

**Світличний Віталій Анатолійович**

кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності

Харківський національний університет внутрішніх справ, Харків, Україна

ORCID: 0000-0003-3381-3350

E-mail: vit.svet@ukr.net

**ОПТИМІЗАЦІЯ ЗАХИСТУ АВТОМОБІЛЯ ВІД ВИКРАДЕННЯ З УРАХУВАННЯМ ВИМОГ
КІБЕРБЕЗПЕКИ**

Анотація. У статті обґрунтовано вибір скороченого заводського тайм-ауту безключової авторизації у складі узгодженого механічного та електронного захисту автомобіля від викрадення. Застосовано аналіз наукових і нормативних джерел, інтервальне оцінювання часових характеристик, аналітичне виведення умов допустимості порога та функціональне порівняння захисних засобів. Розглянуто механічні бар'єри доступу до електронних блоків і проводки, захист діагностичного роз'єму, незалежний дозвіл запуску й сім напрямів протидії ретрансляції. Основний теоретичний результат — формалізація вибору тайм-ауту за гарантованими межами повної тривалості штатного та ретрансльованого обміну, похибками вимірювання й дискретністю налаштування. Для неперервного порога отримано умову додатного інтервалу розділення; для дискретного порога виведено точну умову наявності допустимого значення. Обґрунтовано вибір порога, що максимізує найменший запас до двох часових меж. На умовних безрозмірних прикладах показано, що додатного часового інтервалу не завжди достатньо за обмеженого кроку налаштування. За додаткового припущення про адитивну затримку ретрансляції отримано достатню умову через її нижню межу та діапазон штатного часу відповіді. Експериментальні дані Francillon та співавторів використано для пояснення співвідношення затримок; їх не подано як власні вимірювання чи універсальні параметри автомобілів. Відомий принцип часової перевірки близькості не заявляється як новий протокол. Практична цінність полягає у процедурі перевірки допустимості зміни тайм-ауту та узгодженні цього рішення з фізичними бар'єрами, захистом цифрових команд, діагностики й оновлень. Положення Правил Організації Об'єднаних Націй (ООН) № 155 і № 156 зіставлено із захисними функціями. Робота має теоретико-аналітичний характер: власних експериментів не проведено, кількісного зниження ймовірності викрадення не заявлено. Визначено припущення моделі, межі застосування та необхідність валідації параметрів конкретної системи перед упровадженням.

Ключові слова: захист автомобіля від викрадення; механічні заходи; електронні заходи; безключовий доступ; автентифікація; ретрансляційна атака; тайм-аут.

ВСТУП

Постановка проблеми. У зв'язку з широким використанням інформаційних технологій кібератаки та спроби несанкціонованого втручання в електронні системи автомобіля можуть створювати передумови його фізичного викрадення. Наслідки таких втручань не обмежуються фінансовими втратами й можуть стосуватися безпеки водія та пасажирів. Системний огляд атак на автомобільну електроніку та заходів протидії представлено в роботі П. Клімушина, В. Світличного, Ю. Гнусова та Ю. Онищенка [1]. Питання кібербезпеки та розширення зовнішніх інтерфейсів автомобіля досліджувалися автором у роботі [2]. Збільшення кількості підключених компонентів потребує оцінки нових шляхів несанкціонованого доступу, проте саме по собі не доводить зниження безпеки кожної конкретної моделі.

Автомобільна кібербезпека є викликом для виробників, розробників електронних компонентів і фахівців з установа охоронних систем. Стандарт ISO/SAE 21434:2021, розроблений Міжнародною організацією зі стандартизації (ISO, International Organization for Standardization) та SAE International (історична назва — Society of Automotive Engineers, Товариство автомобільних інженерів), визначає інженерний підхід до управління кіберризиками електричних та електронних систем протягом життєвого циклу транспортного засобу [3]. Механічний і електронний захист доцільно розглядати взаємопов'язано: доступ до електронного вузла може створювати умови для подальшого втручання, а компрометація



електронної авторизації — полегшувати фізичне проникнення. Тому захист сучасних автомобілів від викрадення потребує постійного вдосконалення.

