КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1277
УДК 004.056:629.331

Журавчак Анастасія Юріївна
асистент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID:0000-0002-8196-7963
anastasiia.y.tolkachova@lpnu.ua

Журавчак Даниїл Юрійович
доктор філософії, доцент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID:0000-0003-4989-0203
danyil.y.zhuravchak@lpnu.ua

Журавчак Юрій Юрійович
магістр кафедри інформаційних систем та технологій
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID:0009-0003-2378-5365
yurii.zhuravchak.mitis.2023@lpnu.ua

ОЦІНЮВАННЯ КІБЕРРИЗИКІВ ТРАНСПОРТНИХ ЗАСОБІВ НА ОСНОВІ АНАЛІЗУ ПОВЕРХНІ АТАКИ

Анотація. У статті розглянуто проблему аналізу кіберзагроз у сучасних транспортних засобах, які дедалі більше перетворюються на складні кіберфізичні системи з великою кількістю електронних блоків керування, внутрішніх мереж, бездротових інтерфейсів, сенсорів, діагностичних портів, інформаційно-розважальних модулів і зовнішніх цифрових сервісів. Обґрунтовано, що безпека автомобіля не може обмежуватися лише дослідженням CAN-шини, оскільки реальна поверхня атаки охоплює значно ширший набір каналів взаємодії з навколишнім середовищем та користувачем. Особливу увагу приділено підходу моделювання загроз, який дає змогу послідовно ідентифікувати точки входу, визначати приймачі вхідних сигналів, аналізувати межі довіри між компонентами та встановлювати потенційні маршрути поширення атаки всередині автомобільної архітектури. У роботі систематизовано основні групи загроз, зокрема загрози віддалених комунікаційних інтерфейсів, Wi-Fi, Bluetooth, стільникового зв’язку, систем безключового доступу, TPMS, USB-портів, OBD-II, інформаційно-розважальних систем, діагностичних механізмів та внутрішніх автомобільних мереж. Показано, що найбільш критичними є сценарії, у яких зовнішній канал може бути використаний для доступу до внутрішніх систем транспортного засобу або для впливу на електронні блоки керування. Окремо розглянуто ризики порушення конфіденційності, цілісності та доступності, включно з відстеженням місцезнаходження, підміною даних, встановленням шкідливого програмного забезпечення, блокуванням функцій автомобіля та маніпуляцією повідомленнями у внутрішній мережі. Запропоновано розглядати модель загроз як динамічний документ, що має оновлюватися протягом усього життєвого циклу транспортного засобу з урахуванням змін у програмному забезпеченні, архітектурі та зовнішніх сервісах. Практичне значення дослідження полягає у формуванні структурованого підходу до виявлення, класифікації та пріоритезації ризиків, що може бути використано під час аудиту, тестування та проєктування захищених автомобільних систем.

Ключові слова: CAN bus; вразливість; загроза; автомобіль; кібербезпека; атака.

ВСТУП

Сучасні транспортні засоби дедалі більше перетворюються на складні системи, у яких механічні компоненти тісно інтегровані з електронними блоками керування, мережевими інтерфейсами, програмним забезпеченням, сенсорами та зовнішніми сервісами. Така цифровізація автомобільної галузі підвищує комфорт, безпеку та функціональність транспортних засобів, однак водночас розширює поверхню атаки та створює нові ризики. Потенційні загрози можуть стосуватися не лише внутрішніх

автомобільних мереж, зокрема CAN-шини, а й модулів Bluetooth, Wi-Fi, мобільних застосунків, систем віддаленого доступу, інфраструктури оновлення програмного забезпечення та взаємодії транспортного засобу з хмарними сервісами. У зв'язку з цим аналіз загроз у транспортних засобах є актуальним напрямом досліджень, оскільки успішна кібератака може призвести не лише до порушення конфіденційності даних, а й до впливу на цілісність, доступність і безпечність функціонування автомобіля.

Постановка проблеми. Зростання рівня цифровізації транспортних засобів розширює поверхню кібератак, що потребує комплексного аналізу загроз не лише для внутрішніх автомобільних мереж, а й для зовнішніх інтерфейсів, програмного забезпечення та хмарної інфраструктури.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях автомобіль дедалі частіше розглядається як складна система. Зокрема, у роботі Kifor та співавторів [1] систематизовано напрями автомобільної кібербезпеки, пов'язані зі стандартами, фреймворками, моніторингом, тестуванням і валідацією захищеності автомобільних систем.

