. Vol. 7. P. 21266–21289.

[68] Miller C., Valasek C. The Evolution of Automotive Cybersecurity: From Research to Practice. Black Hat USA Briefings. 2017.

[69] Dupont G., Lekidis A., den Hartog J., Etalle S. Automotive Controller Area Network security: an overview of current challenges. IEEE Communications Surveys & Tutorials. 2019. Vol. 21, No. 4. P. 3548–3574.

[70] Petit J., Shladover S. E. Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems. 2015. Vol. 16, No. 2. P. 546–556.

[71] Salay R., Queiroz R., Czarnecki K. An analysis of ISO 26262: using machine learning safely in automotive software. SAE Technical Paper. 2017. No. 2017-01-1665.

[72] Rosique F., Navarro P. J., Fernández C., Padilla A. A systematic review of perception system and simulators for autonomous vehicles research. Sensors. 2019. Vol. 19, No. 3. Article 648.

[73] Macher G., Sporer H., Berlach R., Armengaud E., Kreiner C. SAHARA: a security-aware hazard and risk analysis method. Design, Automation & Test in Europe Conference & Exhibition. 2016. P. 621–624.

[74] Schmittner C., Ma Z., Reyes C., Dillinger O., Puschner P. Using SAE J3061 for automotive security requirement engineering. Computer Safety, Reliability, and Security. Cham: Springer, 2016. P. 157–170.

[75] Koopman P., Wagner M. Challenges in autonomous vehicle testing and validation. SAE International Journal of Transportation Safety. 2016. Vol. 4, No. 1. P. 15–24.

[76] Koopman P., Wagner M. Autonomous vehicle safety: an interdisciplinary challenge. IEEE Intelligent Transportation Systems Magazine. 2017. Vol. 9, No. 1. P. 90–96.

[77] Huang W., Wang K., Lv Y., Zhu F. Autonomous vehicles testing methods review. IEEE Intelligent Transportation Systems Magazine. 2016. Vol. 8, No. 2. P. 72–85.

[78] Abbasi A., Sargolzaei A., Yen K. K., Abdelghani M. N., Sargolzaei S. A survey on active fault-tolerant control systems. Electronics. 2020. Vol. 9, No. 9. Article 1513.

[79] Tariq M. U., Floriano A., González L. C. A survey on sensor failures in autonomous vehicles: challenges and solutions. Sensors. 2024. Vol. 24, No. 16. Article 5108.

[80] Jiang Y., Zhang H., Wang H., Li L., Li K. Anomaly diagnosis of connected autonomous vehicles: a survey. Information Fusion. 2024. Vol. 106. Article 102223.

[81] Sarker I. H., Furhad M. H., Nowrozy R. AI-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science. 2021. Vol. 2. Article 173.

[82] Hegde J., Rokseth B. Applications of machine learning methods for engineering risk assessment: a review. Safety Science. 2020. Vol. 122. Article 104492.

[83] Avcı, I., & Koca, M. (2024). Intelligent transportation system technologies, challenges and security. *Applied Sciences, 14*(11), 4646. https://doi.org/10.3390/app14114646.

[84] Wang, F., Wang, X., & Ban, X. J. (2024). Data poisoning attacks in intelligent transportation systems: A survey. *Transportation Research Part C: Emerging Technologies, 165*, 104750. https://doi.org/10.1016/j.trc.2024.104750.

[85] Sedar, R. M. M., Kalalas, C., Vázquez-Gallego, F., Alonso-Zarate, J., & Alonso-Zarate, L. (2023). A comprehensive survey of V2X cybersecurity mechanisms and future research paths. *IEEE Open Journal of the Communications Society, 4*, 325–391. https://doi.org/10.1109/OJCOMS.2023.3239115.

[86] Bhosale, A., & Roychowdhury, S. (2024). A survey of cybersecurity challenges and mitigation techniques for connected and autonomous vehicles. *IEEE Transactions on Intelligent Vehicles*. https://doi.org/10.1109/TIV.2024.3493938.

[87] Kour, R., Patwardhan, A., Thaduri, A., & Karim, R. (2023). A review on cybersecurity in railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*. https://doi.org/10.1177/09544097221089389.

[88] Karthikeyan, H., & Usha, G. (2022). Real-time DDoS flooding attack detection in intelligent transportation systems. *Computers and Electrical Engineering, 101*, 107995. https://doi.org/10.1016/j.compeleceng.2022.107995.