Аналіз останніх досліджень і публікацій. Огляд Клімушина та співавторів [1] є вихідним джерелом роботи. Попередні праці про технічний захист і кібербезпеку автомобіля [2], [4] визначають практичний контекст поєднання захисних засобів. Checkoway та співавтори [5] досліджували зовнішні поверхні атаки; Francillon, Danev і Capkun [6] експериментально продемонстрували ретрансляцію систем пасивного безключового доступу та запуску (PKES, Passive Keyless Entry and Start) та розглянули часові характеристики й обмеження відстані; Garcia та співавтори [7] дослідили вразливості окремих схем дистанційного безключового доступу (RKE, Remote Keyless Entry). Опис Tindell [8] пояснює введення підроблених повідомлень у мережу контролерів (CAN, Controller Area Network), відоме як CAN injection, а робота Leu та співавторів [9] демонструє необхідність оцінювання конкретної реалізації надширокопasmової технології (UWB, Ultra-Wideband). Отже, сам принцип часової перевірки близькості вже відомий. Завдання цієї статті — оптимізувати процедуру вибору загального тайм-ауту з урахуванням гарантованих часових меж, похибок і дискретності налаштування, а також визначити, коли таке налаштування не забезпечує розділення. Це прикладна формалізація відомого принципу, а не твердження про винайдення нового протоколу.

Мета статті — обґрунтувати вибір скороченого заводського тайм-ауту безключової авторизації у складі узгодженого механічного та електронного захисту автомобіля від викрадення. Завдання: зіставити захисні функції, переваги та обмеження практичних засобів; побудувати інтервальну модель повного обміну; вивести умови допустимості неперервного й дискретного порога; визначити поріг із найбільшим мінімальним часовим запасом; оцінити модель на умовних розрахункових випадках і зіставити її з відомими рішеннями. Оптимізація стосується часового запасу в заданій моделі, а узгодження комплексу — сумісності, безпечності та зручності засобів.

Науковий внесок і практичне значення. Аналітичний результат роботи — процедура вибору тайм-ауту, яка поєднує межі штатної й ретрансльованої авторизації, похибки вимірювання та сітку допустимих налаштувань. Виведено точний критерій існування дискретного порога й правило максимізації мінімального запасу. Практичне значення — можливість перевірити доцільність скорочення тайм-ауту до його застосування та пов'язати часову перевірку з незалежним дозволом запуску і фізичним захистом вузлів. Формули є аналітичними наслідками заявленої моделі; їх математичну форму не подано як новий принцип автентифікації. Власних експериментальних вимірювань у роботі не проводилося.

МЕТОДИКА ДОСЛІДЖЕННЯ

Досліджуваний об'єкт — авторизація доступу та запуску автомобіля у складі механічного й електронного захисту. Предмет — допустимий часовий поріг відхилення ретрансльованої відповіді. Джерела добиралися цільово; бібліографічний аналіз не заявляється як систематичний огляд. Для кожного засобу зіставляються захисна функція, сценарій обходу та обмеження сумісності. Теоретичний аналіз використовує гарантовані інтервали часу й обмежені похибки без припущення про їх імовірнісний розподіл. Критерій оптимізації — найбільший мінімальний запас між установленим порогом і двома часовими межами. Якісне оцінювання доповнено точними розрахунками умовних безрозмірних випадків. Вони перевіряють поведінку формул, а не характеристики серійного автомобіля. Параметри конкретної PKES-системи в цій роботі не встановлюються.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасні підключені автомобілі, по суті, є частиною Інтернету речей (IoT, Internet of Things). Ці транспортні засоби можуть отримувати дані та надсилати їх, завантажувати оновлення програмного забезпечення й підключатися до інших пристроїв IoT через Інтернет або бездротову локальну мережу (WLAN, Wireless Local Area Network). Вони можуть надавати своїм користувачам розширені можливості підключення та інформаційно-розважальні функції, а також сприяти безпечнішому водінню. Однак підключення автомобіля до телекомунікаційних мереж потребує захисту зовнішніх інтерфейсів [5]. Поняття підключеного й автономного автомобіля не є тотожними.

Початок цифровізації автомобіля пов'язаний із поступовим упровадженням електронного запалювання, антиблокувальних систем і електронного керування двигуном. Надалі компоненти ставали не лише електронними, а й мережними: окремі блоки почали обмінюватися повідомленнями для узгодженого виконання функцій.