Окремий напрям досліджень пов'язаний із моделюванням загроз. У роботі Ebrahimi та співавторів [2] розглянуто побудову моделей загроз для connected vehicles на основі attack-tree підходу в контексті ISO/SAE 21434 [3] та UN R155 [4]. Автори підкреслюють, що простого переліку ізольованих загроз недостатньо, оскільки необхідно враховувати архітектуру транспортного засобу, взаємозв'язки між компонентами та можливі шляхи компрометації від зовнішнього інтерфейсу до цільового активу. Подібну ідею розвивають Häckel та співавтори [5], які пропонують багаторівневу інфраструктуру безпеки для connected vehicles, що охоплює мережевий захист, моніторинг, виявлення аномалій, управління інцидентами та хмарний центр захисту. Це підтверджує, що ефективний захист транспортного засобу має бути комплексним і не може обмежуватися лише окремим протоколом або компонентом.

У сучасних працях також акцентується увага на розширенні поверхні атаки за рахунок автономних систем, V2X-комунікацій, OTA-оновлень, мобільних застосунків, хмарних сервісів та цифрових двійників. Зокрема, Yousseef та співавтори показують [6], що безпека автономного транспортного засобу має охоплювати не лише CAN, LIN, MOST, FlexRay чи Automotive Ethernet, а й Bluetooth, Wi-Fi, eSIM, супутниковий зв'язок, сенсори та AI-компоненти. Shah та співавтори [7] розглядають новий напрям – threat modeling для цифрових двійників транспортних засобів, де додатковими ризиками стають синхронізація з фізичним об'єктом, достовірність симуляційних моделей і захист каналів обміну даними.

Аналіз сучасних джерел свідчить, що значна частина досліджень уже охоплює стандартизацію, attack-tree моделі, захисні інфраструктури, автономні автомобілі та цифрові двійники. Водночас недостатньо вирішеною залишається проблема узагальненої систематизації основних типів загроз для транспортних засобів з позиції повної поверхні атаки.

Саме тому наукова новизна цієї статті полягає у формуванні комплексного підходу до аналізу загроз, який не обмежується CAN-шиною, а враховує зовнішні та внутрішні канали взаємодії: стільниковий зв'язок, Wi-Fi, Bluetooth, TPMS, системи безключового доступу, USB, OBD-II, infotainment-модулі, діагностичні механізми та внутрішні автомобільні мережі.

Метою статті є висвітлення основних нових загроз для сучасних транспортних засобів, що виникають внаслідок їх цифровізації, підключення до зовнішніх мереж та інтеграції з програмними й хмарними сервісами.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Одним із ключових понять під час аналізу кібербезпеки транспортних засобів є поверхня атаки, тобто сукупність усіх можливих точок входу, через які зловмисник може взаємодіяти з системою або впливати на її роботу [8]. Під час визначення поверхні атаки основна увага приділяється каналам надходження даних до автомобіля. До таких каналів можуть належати системи безключового доступу, радіосигнали, Bluetooth, Wi-Fi, USB-порти, діагностичні інтерфейси, GPS-навігація, інформаційно-розважальні системи, мобільні застосунки, телематичні модулі та зарядна інфраструктура електромобілів. Кожен із цих елементів може створювати потенційний ризик у разі оброблення помилкових, підроблених або шкідливих даних.

З огляду на значну кількість можливих точок входу, аналіз загроз у транспортних засобах доцільно здійснювати із застосуванням моделювання загроз [9]. Цей підхід передбачає вивчення архітектури автомобіля, визначення основних компонентів, каналів обміну даними та взаємозв'язків між ними. На основі такої моделі можна виявити найбільш ризиковані інтерфейси й визначити пріоритетні напрями для подальшого аудиту та тестування.

Модель загроз має розглядатися як динамічний документ, що оновлюється протягом життєвого циклу транспортного засобу, оскільки його програмне забезпечення, архітектура та зовнішні сервіси можуть змінюватися. Таким чином, аналіз поверхні атаки та моделювання загроз є важливими етапами оцінювання кібербезпеки сучасних автомобільних систем [10].