[89] Magsi, A. H., Mohsan, S. A. H., Muhammad, G., & Abbasi, S. (2023). A machine learning-based interest flooding attack detection system in vehicular named data networking. *Electronics, 12*(18), 3870. https://doi.org/10.3390/electronics12183870.

[90] Maity, S. (2022). Beacon non-transmission attack and its detection in intelligent transportation systems. *Internet of Things, 20*, 100602. https://doi.org/10.1016/j.iot.2022.100602.

[91] Nguyen-Minh, T., Tran, N. H., & Nguyen, T. (2023). Machine learning-based придушення каналу detection for safety applications in vehicular networks. *Security and Communication Networks, 2023*, 8080669. https://doi.org/10.1155/2023/8080669.

[92] Al-Mekhlafi, Z. G., & Mohammed, B. A. (2021). A survey on security schemes based on conditional privacy-preserving in vehicular ad hoc networks. *International Journal of Computer Science and Network Security, 21*(11), 96–104. https://doi.org/10.22937/IJCSNS.2021.21.11.14.

[93] Javed, M. A., Zeadally, S., & Hamida, E. B. (2019). Data analytics for cooperative intelligent transport systems. *Vehicular Communications, 15*, 63–72. https://doi.org/10.1016/j.vehcom.2018.10.004.

[94] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. K. M. N., & Shorfuzzaman, M. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems, 23*(7), 7667–7679.

[95] Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things. *IEEE Internet of Things Journal, 9*(11), 8229–8249. https://doi.org/10.1109/JIOT.2022.3150363.

[96] Ali, I., Lawrence, T., Omala, A. A., & Li, F. (2020). An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs. *IEEE Transactions on Vehicular Technology, 69*(10), 11266–11280. https://doi.org/10.1109/TVT.2020.3008781.

[97] Baza, M., Mahmoud, M., Abdallah, M., & Lin, X. (2021). Blockchain-based distributed key management approach tailored for smart grid and vehicular communication systems. *IEEE Transactions on Vehicular Technology, 70*(6), 5697–5711.

[98] Alladi, T., Chamola, V., Rodrigues, J. J. P. C., & Kozlov, S. A. (2021). Blockchain in smart grids: A review on different use cases. *Sensors, 21*(14), 4862. https://doi.org/10.3390/s21144862.

[99] Ghori, M. R., Wan, T.-C., Sodhy, G. C., & Rizvi, S. S. H. (2021). Blockchain-enabled vehicular ad hoc networks: A systematic literature review. *Sustainability, 14*(7), 3919. https://doi.org/10.3390/su14073919.

[100] Grover, J. (2022). Security of vehicular ad hoc networks using blockchain: A comprehensive review. *Vehicular Communications, 34*, 100458. https://doi.org/10.1016/j.vehcom.2022.100458.

[101] Fayi, S. Y., & Sheng, Z. (2023). A survey of security, privacy and trust issues in vehicular computation offloading and their solutions using blockchain. *Open Research Europe, 3*, 110. https://doi.org/10.12688/openreseurope.16189.2.

[102] Mollah, M. B., Zhao, J., Niyato, D., Guan, Y. L., Yuen, C., Sun, S., Lam, K.-Y., & Koh, L. H. (2021). Blockchain for the Internet of Vehicles (IoV) towards intelligent transportation systems: A survey. *IEEE Internet of Things Journal, 8*(6), 4157–4185. https://doi.org/10.1109/JIOT.2020.3028368.

[103] Khoshavi, N., Tristani, G., & Sargolzaei, A. (2021). Blockchain applications to improve operation and security of transportation systems: A survey. *Electronics, 10*(5), 629. https://doi.org/10.3390/electronics10050629.

[104] Yang, W., Wang, S., Li, X., & Zhang, J. (2023). Flow-based intrusion detection system in vehicular ad hoc network using context-aware feature extraction. *Vehicular Communications, 41*, 100585. https://doi.org/10.1016/j.vehcom.2023.100585.

[105] Sharma, P., Moon, S. Y., & Park, J. H. (2023). A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. *Digital Communications and Networks, 9*(5), 1113–1122. https://doi.org/10.1016/j.dcan.2022.06.018.

