УДК 004.056
DOI https://doi.org/10.32782/2663-5941/2024.6.2/34

Цяпа С.М.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

ЗАГРОЗИ ТА ВРАЗЛИВОСТІ КІБЕРБЕЗПЕКИ В МЕРЕЖЕВИХ ТА АВТОНОМНИХ ТРАНСПОРТНИХ СИСТЕМАХ

Стаття присвячена дослідженню загроз кібербезпеки, пов'язаних з мережевими та автономними транспортними засобами (CAV) – ключовим напрямком розвитку автомобільної промисловості. CAV мають потенціал покращити транспортну галузь, забезпечуючи підвищену безпеку дорожнього руху, покращену доступність та ефективність перевезень. Незважаючи на значний прогрес у розвитку CAV систем, питання їхньої кібербезпеки залишається актуальним. Зростання кількості мережевих пристроїв та підвищення складності систем управління CAV створюють нові можливості для кібератак, які можуть призвести до серйозних наслідків. У статті розкривається критична роль датчиків і мережевих комунікацій у вдосконаленні автомобільної інфраструктури, зменшенні заторів і аварійності, а також у створенні єдиної транспортної системи. Незважаючи на очевидні переваги цих технологій, у статті визначено, що загрози кібербезпеки становлять значні ризики для безпеки та ефективності CAV. З'ясовано, що зростаюча інтеграція автоматизованих і мережевих систем розширює можливості для злочинних суб'єктів використовувати вразливості, ставлячи під загрозу безпеку CAV. Для вирішення цієї проблеми у дослідженні проводиться класифікація загрози кібербезпеці на чотири окремі групи: атаки на VANET мережу транспортного засобу; атаки, спрямовані на інфраструктуру сенсорів; атаки спрямовані на апаратне забезпечення та зловмисні атаки. Ці класифікації відповідають різним комунікаційним мережам і системам, на які націлені зловмисники. У статті також розкривається потенціал ескалації кібератак, як додаткової загрози, характерної для взаємопов'язаного середовища CAV. Розглядаються сучасні стратегії протидії, призначені для захисту цих транспортних засобів. Розкриваючи ключові моменти, стаття заглиблюється в атаки супротивника на автономні транспортні засоби, висвітлюючи їхні наслідки і підкреслюючи нагальну потребу в більш комплексних захисних механізмах. Наголошується, що подальші дослідження в напрямку підвищення кібербезпеки транспортних засобів, а також суміжної інфраструктури сприятимуть підвищенню безпеки в цілому, підвищенню універсальності CAV та забезпеченню відповідності новим вимогам сучасних транспортних систем.

Ключові слова: *мережеві та автономні транспортні засоби, автомобільна мережа, кібератаки, захист автотранспорту, кіберфізичні системи.*

Постановка проблеми. Протягом останнього десятиліття автомобільна індустрія пережила суттєвий технологічний прорив, що змінив традиційне уявлення про безпеку транспортних засобів. Сучасні автомобілі інтегрують складні системи, які поєднують механічні, електронні та програмні компоненти. Зростання кількості електронних пристроїв і використання бездротових технологій суттєво підвищили рівень автоматизації й підключення транспортних засобів. Водночас зростає популярність створення транспортних мереж (VN – vehicular networks) [1] і мережевих автономних транспортних засобів (CAV – connected and autonomous vehicles) [2], що відкриває нові можливості для підвищення ефективності та безпеки, але водночас створює серйозні загрози кібербезпеці. Розвиток CAV характеризується стрімким зростанням глобального ринку. Очікується, що до 2050 року ринкова вартість цього сегмента досягне 7 трильйонів доларів США [3]. Інтенсивна конкуренція між провідними автовиробниками й технологічними компаніями стимулює дослідження й упровадження нових підходів до створення автономних транспортних засобів. Різноманітні дослідницькі програми, що реалізуються на міжнародному рівні, акцентують увагу на важливому економічному та соціальному потенціалі мережевих та автономних транспортних засобів (CAV). Однак поряд із перевагами, такими як оптимізація логістики, зменшення викидів і підвищення рівня безпеки на дорогах, мережеві й автономні транспортні системи створюють значні загрози, пов'язані із захистом конфіденційності, цілісності та доступності інформації [4]. Головною загрозою для CAV є кібербезпека. Підвищення рівня підключення транспортних засобів до мережі збіль-