Важливим початком цифрової революції в автомобільних технологіях можна вважати лютий 1986 р., коли на конгресі автомобільних інженерів (SAE) компанія Robert Bosch GmbH представила цифровий



мережний протокол комунікації електронних компонентів автомобіля CAN — Controller Area Network [10]. CAN забезпечує послідовний обмін повідомленнями між вузлами; у поширених високошвидкісних реалізаціях застосовується двопровідна диференціальна лінія. Несанкціоноване втручання в обмін даними може здійснюватися через фізичний доступ до відповідної мережі або через підключені мультимедійні й комунікаційні компоненти. Крім різновидів CAN, сьогодні використовуються FlexRay, LIN (Local Interconnect Network — локальна мережа взаємоз'єднання), MOST (Media Oriented Systems Transport — мережа передавання мультимедійних даних) та Automotive Ethernet відповідно до завдань і конструкції системи. Під час проєктування автомобілів застосовуються технології Drive by Wire, які замінюють певні механічні зв'язки електронними. До відповідних функцій належать електронна педаль акселератора, окремі реалізації гальмового й кермового керування, електронне перемикання передач і системи паркування. Обсяг такого заміщення та умови безпечного виконання визначаються конкретною конструкцією.

Одним із ранніх прикладів підключених сервісів є телематична система OnStar, історія якої починається у 1996 р. Вона забезпечувала зв'язок з оператором служби допомоги у випадку аварії [11]. Надалі розвивалися віддалена діагностика, звіти про стан бортових систем і взаємодія смартфонів з автомобілями. На сьогодні в автомобільній індустрії кібербезпека забезпечується як апаратними, так і програмними рішеннями. Її забезпечення ускладнюється особливостями автомобільної архітектури:

а) існують численні електронні блоки керування (ЕБК), з'єднані електронними шинами, які відповідають за різні функції та характеристики; навіть в одній моделі кількість ЕБК може різнитися залежно від комплектації;

б) існує множина потенційних точок доступу як розташованих усередині автомобіля, так і віддалених, зокрема: OBD-II (On-Board Diagnostics II — бортова діагностика другого покоління), USB (Universal Serial Bus — універсальна послідовна шина) та SD (Secure Digital — формат карт пам'яті), безключовий доступ, Bluetooth і Wi-Fi, вбудований модем, інформаційно-розважальна система або застосунок для смартфона, а також підключення до телематичних і хмарних сервісів [5]. Доступ до одного інтерфейсу не обов'язково означає доступ до всіх функцій автомобіля.

Частина підключених моделей автомобілів має вбудовані картки ідентифікації абонента (SIM, Subscriber Identity Module) або їх вбудований різновид eSIM (embedded SIM). Вони використовуються для передавання телематичних даних, зв'язку з хмарними сервісами, створення точок доступу Wi-Fi та отримання інформації про дорожні умови. Прикладами серверних застосунків є сервіси, які залежно від комплектації та активованої послуги можуть підтримувати дистанційний запуск, замикання й відмикання автомобіля або передавання його стану. Захист таких функцій потребує контролю облікових записів і дозволів.

Система передавання радіоданих RDS (Radio Data System) використовується для вбудовування невеликих обсягів цифрової інформації у мовлення з частотною модуляцією (FM, Frequency Modulation). Зазвичай передаються назва радіостанції та службові дані. Використовуючи канал повідомлень про дорожній рух RDS-TMC (Radio Data System — Traffic Message Channel), сумісна автомобільна система може отримувати повідомлення про дорожній рух, які відображаються на головному пристрої. Наявність зовнішнього інформаційного каналу потребує перевірки оброблення його даних, але сама по собі не доводить можливості викрадення.

Bluetooth і Wi-Fi поширені в автомобілях. Мобільні телефони користувачів підключаються через Bluetooth до головного пристрою для відтворення музики, телефонних дзвінків і доступу до адресних книг. Залежно від конструкції автомобіль може підключатися до мереж Wi-Fi та завантажувати пакети оновлення програмного забезпечення через бездротову мережу (OTA, Over-the-Air — передавання «по ефіру»). Окремі автомобілі можуть створювати точки доступу Wi-Fi для доступу до Інтернету через вбудований модем. Безпека залежить від налаштувань, актуальності програмного забезпечення й контролю доступу.