[106] Rajendran, S., & Sethukarasi, T. (2023). An authentication approach in SDN-VANET architecture with optimized neural network for intrusion detection. *Internet of Things, 22*, 100723. https://doi.org/10.1016/j.iot.2023.100723.

[107] Alshammari, B., & Alshammari, R. (2023). Vehicular network intrusion detection using a cascaded deep learning approach with multi-variant metaheuristic. *Sensors, 23*(21), 8772. https://doi.org/10.3390/s23218772.

[108] Ahmad, I., Shah, S. A., & Kumar, N. (2025). DDoS attack detection in intelligent transport systems using adaptive neuro-fuzzy inference system. *Scientific Reports, 15*, Article 06719. https://doi.org/10.1038/s41598-025-06719-x.

[109] Nayak, N. M., & Cholli, N. G. (2024). Cybersecurity challenges and risks in connected autonomous vehicles: A literature review. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4917100.

[110] Hasan, M. M., Bhattacharya, M., & Islam, R. (2026). Cyber threats in connected autonomous vehicles: A protocol-grounded survey. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.6902580.

[111] Silva, A., Cardoso, J., & Ribeiro, B. (2024). Cyber resilience and intelligent transport systems: A scoping review. *Procedia Computer Science, 239*, 139–148. https://doi.org/10.1016/j.procs.2024.06.156.

[112] Zhang, Y., Wang, X., & Liu, H. (2026). Assessing cybersecurity risks and traffic impact in connected autonomous vehicles. *arXiv preprint arXiv:2602.13898*.

[113] Liu, Z., Li, Y., & Chen, J. (2026). Post-quantum cryptography for intelligent transportation systems: An implementation-focused review. *arXiv preprint arXiv:2601.01068*.

[114] Gallagher, S. (2016). Muni system hacker hit others by scanning for year-old Java vulnerability. *Ars Technica*. https://arstechnica.com/information-technology/2016/11/san-francisco-transit-ransomware-attacker-likely-used-year-old-java-exploit/.

[115] Kaspersky. (2016). Mamba ransomware infects San Francisco Municipal Railway. *Kaspersky Official Blog*. https://www.kaspersky.com/blog/mamba-hddcryptor-ransomware/13539/.

[116] NY1. (2021). MTA computer systems hack. *NY1*. https://ny1.com/nyc/all-boroughs/transit/2021/06/02/mta-computer-systems-hack.

[117] Axios. (2021). Hackers breached New York's transit agency systems in April. *Axios*. https://www.axios.com/2021/06/02/new-york-mta-hackers-breach.

[118] Altawy, R., & Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems, 1*(2), 1–25. https://doi.org/10.1145/3001836

[119] Shafique, A., Mehmood, A., & Elhadef, M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. *IEEE Access, 9*, 46927–46948. https://doi.org/10.1109/ACCESS.2021.3066778

[120] Kong, P.-Y. (2021). A survey of cyberattack countermeasures for unmanned aerial vehicles. *IEEE Access, 9*, 148244–148263. https://doi.org/10.1109/ACCESS.2021.3124996

[121] Alharbi, Y., & Alghazzawi, D. (2021). A survey of cybersecurity attacks, detection techniques, and mitigation strategies in unmanned aerial vehicles. *Journal of Information Security and Applications, 58*, 102784. https://doi.org/10.1016/j.jisa.2021.102784

[122] Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things, 11*, 100218. https://doi.org/10.1016/j.iot.2020.100218

[123] Pandey, G. K., Gurjar, D., Nguyen, H. H., & Yadav, S. (2022). Security threats and mitigation techniques in UAV communications: A comprehensive survey. *IEEE Access, 10*, 112858–112897. https://doi.org/10.1109/ACCESS.2022.3215975

[124] Zhang, J., Li, X., Luo, Y., & Chen, J. (2022). Cybersecurity for autonomous unmanned aerial vehicles: Threats, vulnerabilities, and countermeasures. *IEEE Internet of Things Journal, 9*(24), 24839–24859. https://doi.org/10.1109/JIOT.2022.3195748

[125] Gurtov, A., Polishchuk, T., & Wernberg, M. (2018). Controller–pilot data link communication security. *Sensors, 18*(5), 1636. https://doi.org/10.3390/s18051636