шує ризик несанкціонованого втручання в їхню роботу. Зловмисники можуть взяти під контроль автомобіль або його аксесуари, отримати доступ до конфіденційних даних користувачів чи змінити цілісність переданих даних. Вважається, що основними векторами атак стають бездротові технології зв'язку та обмін даними. Проблеми безпеки CAV зосереджуються на трьох ключових аспектах: захист конфіденційності користувацьких даних, забезпечення цілісності переданих і отриманих даних, а також безпеці електронних блоків управління (ECU – electronic control units) [5]. Сучасні стандарти в автомобільних системах зв'язку та обміну даними часто не відповідають усталеним нормам кібербезпеки, що зумовлено обмеженнями апаратного забезпечення та змінами в мережевій архітектурі. Недостатній захист хоча б одного компонента системи може викликати суттєві порушення безпеки, що ставить під загрозу як сам автомобіль, так і його користувачів. Актуальність досліджень кібербезпеки мережевих транспортних засобів обумовлена зростаючим числом кіберзагроз і складністю атак, які з часом стають дедалі витонченішими. З метою досягнення безпечного використання CAV необхідно розробляти нові методи захисту, враховуючи сучасні вразливості та способи їх подолання. Безпечні транспортні засоби є ключовим компонентом для успішного впровадження сервісів CAV і подальшого розвитку транспортних мереж.

Аналіз останніх досліджень і публікацій. Очікується, що майбутні мережеві та автономні транспортні засоби досягнуть високого рівня автоматизації, а основні функції водіння повністю контролюватимуться сучасними системами. Хоча цей прогрес надає значні переваги, він також створює широкий спектр вразливостей у сфері безпеки та конфіденційності. Зростаюча взаємопов'язаність цих транспортних засобів створює нові можливості для зловмисників використовувати слабкі місця системи. Задокументовані випадки кібератак на мережеві транспортні засоби спричинили значні відкликання та змусили виробників посилити протоколи безпеки.

Результати недавніх досліджень свідчать про суттєві успіхи у виявленні та аналізі загроз безпеці, що стосуються мережевих і автономних транспортних систем. В дослідженні [6] увага приділяється аналізу вразливостей систем допомоги водієві (ADAS – advanced driver assistance systems) при атаках на мережу CAN (controller area network). Автори показують, що шляхом маніпуляції даними в мережі CAN можливо порушити функціональність адаптивного круїз-контролю (ACC – adaptive cruise control), що потенційно може призвести до небезпечних ситуацій на дорозі. У своєму дослідженні вони використовували промислове програмне рішення для ADAS, пропонуючи практичне розуміння вразливостей, пов'язаних з комунікаціями по шині CAN, та їхніх наслідків для систем, критично важливих для безпеки. У роботах [7, 8] автори досліджували архітектурний дизайн та інтеграцію різних сенсорних систем в автономних транспортних засобах (AVs – autonomous vehicles). Їхнє дослідження висвітлює проблеми об'єднання сенсорів, підкреслюючи необхідність надійних фреймворків, які забезпечують безперешкодну інтеграцію гетерогенних джерел даних для підвищення продуктивності безпілотного автомобіля. У роботі [9] проведено всебічний огляд досягнень у технологіях сприйняття і зондування, що мають вирішальне значення для досягнення безпечних і ефективних операцій в CAV. Їхні висновки акцентують увагу на важливості інноваційних сенсорних системах, здатних протистояти потенційним кіберзагрозам, зберігаючи при цьому високу точність в динамічному середовищі. Авторами в роботі [10] запропоновано складну систему бортових сенсорів, яка використовує поєднання багатоцільових компонентів і компонентів які оперують інформацією від багатьох джерел, створюючи більш стійку і адаптивну систему сприйняття. Ця система покращує ситуаційну обізнаність і зменшує вразливість, пов'язану з ізольованими сенсорними атаками. Аналогічно, в роботі [11] представлено детальний аналіз п'ятишарової архітектури для CAV. В їхньому дослідженні описується ієрархічний підхід, який об'єднує рівні зондування, зв'язку, обчислень, управління і додатків, забезпечуючи надійну основу для пом'якшення потенційних порушень безпеки. Хоча ці дослідження роблять значний внесок у розумінні вразливостей CAV, інші автори приділили увагу критично важливим бездротовим технологіям, які полегшують передачу даних. В роботі [12], окреслено стратегії розподілу ресурсів, характерні для виділеного зв'язку малої дальності (DSRC – dedicated short range communication) і технологій «мобільний транспортний засіб до всього» (C-V2X – cellular vehicle-to-anything). У їхній роботі підкреслюється необхідність безпечного та ефективного управління ресурсами для зменшення ризиків, притаманних автомобільним комунікаційним мережам. Крім того, зловмисні атаки, спрямовані на CAV, були в центрі уваги кількох досліджень. В роботі [13] проаналізували наслідки шкідливих кібера-