Для моделювання загроз у транспортному засобі доцільно використовувати багаторівневий підхід. На початковому рівні формується загальна схема, яка відображає транспортний засіб як єдину систему та фіксує основні зовнішні й внутрішні канали надходження даних. До таких каналів можуть належати стільниковий зв'язок, Wi-Fi, Bluetooth, система контролю тиску в шинах, безключовий доступ, USB-інтерфейси, діагностичний роз'єм OBD-II, інформаційно-розважальна система та внутрішня CAN-мережа.

На наступному рівні аналізу важливо визначити не лише самі канали входу, а й компоненти, які приймають і обробляють ці дані. Наприклад, Bluetooth або USB можуть взаємодіяти з інформаційно-розважальною системою, TPMS – із приймачем системи контролю тиску в шинах, безключовий доступ – з іммобілайзером, а діагностичний роз'єм OBD-II – з електронними блоками керування. Такий розподіл є важливим, оскільки ризик визначається не лише самим каналом зв'язку, а й тим, до яких внутрішніх систем він може привести. Найбільш небезпечними є ті сценарії, у яких зовнішній інтерфейс опосередковано надає доступ до критичних внутрішніх мереж автомобіля.

Важливим елементом такого аналізу є поняття меж довіри. У транспортному засобі різні канали комунікації мають різний рівень довіри. Наприклад, віддалений стільниковий інтерфейс або Wi-Fi-з'єднання мають нижчий рівень довіри, ніж внутрішня мережа автомобіля. Однак якщо дані з малодовіреного каналу через інформаційно-розважальну систему або інший шлюз потрапляють до внутрішньої мережі, ризик значно зростає. Чим більше меж довіри перетинає комунікаційний канал, тим більш критичним він є з погляду кібербезпеки.

Одним із ключових типів загроз є загрози, пов'язані з віддаленими комунікаційними інтерфейсами. До цієї групи належать стільниковий зв'язок, Wi-Fi та інші мережеві канали, які можуть забезпечувати взаємодію автомобіля з виробником, сервісною інфраструктурою, мобільними застосунками або хмарними платформами. Потенційна небезпека таких каналів полягає в тому, що атака може виконуватися без фізичного доступу до автомобіля. Зловмисник може намагатися перехопити трафік, використати вразливість у програмному забезпеченні, підмінити точку доступу, атакувати телематичний модуль або використати слабкі механізми аутентифікації. Особливо критичними є сценарії, у яких через віддалений канал можна отримати доступ до внутрішньої мережі автомобіля або до функцій дистанційної діагностики.

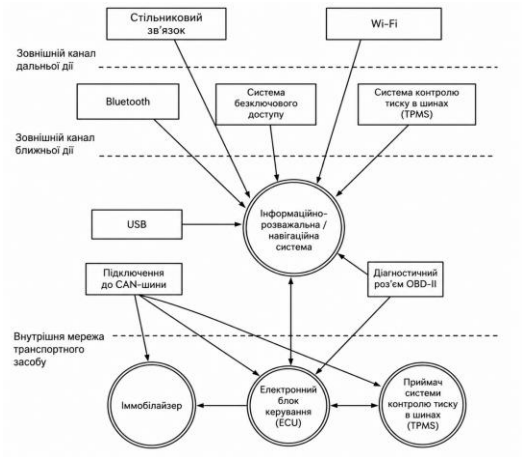

Рис. 1. Карта вхідних каналів і компонентів транспортного засобу в моделі загроз

Окрему групу становлять загрози ближнього радіусу дії. До них належать Bluetooth, системи безключового доступу, датчики тиску в шинах та інші бездротові компоненти, що працюють на обмеженій відстані. На перший погляд такі інтерфейси можуть здаватися менш небезпечними, оскільки потребують фізичної близькості до автомобіля. Однак на практиці вони залишаються важливою частиною поверхні атаки. Наприклад, Bluetooth може використовуватися для передавання контактів, аудіоданих або інших файлів до інформаційно-розважальної системи. Якщо обробка таких даних реалізована некоректно, це може призвести до збоїв або виконання небажаних дій. Системи

безключового доступу також є критичними, оскільки вони безпосередньо пов'язані з автентифікацією власника, блокуванням дверей та роботою іммобілайзера.