[126] Leonardi, M., Piracci, E. G., & Galati, G. (2019). ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions. *IEEE Aerospace*

and Electronic Systems Magazine, 34(11), 24–35. https://doi.org/10.1109/MAES.2019.2927895

[127] Sciancalepore, S., Ibrahim, O. A., Oligeri, G., & Di Pietro, R. (2019). Detecting ADS-B spoofing attacks using deep neural networks. *IEEE Conference on Communications and Network Security*, 187–195. https://doi.org/10.1109/CNS.2019.8802831

[128] Yang, A., Tan, X., Baek, J., & Wong, D. S. (2019). A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification. *IEEE Transactions on Services Computing, 12*(2), 165–175. https://doi.org/10.1109/TSC.2016.2540632

[129] Wesson, K. D., Humphreys, T. E., & Evans, B. L. (2019). Can cryptography secure next generation air traffic surveillance? *IEEE Security & Privacy, 17*(3), 50–59. https://doi.org/10.1109/MSEC.2019.2899395

[130] Moser, D., Lenders, V., & Martinovic, I. (2019). Intrusion detection for air traffic communication networks. *IEEE Transactions on Dependable and Secure Computing, 16*(5), 812–825. https://doi.org/10.1109/TDSC.2017.2723891

[131] Jansen, K., Schäfer, M., Moser, D., Lenders, V., Schmitt, J. B., & Martinovic, I. (2019). Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS підміни attacks. *IEEE Symposium on Security and Privacy*, 1018–1031. https://doi.org/10.1109/SP.2018.00075

[132] Alzubaidi, A. A. (2025). Systematic literature review for detecting intrusions in unmanned aerial vehicles using machine and deep learning. *IEEE Access, 13*, 58576–58599. https://doi.org/10.1109/ACCESS.2025.3559142

[133] Ogab, M., Zaidi, S., Bourouis, A., & Calafate, C. T. (2025). Machine learning-based intrusion detection systems for the Internet of Drones: A systematic literature review. *IEEE Access, 13*, 96681–96714. https://doi.org/10.1109/ACCESS.2025.3575378

[134] Casals, L., Devlin, K., & Wills, G. B. (2019). Cyber security for aviation:

A systematic literature review. *Journal of Air Transport Management, 79*, 101673. https://doi.org/10.1016/j.jairtraman.2019.101673

[135] Fotouhi, A., Qiang, H., Ding, M., Hassan, M., Giordano, L. G., Garcia-Rodriguez, A., & Yuan, J. (2019). Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials, 21*(4), 3417–3442. https://doi.org/10.1109/COMST.2019.2906228

[136] Alshbatat, A. I., & Dong, L. (2020). Cross layer design for mobile ad-hoc unmanned aerial vehicle communication networks. *International Journal of Computer Networks & Communications, 12*(2), 1–19. https://doi.org/10.5121/ijcnc.2020.12201

[137] Li, B., Fei, Z., & Zhang, Y. (2022). UAV communications for 5G and beyond: Recent advances and future trends. *IEEE Internet of Things Journal, 6*(2), 2241–2263. https://doi.org/10.1109/JIOT.2018.2887086

[138] Bera, B., Saha, S., Das, A. K., Kumar, N., & Rodrigues, J. J. P. C. (2022). Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled Internet of Drones environment. *IEEE Transactions on Vehicular Technology, 71*(3), 3264–3278. https://doi.org/10.1109/TVT.2022.3140458

[139] Sharma, V., Kumar, R., & Kim, J. (2024). A comprehensive survey on UAV communication networks: Security, privacy, and future research directions. *Computer Networks, 241*, 110202. https://doi.org/10.1016/j.comnet.2024.110202

[140] Khan, M. A., Menouar, H., Eldeeb, A., Abu-Dayya, A., & Salim, F. D. (2020). On the detection of unauthorized drones: Techniques and future perspectives. *IEEE Access, 8*, 110352–110370. https://doi.org/10.1109/ACCESS.2020.3001141

[141] Lykou, G., Moustakas, D., & Gritzalis, D. (2022). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors, 22*(10), 3537. https://doi.org/10.3390/s22103537

[142] Akram, R. N., Markantonakis, K., Mayes, K., Habachi, O., Sauveron, D., Steyven, A., & Chaumette, S. (2022). Security, privacy and safety evaluation of dynamic and static fleets of drones. *Ad Hoc Networks, 132*, 102868. https://doi.org/10.1016/j.adhoc.2022.102868