так, надаючи уявлення про потенційні стратегії пом'якшення наслідків. В роботі [14] дослідники розглянули конкретні реальні сценарії атак, пропонуючи детальний аналіз методів використання експлойтів та їхніх наслідків для автомобільних систем. Цей аналіз підкреслює актуальність розробки проактивних заходів безпеки для протидії постійно мінливому ландшафту кіберзагроз для CAV.

Постановка завдання. Швидкий розвиток технологій CAV створює нові загрози в галузі кібербезпеки. Відсутність детального аналізу різного типу атак на CAV, який би описував їх особливості та вплив на CAV, ускладнює проведення аналізу та обмежує можливості для розробки ефективних систем протидії зловмисним атакам. Мета даної роботи полягає в проведенні комплексного аналізу сучасних кіберзагроз для CAV з метою: зведення відомостей про кібератаки на CAV в єдину структуру, що дозволить ідентифікувати прогалини в існуючих дослідженнях; аналізу технічних аспектів реалізації атак, включаючи методи проникнення, використання вразливостей та впливу на компоненти CAV; визначення потенційних наслідків різних типів атак для безпеки руху, конфіденційності даних та доступності функціоналу транспортних засобів; формулювання практичних рекомендацій щодо підвищення рівня кібербезпеки.

Виклад основного матеріалу. На відміну від традиційних транспортних засобів, AVs працюють у високо взаємопов'язаній екосистемі, покладаючись на безперебійний зв'язок із зовнішніми мережами, що включають інші транспортні засоби, придорожню інфраструктуру та централізовані хмарні сервіси. Хоча така взаємопов'язаність підвищує ефективність і безпеку, вона одночасно створює середовище для атак, забезпечуючи потенційні точки входу для зловмисників [15]. Така дуальність мережевих систем підкреслює гостру потребу в надійних заходах кібербезпеки.

Суттєвою відмінністю AVs є їхня залежність від обробки величезних обсягів даних для підтримки таких функцій, як навігація, прийняття рішень і розпізнавання об'єктів. Ці потоки даних часто включають зображення і дані з датчиків, які є особливо вразливими до ворожих атак. Алгоритмами глибокого навчання, які широко використовуються для обробки зображень в AVs, можна маніпулювати. І як результат – система неправильно інтерпретує навколишнє середовище. Зі збільшенням обсягу оброблюваних даних зростає ймовірність такого втручання, що збільшує ризик хибних спрацьовувань і збоїв у роботі системи. Ця вразливість посилюється обмеженнями в надійності сучасних моделей машинного навчання і проблемами забезпечення цілісності даних у реальному часі в різних умовах експлуатації. Крім того, початковий етап розвитку технологій відеоспостереження, як в апаратній, так і в програмній сферах значно підвищує їхню вразливість до кіберзагроз. Апаратні компоненти, такі як датчики та модулі зв'язку, можуть містити вразливості, які можна використати, через недоліки конструкції або недостатньо захищене програмне забезпечення. Аналогічно, програмна архітектура антивірусів, що складається з операційних систем, програмного забезпечення та прикладних рівнів, надає численні можливості для втручання. Зловмисники можуть використовувати ці вразливості для порушення роботи, маніпулювання поведінкою автомобіля або викрадення конфіденційних даних користувача. Особливо небезпечним вектором атак є зовнішні інтерфейси зв'язку автомобілів. Зв'язок «транспортний засіб – все» (V2X – vehicle-to-everything), що охоплює взаємодію «транспортний засіб – транспортний засіб» (V2V – vehicle-to-vehicle) та «транспортний засіб – інфраструктура» (V2I – vehicle-to-infrastructure), має головне значення для забезпечення спільного водіння та управління дорожнім рухом. Однак ці канали зв'язку дуже вразливі до підміни, атак типу «людина посередині» та ін'єкції даних. Відсутність стандартизованих протоколів шифрування та автентифікації для V2X-комунікацій ще більше ускладнює проблему, підкреслюючи значну прогалину в існуючих системах безпеки. Крім внутрішніх технологічних слабкостей, AVs стикаються з зовнішніми загрозами, пов’язаними з мінливістю та непередбачуваністю умов дорожнього руху, що ускладнює забезпечення їхньої надійності.