Загрози, пов'язані з ключами та іммобілайзером, мають особливе значення, оскільки вони стосуються контролю доступу до транспортного засобу. Потенційні атаки можуть бути спрямовані на перехоплення або повторне використання сигналів, клонування ключа, блокування роботи брелока, порушення процесу аутентифікації або створення ситуації, за якої іммобілайзер переходить у некоректний стан. У таких сценаріях ризик полягає не лише у можливості несанкціонованого відкриття автомобіля, а й у потенційному викраденні транспортного засобу або блокуванні доступу для легітимного власника.

Система контролю тиску в шинах також може бути джерелом кіберризиків. TPMS зазвичай передає дані бездротовим каналом, а тому може бути об'єктом підміни сигналів або відстеження. Потенційний зловмисник може спробувати сформувати неправдиві повідомлення про стан шин, викликати помилкові попередження або використати унікальні ідентифікатори датчиків для відстеження переміщення автомобіля. Хоча така система не завжди має прямий доступ до критичних функцій керування, вона може впливати на поведінку водія, створювати помилкові аварійні ситуації або використовуватися як додатковий канал збору інформації.

Інформаційно-розважальна система є одним із найбільш важливих елементів поверхні атаки сучасного автомобіля. Вона часто поєднує в собі багато інтерфейсів: Bluetooth, USB, Wi-Fi, навігацію, мультимедіа, мобільні застосунки, голосові функції та інколи доступ до телематичних сервісів. Проблема полягає в тому, що така система може бути одночасно зручною для користувача і небезпечною з погляду кібербезпеки, якщо вона має зв'язок із внутрішніми мережами автомобіля. У разі компрометації інформаційно-розважального модуля зловмисник потенційно може отримати можливість прослуховувати дії користувача, змінювати відображувану інформацію, маніпулювати навігаційними даними, встановлювати шкідливе програмне забезпечення або використовувати систему як проміжний етап для подальшого доступу до CAN-шини чи електронних блоків керування.

USB-інтерфейси становлять окремий клас загроз, оскільки вони передбачають фізичне підключення зовнішнього пристрою або носія даних. Через USB можуть передаватися мультимедійні файли, оновлення програмного забезпечення, контактні дані або інші об'єкти, які повинні бути оброблені програмним забезпеченням автомобіля. Небезпека полягає у можливості використання спеціально сформованих файлів, шкідливих пристроїв або модифікованих оновлень. Якщо система недостатньо перевіряє джерело, формат або цілісність даних, USB може стати каналом встановлення шкідливого коду або порушення роботи інформаційно-розважального модуля.

Діагностичні інтерфейси, зокрема OBD-II, є ще одним важливим джерелом ризику. Спочатку такі інтерфейси призначалися для технічного обслуговування, діагностики несправностей і взаємодії з електронними блоками керування. Однак з погляду кібербезпеки вони є потенційно небезпечними, оскільки можуть забезпечувати прямий або опосередкований доступ до внутрішніх мереж автомобіля. Якщо до діагностичного порту підключити шкідливий пристрій, він може надсилати повідомлення до CAN-шини, збирати дані про стан автомобіля, виконувати несанкціоновані діагностичні запити або створювати канал для віддаленої взаємодії. Таким чином, атака, яка спочатку є фізичною, може бути перетворена на віддалену, якщо шкідливий діагностичний пристрій має власний модуль зв'язку.

CAN-шина є критичним елементом автомобільної архітектури, оскільки забезпечує обмін повідомленнями між електронними блоками керування. Її основна проблема з погляду безпеки полягає в тому, що історично вона проєктувалася для надійної комунікації всередині довіреного середовища, а не для протидії зловмисним діям. У багатьох реалізаціях повідомлення в мережі не містять достатніх механізмів автентифікації джерела, а тому пристрій, який отримав доступ до шини, потенційно може імітувати інші компоненти. Це створює ризик підміни повідомлень, ін'єкції команд, перевантаження мережі або маніпуляції даними, які використовуються іншими системами автомобіля.

Важливо розуміти, що найбільш небезпечні загрози часто виникають не в одному окремому компоненті, а на стику кількох систем. Наприклад, Bluetooth сам по собі може мати обмежений вплив, але якщо через нього можна скомпрометувати інформаційно-розважальну систему, а та має зв'язок із внутрішньою мережею автомобіля, ризик стає значно вищим. Аналогічно USB-носій може бути лише локальним каналом передачі файлів, але за наявності вразливості в обробнику файлів він може перетворитися на шлях до виконання коду. Тому аналіз загроз повинен враховувати не лише окремі інтерфейси, а й маршрути поширення атаки між компонентами.