[143] Tomic, I., McCann, J. A., & Potdar, V. (2021). A survey of security threats and defensive techniques for wireless sensor networks in cyber-physical systems. *IEEE Communications Surveys & Tutorials, 23*(1), 157–191. https://doi.org/10.1109/COMST.2020.3029842

[144] Wang, H., Wang, J., Ding, G., Chen, J., & Li, Y. (2022). A survey on security and privacy of federated learning for UAV networks. *IEEE Network, 36*(6), 64–70. https://doi.org/10.1109/MNET.001.2100634

[145] Kacem, T., & Benjamin, K. (2026). Artificial intelligence methods for unmanned aerial vehicles cybersecurity: A comprehensive survey. *Drones, 10*(6), 400. https://doi.org/10.3390/drones10060400

[146] Yan, M., Dong, R., Han, Q.-L., Deng, Z., Ma, W., Zhu, X., Zhou, W., Wen, S., & Xiang, Y. (2026). Securing the low-altitude economy: A survey. *Science China Information Sciences, 69*, 141202. https://doi.org/10.1007/s11432-025-4811-2

[147] Hartmann, K., & Steup, C. (2023). The vulnerability of UAVs to cyber attacks: An approach to the risk assessment. *Cybersecurity, 6*, 3. https://doi.org/10.1186/s42400-023-00136-7

[148] Liu, Y., Wang, L., & Chen, X. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture, 138*, 102870. https://doi.org/10.1016/j.sysarc.2023.102870

[149] Chen, J., Zhang, Y., Wu, L., You, T., & Ning, X. (2023). An adaptive clustering-based algorithm for automatic path planning of heterogeneous UAVs. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 1682–1693. https://doi.org/10.1109/TITS.2022.3215073

[150] Mersha, A., De Croon, G. C. H. E., & Stramigioli, S. (2023). A survey on sensor- and communication-based issues of autonomous UAVs. *Computer*

Modeling in Engineering & Sciences, 138(2), 1019–1050. https://doi.org/10.32604/cmes.2023.029075

[151] Zhao, N., Lu, W., Sheng, M., Chen, Y., Tang, J., Yu, F. R., & Wong, K.-K. (2023). UAV-assisted emergency networks in disasters. *IEEE Wireless Communications, 30*(3), 64–71. https://doi.org/10.1109/MWC.001.2200330

[152] Meyer, M. D., & Miller, E. J. (2001). *Urban transportation planning: A decision-oriented approach* (2nd ed.). McGraw-Hill.

[153] Ortúzar, J. de D., & Willumsen, L. G. (2011). *Modelling transport* (4th ed.). Wiley.

[154] Vuchic, V. R. (2005). *Urban transit: Operations, planning, and economics*. Wiley.

[155] Sheffi, Y. (1985). *Urban transportation networks: Equilibrium analysis with mathematical programming methods*. Prentice-Hall.

[156] Cascetta, E., & Nguyen, S. (1988). A unified framework for estimating or updating origin/destination matrices from traffic counts. *Transportation Research Part B: Methodological, 22*(6), 437–455.

[157] Cascetta, E. (1984). Estimation of trip matrices from traffic counts and survey data: A generalized least squares estimator. *Transportation Research Part B: Methodological, 18*(4–5), 289–299.

[158] Van Zuylen, H. J., & Willumsen, L. G. (1980). The most likely trip matrix estimated from traffic counts. *Transportation Research Part B: Methodological, 14*(3), 281–293.

[159] Yang, H., Iida, Y., & Sasaki, T. (1991). An analysis of the reliability of an origin-destination trip matrix estimated from traffic counts. *Transportation Research Part B: Methodological, 25*(5), 351–363.

[160] Yang, H. (1995). Heuristic algorithms for the bilevel origin-destination matrix estimation problem. *Transportation Research Part B: Methodological, 29*(4), 231–242.

[161] Zhou, X., Qin, X., & Mahmassani, H. S. (2003). Dynamic origin-destination demand estimation with multiday link traffic counts for planning applications. *Transportation Research Record, 1831*(1), 30–38.

[162] Bierlaire, M., Crittin, F., & Toint, P. L. (2008). A Monte-Carlo approach for estimating origin-destination matrices. *Transportation Research Part B: Methodological, 42*(6), 590–607.