Загрози кібербезпеки для AV можна класифікувати на чотири основні категорії (наведено на рис. 1): атаки на мережеві протоколи, маніпуляції з сенсорними даними, пошкодження апаратних компонентів та прямі фізичні атаки.

Спектр атак на мережі VANET (vehicular ad-hoc network) досить широкий і включає в себе як зовнішні, так і внутрішні загрози. Одним із найпоширеніших методів є атаки на механізми автентифікації, які дозволяють зловмисникам підробляти ідентифікатори транспортних засобів та отримувати несанкціонований доступ до мережі. Важливими компонентами механізмів безпеки в CAV є – паролі та криптографічні ключі, що діють як захист від несанкціонованого доступу. Однак,

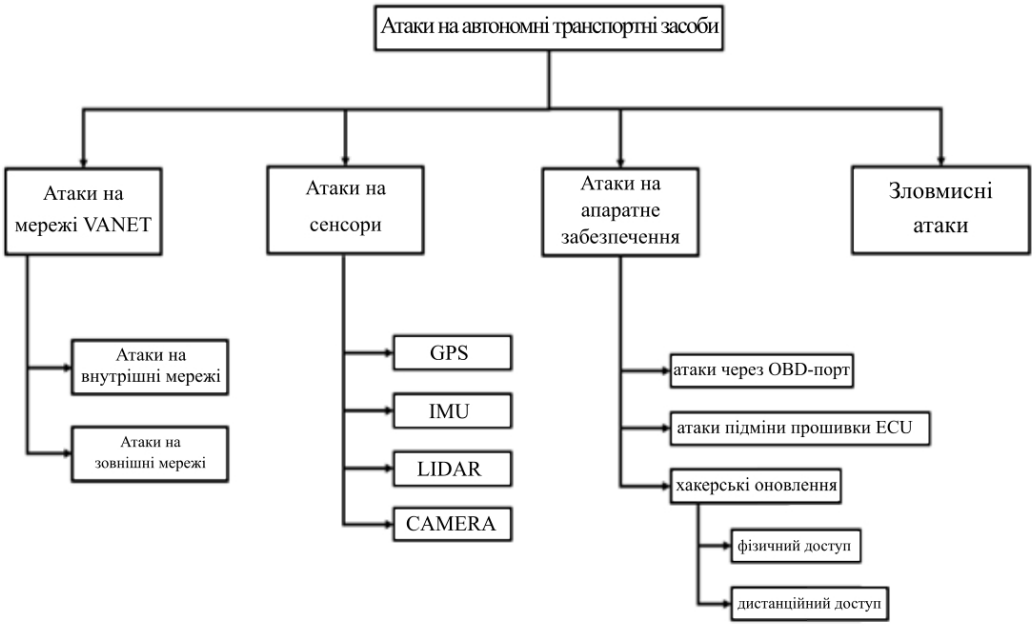

Рис. 1. Потенціальна атаки на мережеві та автономні транспортні засоби

ці механізми не є невразливими до кіберзагроз. Зловмисники часто використовують вразливості в системах, що базуються на ключах і паролях, використовуючи такі методи, як атаки грубої сили, коли робляться багаторазові спроби вгадати або обійти облікові дані для автентифікації [16]. Такі методи є особливо проблематичними для систем, що використовують інфрачервону технологію, оскільки вони можуть бути вразливими до таких атак після серії невдалих спроб, що призводить до несанкціонованого доступу. Атаки грубої сили не тільки ставлять під загрозу безпеку автомобіля, але й створюють значні ризики для конфіденційності користувачів. Після того, як пароль автомобіля зламаний, конфіденційна особиста інформація, така як історія поїздок, вподобання користувача та контактні дані, що зберігаються в системі автомобіля, може стати доступною. Ця проблема стає ще більш гострою через дедалі ширшу інтеграцію технології Bluetooth у транспортні засоби. Порушення з'єднання Bluetooth, навмисне чи випадкове, може слугувати вектором для використання слабких місць у системі безпеки, потенційно надаючи неавторизованим користувачам доступ до персональних даних або контроль над системами транспортного засобу. Ризик, пов'язаний з такого типу атаками, показує необхідність застосування сучасних заходів безпеки. Такі технології, як багатофакторна автентифікація (MFA – multi-factor authentication), біометрична верифікація та динамічна генерація паролів, можуть значно підвищити стійкість цих систем. Більше того, включення систем моніторингу в режимі реального часу і виявлення втручань в спеціальні мережі на базі транспортних засобів (VANET) може забезпечити додатковий рівень захисту, виявляючи і зменшуючи потенційні спроби грубого злому ще до того, як вони стануть успішними.