Окремим напрямом є загрози для конфіденційності та приватності. Сучасні автомобілі можуть збирати інформацію про місцезнаходження, маршрути, стиль водіння, стан систем, підключені пристрої, контакти користувача та інші дані. У разі компрометації телематичних модулів, інформаційно-розважальної системи або бездротових інтерфейсів зловмисник може отримати доступ до чутливої

інформації або використовувати автомобіль для стеження. Загроза відстеження може бути пов'язана не лише з GPS чи стільниковим зв'язком, а й з унікальними ідентифікаторами окремих бездротових компонентів, наприклад датчиків TPMS.

Ще одним важливим типом загроз є порушення доступності. У транспортному засобі відмова системи може мати суттєво серйозніші наслідки, ніж у звичайному IT-сервісі. Атака може бути спрямована на блокування роботи інформаційно-розважальної системи, створення помилкових повідомлень про несправності, перевантаження внутрішньої мережі, розрядження акумулятора через постійне опитування певних компонентів або виведення окремих модулів у нестабільний стан. Такі дії можуть не давати зловмиснику повного контролю над автомобілем, але вони здатні створити небезпечну або економічно збиткову ситуацію для власника.

До окремої категорії можна віднести загрози, пов'язані з оновленням програмного забезпечення та конфігурації автомобіля. Сучасні транспортні засоби дедалі більше залежать від програмного забезпечення, а тому процес його оновлення стає критично важливим. Якщо механізм оновлення не забезпечує належної перевірки цілісності, автентичності та джерела оновлення, виникає ризик встановлення модифікованого або шкідливого коду. Це може стосуватися як інформаційно-розважальної системи, так і електронних блоків керування. Особливо небезпечними є сценарії, у яких оновлення може бути ініційоване через USB, сервісну інфраструктуру або віддалений канал без достатньої криптографічної перевірки.

Для систематизації виявлених загроз доцільно застосовувати методи оцінювання ризику. Одним із можливих підходів є використання критеріїв, які враховують потенційний рівень шкоди, відтворюваність атаки, складність експлуатації, кількість потенційно уражених користувачів і простоту виявлення вразливості. Така оцінка дозволяє відрізнити теоретично можливі, але малоймовірні сценарії від загроз, які мають високий практичний пріоритет. Наприклад, віддалений канал, що може привести до виконання коду в привілейованому середовищі або доступу до внутрішньої мережі автомобіля, повинен отримувати вищий пріоритет, ніж локальний інтерфейс із обмеженим впливом.

З практичної точки зору, результати моделювання загроз мають використовуватися не лише для опису ризиків, а й для формування контрзаходів. Для віддалених каналів важливими є автентифікація, шифрування, перевірка цілісності повідомлень і захист від підміни інфраструктури. Для інформаційно-розважальних систем – ізоляція від критичних мереж, обмеження привілеїв, контроль оновлень і перевірка вхідних даних. Для USB та Bluetooth – фільтрація типів даних, захист від небезпечних пристроїв, безпечна обробка файлів і вимкнення непотрібних сервісів. Для CAN-шини та діагностичних інтерфейсів – сегментація мережі, шлюзи безпеки, контроль діагностичних команд, журналювання дій і обмеження фізичного доступу.

Отже, аналіз загроз у транспортних засобах повинен виходити за межі дослідження лише CAN-шини. Хоча CAN залишається критично важливою частиною автомобільної архітектури, сучасна поверхня атаки охоплює значно ширший набір інтерфейсів і компонентів. Найбільшу небезпеку становлять ті сценарії, у яких зовнішній або малодовірений канал може бути використаний як шлях до внутрішніх систем автомобіля. Тому ефективна модель загроз має враховувати віддалені канали зв'язку, бездротові інтерфейси ближнього радіусу дії, фізичні порти, діагностичні механізми, інформаційно-розважальні системи, внутрішні мережі, програмне забезпечення та хмарні сервіси. Такий комплексний підхід дозволяє краще зрозуміти реальний рівень кіберризику та визначити пріоритетні напрями захисту сучасних транспортних засобів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті здійснено аналіз основних кіберзагроз у сучасних транспортних засобах з урахуванням їх поступового перетворення на складні кіберфізичні системи. Показано, що безпека автомобіля не може обмежуватися лише дослідженням CAN-шини, оскільки реальна поверхня атаки охоплює значно ширший набір зовнішніх і внутрішніх каналів взаємодії. До них належать стільниковий зв'язок, Wi-Fi, Bluetooth, системи безключового доступу, TPMS, USB-порти, діагностичний інтерфейс OBD-II, інформаційно-розважальні системи, телематичні модулі та внутрішні автомобільні мережі. Встановлено, що найбільш критичними є ті сценарії, у яких зовнішній канал може бути використаний як шлях до внутрішніх компонентів транспортного засобу, зокрема електронних блоків керування та мереж обміну даними.