[163] Baum-Snow, N. (2010). Changes in transportation infrastructure and commuting patterns in U.S. metropolitan areas, 1960–2000. *American Economic Review, 100*(2), 378–382.

[164] Agyemang, W., Cheng, L., & Vanclay, F. (2020). Spatial structure, intra-urban commuting patterns and travel mode choice: Analyses of relationships in the Kumasi Metropolis, Ghana. *Cities, 96*, 102432.

[165] Allen, J., & Farber, S. (2021). Suburbanization of transport poverty. *Annals of the American Association of Geographers, 111*(6), 1833–1850.

[166] Le, J., & Teng, J. (2023). Understanding influencing factors of travel mode choice in urban-suburban travel: A case study in Shanghai. *Urban Rail Transit, 9*, 127–146.

[167] Barrat, A., Barthélemy, M., Pastor-Satorras, R., & Vespignani, A. (2004). The architecture of complex weighted networks. *Proceedings of the National Academy of Sciences, 101*(11), 3747–3752.

[168] Guimerà, R., Mossa, S., Turtschi, A., & Amaral, L. A. N. (2005). The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proceedings of the National Academy of Sciences, 102*(22), 7794–7799.

[169] Pelletier, M.-P., Trépanier, M., & Morency, C. (2011). Smart card data use in public transit: A literature review. *Transportation Research Part C: Emerging Technologies, 19*(4), 557–568.

[170] Munizaga, M. A., & Palma, C. (2012). Estimation of a disaggregate multimodal public transport origin–destination matrix from passive smartcard

data from Santiago, Chile. *Transportation Research Part C: Emerging Technologies, 24*, 9–18.

[171] Alexander, L., Jiang, S., Murga, M., & González, M. C. (2015). Origin–destination trips by purpose and time of day inferred from mobile phone data. *Transportation Research Part C: Emerging Technologies, 58*, 240–250.

[172] Zheng, Y., Liu, X., & Chen, W. (2022). Data-driven origin–destination matrix estimation: A review of methods and applications. *Transport Reviews, 42*(6), 743–770.

[173] Ceder, A. (2016). *Public transit planning and operation: Modeling, practice and behavior* (2nd ed.). CRC Press.

[174] Banister, D. (2008). The sustainable mobility paradigm. *Transport Policy, 15*(2), 73–80.

[175] Litman, T. (2023). *Transportation demand management encyclopedia*. Victoria Transport Policy Institute.

[176] Ashok, K., & Ben-Akiva, M. E. (1996). Alternative approaches for real-time estimation and prediction of time-dependent origin-destination flows. *Transportation Science, 34*(1), 21–36.

[177] Cascetta, E., Inaudi, D., & Marquis, G. (1993). Dynamic estimators of origin-destination matrices using traffic counts. *Transportation Science, 27*(4), 363–373.

[178] Lo, H. P., & Chan, Y. C. (1996). Simultaneous estimation of an origin-destination matrix and link choice proportions. *Transportation Research Part A: Policy and Practice, 30*(2), 109–125.

[179] Bell, M. G. H. (1997). The estimation of origin-destination matrices by constrained generalized least squares. *Transportation Research Part B: Methodological, 25*(1), 13–22.

[180] Nielsen, O. A. (2000). A stochastic transit assignment model considering differences in passengers utility functions. *Transportation Research Part B: Methodological, 34*(5), 377–402.

[181] Cipriani, E., Florian, M., Mahut, M., & Nigro, M. (2011). A gradient approximation approach for adjusting temporal origin-destination matrices. *Transportation Research Part C: Emerging Technologies, 19*(2), 270–282.

[182] Ben-Akiva, M., & Lerman, S. R. (1985). *Discrete choice analysis: Theory and application to travel demand*. MIT Press.

[183] Train, K. E. (2009). *Discrete choice methods with simulation* (2nd ed.). Cambridge University Press.

[184] Bovy, P. H. L., & Stern, E. (2001). *Route choice: Wayfinding in transport networks*. Kluwer Academic Publishers.

[185] Spiess, H., & Florian, M. (1989). Optimal strategies: A new assignment model for transit networks. *Transportation Research Part B: Methodological, 23*(2), 83–102.

[186] Nguyen, S., & Pallottino, S. (1988). Equilibrium traffic assignment for large scale transit networks. *European Journal of Operational Research, 37*(2), 176–186.