До зовнішнього типу атак відносяться атаки на мережі V2X, яка інтегрує зв'язок зі смартфонами, хмарними сервісами та іншими пристроями [17]. Функціональність V2X підтримується кількома протоколами зв'язку, такими як Dedicated Short Range Communication (DSRC), IEEE 802.11p та Wireless Access in Vehicle Environments (WAVE). Стандарт DSRC, створений для роботи на частоті 5,9 ГГц з пропускною здатністю 75 МГц, спеціалізується на забезпеченні зв'язку між транспортними засобами. Водночас, протоколи IEEE 802.11p та WAVE, будучи більш універсальними, знайшли своє застосування у V2X-системах, забезпечуючи ширший спектр можливостей для обміну даними між автомобілями та інфраструктурою. Незважаючи на свою спеціалізовану природу, ці протоколи мають спільні вразливості, які роблять їх вразливими до потенційних атак. Наприклад, зловмисники можуть атакувати такі критичні операції, як обгін, зміна смуги руху та обмін даними під час комунікації між транспортними засобами (V2V). Однією з поширених загроз є атака з використанням підробленого ідентифікатора, коли зловмисник використовує підроблений ідентифікатор для

встановлення зв'язку з автомобілем-мішенню. За допомогою цього обману ворожий суб'єкт може передавати та отримувати шкідливі дані, захоплюючи конфіденційну інформацію для зловмисних цілей [16]. Цей тип атак ускладнюється використанням незашифрованих і незахищених протоколів зв'язку, які дозволяють зловмисникам підслуховувати розмови V2V. Такі вразливості можуть призвести до перехоплення конфіденційних даних, таких як ключі автентифікації, які згодом можуть бути використані в подальших атаках. У мережах V2I ризики ще більше зростають. Встановлення з'єднання з базовою станцією створює двосторонній канал зв'язку, що наражає транспортні засоби на потенційні загрози з боку підконтрольних зловмисникам інтелектуальних дорожніх знаків або вузлів стільникових мереж. Зловмисники можуть використовувати ці з'єднання для отримання несанкціонованого доступу до мережі автомобіля, включаючи його електронні блоки керування. Такий доступ не лише загрожує цілісності систем автомобіля, але й ставить під загрозу безпеку та конфіденційність користувачів. Для усунення цих вразливостей слід використовувати стійкі протоколи шифрування, механізми автентифікації в режимі реального часу та вдосконалені системи виявлення вторгнень.

Однією з найсерйозніших загроз для CAV, які підключені до Інтернету є розподілені атаки на відмову в обслуговуванні (DDoS – Distributed Denial of Service). Ці атаки спрямовані на порушення роботи системи шляхом перевантаження мережевих сервісів за допомогою безлічі шкідливих запитів або векторів атаки. Надмірний трафік, що генерується під час DDoS-атаки, призводить до сильного перевантаження мережі, що часто призводить до погіршення або повної відмови критично важливих функцій транспортного засобу. Цей тип збоїв може завдати значної шкоди транспортній інфраструктурі та спричинити значні операційні проблеми. Наслідки таких атак виходять за рамки простих перебоїв в обслуговуванні. Втручання в роботу систем зв'язку та управління CAV створює значний ризик виникнення аварійних ситуацій, що може призвести до катастрофічних наслідків для безпеки як пасажирів, так і оточуючих. Зокрема, DDoS-атаки становлять серйозну загрозу, оскільки можуть призвести до відмови критично важливих систем. Для мінімізації ризиків необхідно розробляти ефективні системи виявлення аномалій та впроваджувати технології адаптивної фільтрації мережевого трафіку.