У результаті дослідження обґрунтовано доцільність використання моделювання загроз як структурованого підходу до виявлення точок входу, аналізу приймачів вхідних сигналів, визначення меж довіри та оцінювання потенційних маршрутів поширення атаки всередині автомобільної архітектури. Такий підхід дозволяє не лише систематизувати основні типи загроз, а й визначити пріоритетні напрями

аудиту, тестування та впровадження захисних механізмів. Особливу увагу слід приділяти захисту віддалених інтерфейсів, сегментації внутрішніх мереж, безпечному оновленню програмного забезпечення, контролю діагностичних функцій та ізоляції інформаційно-розважальних систем від критичних компонентів автомобіля.

Перспективи подальших досліджень полягають у розробленні більш деталізованої моделі загроз для окремих типів транспортних засобів, зокрема connected vehicles, електромобілів та автономних автомобілів. Доцільним є подальше вивчення ризиків, пов'язаних із V2X-комунікаціями, OTA-оновленнями, мобільними застосунками, хмарними сервісами, цифровими двійниками транспортних засобів та використанням штучного інтелекту в системах автономного керування. Окремим напрямом подальших розвідок є формування практичної методики оцінювання ризиків, яка поєднуватиме моделювання загроз, класифікацію активів, аналіз меж довіри та кількісну або якісну пріоритезацію загроз для автомобільних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kifor, C. V., & Popescu, A. (2024). Automotive cybersecurity: A survey on frameworks, standards, and testing and monitoring technologies. *Sensors, 24*(18), Article 6139. https://doi.org/10.3390/s24186139
2. Ebrahimi, M., Striessnig, C., Castella Triginer, J., & Schmittner, C. (2022). Identification and verification of attack-tree threat models in connected vehicles. In *SAE 2022 Intelligent and Connected Vehicles Symposium*. SAE Technical Paper 2022-01-7087. https://doi.org/10.4271/2022-01-7087
3. International Organization for Standardization. (2021). *ISO/SAE 21434:2021: Road vehicles–Cybersecurity engineering*. ISO. https://www.iso.org/standard/70918.html
4. United Nations Economic Commission for Europe. (2021). *UN Regulation No. 155: Cyber security and cyber security management system*. UNECE. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
5. Häckel, T., Meyer, P., Stahlbock, L., Langer, F., Eckhardt, S. A., Korf, F., & Schmidt, T. C. (2023). *A multilayered security infrastructure for connected vehicles: First lessons from the field* (arXiv:2310.10336). arXiv. https://doi.org/10.48550/arXiv.2310.10336
6. Yousseef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). *Autonomous vehicle security: A deep dive into threat modeling* (arXiv:2412.15348). arXiv. https://doi.org/10.48550/arXiv.2412.15348
7. Shah, U. M., Minhas, D. M., Kifayat, K., Shah, K. A., & Frey, G. (2025). Threat modeling and attacks on digital twins of vehicles: A systematic literature review. *Smart Cities, 8*(5), Article 142. https://doi.org/10.3390/smartcities8050142
8. IBM. (n.d.). *What is an attack surface?* IBM Think. Retrieved June 17, 2026, from https://www.ibm.com/think/topics/attack-surface
9. OWASP Foundation. (n.d.). *Threat modeling*. OWASP. Retrieved June 17, 2026, from https://owasp.org/www-community/Threat_Modeling
10. Moshtari, S., Okutan, A., & Mirakhorli, M. (2021). *A grounded theory based approach to characterize software attack surfaces* (arXiv:2112.01635). arXiv. https://doi.org/10.48550/arXiv.2112.01635

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Anastasiia Zhuravchak
Assistant of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID:0000-0002-8196-7963
anastasiia.y.tolkachova@lpnu.ua