[187] Furth, P. G., & Rahbee, A. (2000). Optimal bus stop spacing through dynamic programming and geographic modeling. *Transportation Research Record, 1731*(1), 15–22.

[188] Wilson, A. G. (1970). *Entropy in urban and regional modelling*. Pion.

[189] Timmermans, H. J. P. (Ed.). (2009). *Handbook of urban mobility*. Springer.

[190] Batty, M. (2013). *The new science of cities*. MIT Press.

[191] Cats, O., Larijani, A. N., Koutsopoulos, H. N., & Burghout, W. (2015). Impacts of holding control strategies on transit performance and passenger behaviour. *Transportmetrica A: Transport Science, 11*(10), 1–25.

[192] Mazloumi, E., Currie, G., & Rose, G. (2010). Using GPS data to gain insight into public transport travel time variability. *Journal of Transportation Engineering, 136*(7), 623–631.

[193] Toole, J. L., Colak, S., Sturt, B., Alexander, L. P., Evsukoff, A., & Gonzalez, M. C. (2015). The path most traveled: Travel demand estimation using big data resources. *Transportation Research Part C: Emerging Technologies, 58*, 162–177.

[194] Holtzclaw, J., Clear, R., Dittmar, H., Goldstein, D., & Haas, P. (2002). Location efficiency: Neighborhood and socio-economic characteristics determine auto ownership and use. *Transportation Planning and Technology, 25*(1), 1–27.

[195] El-Geneidy, A., Levinson, D., Diab, E., Boisjoly, G., Verbich, D., & Loong, C. (2016). The cost of equity: Assessing transit accessibility and social disparity using total travel cost. *Transportation Research Part A: Policy and Practice, 91*, 302–316.

[196] Manley, E., Zhong, C., & Batty, M. (2018). Spatiotemporal variation in travel regularity through transit user profiling. *Transportation, 45*(3), 703–732.

[197] Wegener, M. (2004). Overview of land-use transport models. In D. A. Hensher & K. J. Button (Eds.), *Handbook of transport geography and spatial systems* (pp. 127–146). Elsevier.

[198] McNally, M. G. (2007). The four step model. In D. A. Hensher & K. J. Button (Eds.), *Handbook of transport modelling* (2nd ed., pp. 35–53). Elsevier.

[199] Stopher, P. R., & Greaves, S. P. (2007). Household travel surveys: Where are we going? *Transportation Research Part A: Policy and Practice, 41*(5), 367–381.

[200] Derrible, S., & Kennedy, C. (2010). The complexity and robustness of metro networks. *Physica A, 389*(17), 3678–3691.

[201] von Ferber, C., Holovatch, T., Holovatch, Y., & Palchykov, V. (2009). Public transport networks: Empirical analysis and modeling. *The European Physical Journal B, 68*(2), 261–275.

[202] Rodrigue, J.-P. (2020). *The geography of transport systems* (5th ed.). Routledge.

[203] Kivel"a, M., Arenas, A., Barthelemy, M., Gleeson, J. P., Moreno, Y., & Porter, M. A. (2014). Multilayer networks. *Journal of Complex Networks, 2*(3), 203–271.

[204] Boccaletti, S., Bianconi, G., Criado, R., Del Genio, C. I., Gómez-Gardeñes, J., Romance, M., et al. (2014). The structure and dynamics of multilayer networks. *Physics Reports, 544*(1), 1–122.

[205] De Domenico, M., Solé-Ribalta, A., Cozzo, E., Kivel"a, M., Moreno, Y., Porter, M. A., et al. (2013). Mathematical formulation of multilayer networks. *Physical Review X, 3*(4), 041022.

[206] Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Review, 45*(2), 167–256.

[207] Latora, V., & Marchiori, M. (2001). Efficient behavior of small-world networks. *Physical Review Letters, 87*(19), 198701.

[208] Sienkiewicz, J., & Ho lyst, J. A. (2005). Statistical analysis of public transport networks. *Physical Review E, 72*(4), 046127.

[209] Fruin, J. J. (1971). *Pedestrian planning and design*. Metropolitan Association of Urban Designers.

[210] Geurs, K. T., & van Wee, B. (2004). Accessibility evaluation of land-use and transport strategies. *Journal of Transport Geography, 12*(2), 127–140.