Серед найпоширеніших загроз для AV можна виділити атаки, спрямовані на втручання в роботу сенсорів:

– система глобального позиціонування (GPS) є основою для ідентифікації та навігації транспортних засобів, використовуючи точні дані геолокації. Поширення супутникових систем позиціонування GPS та відкритий доступ до їхніх даних, хоча й сприяли розвитку навігаційних технологій, проте суттєво підвищили ризик кібератак. Зловмисники можуть спотворювати GPS-сигнали, що призводить до неточностей у визначенні місцезнаходження та, як наслідок, створює загрозу для безпеки як окремих користувачів, так і цілих транспортних систем. Зловмисники можуть використовувати дані з відкритим доступом для маніпулювання навігацією, передаючи спотворені сигнали. Такий метод, відомий як підміна GPS. Це передбачає трансляцію фальшивих сигналів, які є потужнішими за справжні, що призводить до того, що транспортні засоби неправильно інтерпретують своє місцезнаходження і відхиляються від запланованих маршрутів. Аналогічно, глушіння GPS виводить систему з ладу, переповнюючи її шумовими сигналами. Обидва види атак становлять значну загрозу для безпеки пасажирів, порушуючи роботу системи навігації та управління транспортним засобом [18];

– інерційний вимірювальний блок (IMU – inertial measurement unit), що складається з гіроскопа та акселерометра, вимірює швидкість, прискорення та орієнтацію транспортного засобу. IMU також відстежує динаміку навколишнього середовища, наприклад, градієнти. Зловмисники можуть змінити або пошкодити дані датчиків, маніпулюючи показниками нахилу дороги. Наприклад, зловмисник може фальсифікувати дані про нахил, змушуючи транспортний засіб надмірно сповільнюватися на рівній місцевості. Ця маніпуляція не тільки порушує роботу транспортного засобу, але й впливає на навколишній рух, що потенційно може призвести до заторів або аварій;

– системи виявлення світла і визначення дальності (LiDAR) – полегшують локалізацію, виявлення перешкод і уникнення зіткнень, вимірюючи час, необхідний для відбиття світла від об'єктів. Ці системи є високоефективними, але чутливими до перешкод сигналу. Зловмисники можуть скористатися цим, передаючи схожі сигнали, змушуючи автомобіль неправильно ідентифікувати об'єкти або сприймати неіснуючі перешкоди. Такі атаки можуть змусити транспортні засоби надмірно сповільнитися або зупинитися, порушуючи транспортний потік і наражаючи на небезпеку пасажирів;

– моноскопічні та стереоскопічні камери – виконують такі важливі завдання, як визначення смуги руху, розпізнавання дорожніх знаків та

ідентифікація перешкод. Однак вони вразливі до цілеспрямованих атак. Наприклад, інтенсивні джерела світла, такі як фари дальнього світла або фари зустрічного автомобіля, можуть перевантажити датчики камери. Це може призвести до хибних спрацьовувань або збоїв у розпізнаванні об'єктів, що підвищує ризик аварій. Більше того, CMOS датчики, що використовуються в камерах, можуть зазнати пошкоджень від надзвичайно яскравого світла, що робить систему неефективною.

Окрему категорію становлять атаки, спрямовані безпосередньо на апаратне забезпечення транспортних засобів:

− атаки через OBD-порт – більшість транспортних засобів оснащуються портом бортової діагностики (OBD), що дозволяє отримувати діагностичні дані та дані про функціонування. Цей інтерфейс забезпечує зв'язок між електронними блоками керування (ECU) автомобіля через шину CAN. Пристрій OBD підключається до комп'ютера через USB або Bluetooth, що полегшує діагностику. Однак ця функція становить значний ризик для кібербезпеки. Зловмисники можуть використовувати інтерфейс OBD для доступу до електронних блоків керування автомобілем, пошкоджуючи мережу. Ця вразливість підкреслює необхідність надійного контролю доступу та механізмів шифрування для таких інтерфейсів;