Danyil Zhuravchak
PhD, Associate Professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID:0000-0003-4989-0203
danyil.y.zhuravchak@lpnu.ua

Yurii Zhuravchak
Master's student in the Department of Information Systems and Technologies
Lviv Polytechnic National University, Lviv, Ukraine
ORCID:0009-0003-2378-5365
yurii.zhuravchak.mitis.2023@lpnu.ua

ASSESSMENT OF CYBER RISKS IN VEHICLES BASED ON ATTACK SURFACE ANALYSIS

Abstract. The article examines the problem of analyzing cyber threats in modern vehicles, which are increasingly becoming complex cyber-physical systems with a large number of electronic control units, internal networks, wireless interfaces, sensors, diagnostic ports, infotainment modules, and external digital services. It is substantiated that vehicle security cannot be limited solely to the study of the CAN bus, since the actual attack surface includes a much broader set of interaction channels with the environment and the user. Particular attention is paid to the threat modeling approach, which enables the systematic identification of entry points, the determination of input signal receivers, the analysis of trust boundaries between components, and the identification of potential attack propagation paths within the automotive architecture. The paper systematizes the main groups of threats, including threats related to remote communication interfaces, Wi-Fi, Bluetooth, cellular communication, keyless entry systems, TPMS, USB ports, OBD-II, infotainment systems, diagnostic mechanisms, and internal vehicle networks. It is shown that the most critical scenarios are those in which an external channel can be used to access the internal systems of a vehicle or to influence electronic control units. The risks of violating confidentiality, integrity, and availability are considered separately, including location tracking, data spoofing, malware installation, blocking vehicle functions, and manipulating messages within the internal network. It is proposed to consider the threat model as a dynamic document that should be updated throughout the entire vehicle life cycle, taking into account changes in software, architecture, and external services. The practical significance of the study lies in the formation of a structured approach to identifying, classifying, and prioritizing risks, which can be used during the auditing, testing, and design of secure automotive systems.

Keywords: CAN bus; vulnerability; threat; automobile; cybersecurity; attack.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kifor, C. V., & Popescu, A. (2024). Automotive cybersecurity: A survey on frameworks, standards, and testing and monitoring technologies. *Sensors, 24*(18), Article 6139. https://doi.org/10.3390/s24186139
2. Ebrahimi, M., Striessnig, C., Castella Triginer, J., & Schmittner, C. (2022). Identification and verification of attack-tree threat models in connected vehicles. In *SAE 2022 Intelligent and Connected Vehicles Symposium.* SAE Technical Paper 2022-01-7087. https://doi.org/10.4271/2022-01-7087
3. International Organization for Standardization. (2021). *ISO/SAE 21434:2021: Road vehicles–Cybersecurity engineering*. ISO. https://www.iso.org/standard/70918.html
4. United Nations Economic Commission for Europe. (2021). *UN Regulation No. 155: Cyber security and cyber security management system*. UNECE. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

5. Häckel, T., Meyer, P., Stahlbock, L., Langer, F., Eckhardt, S. A., Korf, F., & Schmidt, T. C. (2023). *A multilayered security infrastructure for connected vehicles: First lessons from the field* (arXiv:2310.10336). arXiv. https://doi.org/10.48550/arXiv.2310.10336
6. Yousseef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). *Autonomous vehicle security: A deep dive into threat modeling* (arXiv:2412.15348). arXiv. https://doi.org/10.48550/arXiv.2412.15348
7. Shah, U. M., Minhas, D. M., Kifayat, K., Shah, K. A., & Frey, G. (2025). Threat modeling and attacks on digital twins of vehicles: A systematic literature review. *Smart Cities, 8*(5), Article 142. https://doi.org/10.3390/smartcities8050142
8. IBM. (n.d.). *What is an attack surface?* IBM Think. Retrieved June 17, 2026, from https://www.ibm.com/think/topics/attack-surface
9. OWASP Foundation. (n.d.). *Threat modeling*. OWASP. Retrieved June 17, 2026, from https://owasp.org/www-community/Threat_Modeling
10. Moshtari, S., Okutan, A., & Mirakhorli, M. (2021). *A grounded theory based approach to characterize software attack surfaces* (arXiv:2112.01635). arXiv. https://doi.org/10.48550/arXiv.2112.01635

Отримано редакцією журналу / Received: 19.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 24.09.26