− атаки на прошивку електронних блоків керування (ECU, engine control units) – сучасні транспортні засоби покладаються на численні електронні блоки управління, кожен з яких відповідає за управління певними підсистемами. Хоча прошивка ECU є захищеною і розроблена з метою безпеки, зловмисники все частіше застосовують методи перепрошивки ECU шкідливою прошивкою. Ця форма атаки з прямим доступом передбачає, що зловмисник отримує фізичний доступ до ECU, використовуючи зовнішні інтерфейси для модифікації прошивки та зміни поведінки ECU. Превентивні стратегії включають впровадження протоколів автентифікації для оновлення програмного забезпечення, використання методів хешування для перевірки цілісності прошивки та захист пам'яті ECU від несанкціонованих змін або підміни ключів безпеки;

− несанкціоновані оновлення прошивки часто не містять критично важливих виправлень безпеки, що робить транспортні засоби вразливими до кібератак, здатних вилучати конфіденційні дані або встановлювати шкідливе програмне забезпечення. Несанкціоновані оновлення можуть бути впроваджені двома основними способами:

− фізичний доступ – зловмисники можуть перевантажити фізичні рівні або втрутитися в окремі модулі, такі як датчики та комунікаційні інтерфейси, створюючи вразливості;

− віддалені атаки використовують такі мережі, як WiFi, Bluetooth і стільниковий зв'язок (наприклад, 4G). У деяких випадках пряме з'єднання між ECU та CAN-шиною збільшує ризик порушення роботи через шкідливий код, введений через прошивку з доступом до Інтернету.

До числа найпоширеніших загроз безпеки CAV належать зловмисні атаки. Для забезпечення безпеки автономних транспортних засобів важливою є точна ідентифікація об'єктів на дорозі. Глибоке навчання, завдяки своїй здатності до імовірнісної оцінки, дозволяє з високою вірогідністю класифікувати різноманітні об'єкти, такі як пішоходи, транспортні засоби та дорожні знаки. Цей підхід дозволяє AV ефективно інтерпретувати навколишній світ і приймати безпечні рішення, необхідні для автономного руху. Однак нейронні мережі (DNN, Deep Neural Networks) чутливі до ворожих атак – цілеспрямованих кіберзагроз, коли незначні зміни вхідних даних змушують модель приймати помилкові рішення. Такі ворожі атаки використовують вразливі місця в DNN, що потенційно загрожує безпеці та функціональності штучного інтелекту. Наприклад, незначні модифікації фізичних об'єктів, такі як відповідно розміщені наклейки на знаках зупинки, можуть ввести в оману алгоритми розпізнавання дорожніх знаків, змушуючи їх неправильно ідентифікувати критичні символи. Це показує, як ворожі атаки можуть перетворити, здавалося б, нешкідливі зміни на небезпечні помилки в роботі AV-систем.

Висновки. Аналіз сучасного стану безпеки мережевих та автономних транспортних засобів (CAV) свідчить про зростання різноманітності та складності кіберзагроз. Складність систем CAV, що об'єднують механічні, електронні та програмні компоненти, створює сприятливе середовище для атак різного типу. Особливу увагу заслуговують вразливості систем безключового доступу, які можуть бути використані для несанкціонованого доступу до транспортного засобу, а також атаки на зарядну інфраструктуру електромобілів, що відкривають нові шляхи для проникнення зловмисників. Розмаїття виробників обладнання та відсутність єдиних стандартів безпеки ускладнюють процес забезпечення кібербезпеки CAV. Незважаючи на це, нові технології, такі як штучний інтелект та машинне навчання, відкривають нові можливості для розробки ефективних систем захисту. Однак, паралельно з розвитком захисних засобів, з'являються нові вектори атак, що підкреслює необхідність постійного моніторингу та адаптації стратегій кібербезпеки.

Список літератури:

1. Olariu S., Weigle M.C. Vehicular networks: from theory to practice. Chapman and Hall/CRC, New York, 2009, p.472.
2. Kopelias P., Demiridi E., Vogiatzis K., Skabardonis A., Zafiropoulou V. Connected & autonomous vehicles–Environmental impacts–A review. Science of the total environment, 712, 2020, p.135237-135251.
3. Thierer A., Castillo A. Projecting the growth and economic impact of the internet of things, George Mason University, Mercatus Center, 15, 2015, pp.158-169.
4. Pype P., Daalderop G., Schulz-Kamm E., Walters E., Grafenstein M.V. Privacy and security in autonomous vehicles., Automated driving, Cham., 2016, pp. 17-27.
5. David C., Fry S. Automotive security best practices, Intel Security, 2016, p.17.
6. Hoque M.A., Hasan R. Exposing adaptive cruise control in advanced driving assistance systems, 8th WF-IoT, IEEE, 2022, pp. 1-6.
7. Zong W., Zhang C., Wang Z., Zhu J., Chen Q. Architecture design and implementation of an autonomous vehicle, IEEE Access 6, 2018, pp.21956-21970.
8. Wang Z., Wu Y., Niu Q. Multi-sensor fusion in automated driving: a survey, IEEE Access 8, 2019, pp.2847-2868.
9. Llorca D.F., Daza I.G., Parra N.H., Alonso I.P. Sensors and Sensing for Intelligent Vehicles, 2020, pp. 5115-5123.
10. Xiao Z., Yang D., Wen F., Jiang K. A unified multiple-target positioning framework for intelligent connected vehicles, Sensors, 19 (9), 2019, pp.1967-1988.
11. Kaiwartya O., Abdullah A.H., Cao Y., Altameem A., Prasad M., Lin C.- T., Liu X. Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects, IEEE Access, 4, 2016, pp.5356-5373.
12. Noor-A-Rahim M., Liu Z., Lee H., Ali G.M.N., Pesch D., Xiao P. A survey on resource allocation in vehicular networks, IEEE Trans. Intell. Transport. Syst., 23 (2), 2020, pp.701-721.
13. Kopencova D., Rak R. Issues of vehicle digital forensics, in: XII International Science-Technical Conference Automotive Safety, IEEE, 2020, pp.1-6.
14. Rak R., Kopencová D. Actual issues of modern digital vehicle forensics, Internet Thinks Cloud Comp., 8 (1), 2020, pp.208-234.
15. Saoudi O., Singh I., Mahyar H. Autonomous Vehicles: Open-Source Technologies, Considerations and Development, Advances in Artificial Intelligence and Machine Learning, 3(1), 2022, pp.669-692.
16. Almeaibed S., Al-Rubaye S., Tsourdos A., Avdelidis N.P. Digital twin analysis to promote safety and security in autonomous vehicles, IEEE Communications Standards Magazine, 5(1) , 2021, pp.40-46.
17. Harvey J., Kumar S. A survey of intelligent transportation systems security: challenges and solutions, IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE, 2020, pp. 263-268.
18. Luo Q., Cao Y., Liu J., Benslimane A. Localization and navigation in autonomous driving: Threats and countermeasures, IEEE Wireless Communications, 26(4), 2019, pp.38-45.

Ciapa S.M. CYBERSECURITY THREATS AND VULNERABILITIES IN CONNECTED AND AUTONOMOUS TRANSPORTATION SYSTEMS

The article is devoted to the study of cybersecurity threats associated with networked and autonomous vehicles (CAVs), a key area of development in the automotive industry. CAVs have the potential to improve the transport industry by providing enhanced road safety, improved accessibility and efficiency of transportation. Despite the significant progress in the development of CAV systems, the issue of their cybersecurity remains relevant. The growing number of networked devices and the increasing complexity of CAV control systems create new opportunities for cyberattacks that can lead to serious consequences. This article reveals the critical role of sensors and network communications in improving automotive infrastructure, reducing congestion and accidents, and creating a unified transport system. Despite the obvious advantages of these technologies, the article identifies that cybersecurity threats pose significant risks to the safety and efficiency of CAVs. It is found that the growing integration of automated and networked systems expands the opportunities for criminal actors to exploit vulnerabilities, jeopardising the security of CAVs. To address this problem, the study classifies cybersecurity threats into four distinct groups: attacks on the vehicle's VANET network; attacks targeting the sensor infrastructure; attacks targeting the hardware; and malicious attacks. These classifications correspond to the different communication networks and systems targeted by attackers. The article also reveals the potential for escalation of cyber attacks as an additional threat inherent in the interconnected CAV environment. It also discusses current countermeasures designed to protect these vehicles. By highlighting the key points, the article delves into adversary attacks on autonomous vehicles, highlighting their consequences and emphasising the urgent need for more comprehensive defence mechanisms. It is emphasised that further research into enhancing the cybersecurity of vehicles and related infrastructure will contribute to improving security in general, increasing the versatility of CAVs and ensuring compliance with the new requirements of modern transport systems..

Key words: *connected and autonomous vehicles, automotive network, cyberattacks, vehicle protection, cyber-physical systems.*