Отже, з упровадженням телекомунікаційних технологій автомобільна телематика перейшла від телефонних дзвінків та доступу до адресних книг до надання користувачам доступу до застосунків, карт, повідомлень і музики. Apple CarPlay та Android Auto забезпечують інтеграцію сумісного смартфона з автомобільною системою. Розширення цих можливостей потребує оцінки шляхів оброблення зовнішніх даних і дозволів; воно не є автоматичним доказом відкритого доступу злоумисника.

Таким чином, сьогодні питання кіберзахисту мають важливе значення, а серед них окремо стоїть захист автомобілів від викрадення. Сучасні автомобілі — це складні технічні комплекси; виробники охоронних систем постійно впроваджують нові опції, щоб підвищувати рівень їх захисту. Злоумисники вдосконалюють наявні й створюють нові способи обходу. Тому доцільно розглянути, якими засобами можна ускладнити викрадення конкретного автомобіля.

У попередній роботі В. А. Світличного [4] наголошено на необхідності комплексного використання



механічних та електронних засобів. Практичний зміст цього підходу полягає в ускладненні несанкціонованого проникнення та запуску автомобіля, а також у підтримці своєчасного виявлення й реагування.

Розглянемо два типи заходів захисту: механічні створюють фізичну перешкоду доступу або переміщенню; електронні контролюють доступ, охорону й дозвіл запуску та забезпечують захист цифрових команд і програмного забезпечення. До електронних заходів віднесено апаратні, програмні та криптографічні механізми. Поділ є функціональним: електромеханічний замок, наприклад, поєднує фізичний бар'єр з електронним керуванням.

1. Механічні заходи захисту від викрадення: можливості, обмеження та вдосконалення

Кожен відповідальний автовласник дбає про безпеку своєї машини й шукає способи захисту від викрадення. Розробники постійно вдосконалюють системи безпеки, але й викрадачі шукають способи обійти їх. Проте відсутність абсолютної гарантії не означає відсутності сенсу в захисних заходах. Необхідно розумно підходити до захисту автомобіля, поєднуючи бар'єри, які ускладнюють різні дії зловмисника.

Власники старих, уживаних автомобілів іноді вважають, що недорогі машини не становлять інтересу для злочинців. Такі автомобілі можуть залишатися без додаткових охоронних систем. Однак вартість не є єдиним чинником ризику: значення мають стан захисту, доступність компонентів та умови зберігання. Твердження про більшу частоту викрадень певної цінової категорії потребує окремої статистики.

Механічне проникнення може включати пошкодження скла чи замків, доступ до підкапотного простору та спробу відключити охоронний компонент або його живлення. Тому доцільно оцінювати не лише міцність дверного замка, а й доступність електронних блоків, проводки та джерел живлення охоронної системи.

Для ускладнення механічного проникнення й подальшого викрадення розглянемо наступні напрями захисту.

Одним із допоміжних методів є *зміна розташування індикаторного світлодіода та прихований монтаж блока сигналізації*. Зміна прокладання комутаційних дротів дозволяє розмістити блок у менш передбачуваному для зловмисника місці. Проте зміна кольору або режиму індикації сама по собі не доводить стійкості захисту. Монтаж має зберігати надійність електричних з'єднань і можливість обслуговування.

Наступна група методів призначена безпосередньо для захисту електронного блока керування (ЕБК) та діагностичного роз'єму.

Зміна розташування контактів у з'єднувальній колодці (перепінування) може розглядатися як спосіб ускладнити несанкціоновану заміну ЕБК. Проте її наслідки залежать від електричної схеми, а пошкодження підключеного блока не слід визначати як мету захисту. Такий спосіб потребує окремої оцінки сумісності, ремонтпридатності та функціональної безпеки.

Створення міцного захисного корпусу («сейфу») для штатного ЕБК може ускладнити його демонтаж. Кріплення до корпусу автомобіля має перешкоджати несанкціонованому зняттю, водночас зберігаючи необхідний тепловий режим, захист від вологи й можливість сервісних робіт.

Встановлення додаткових замків капота призначене для захисту підкапотного простору, в якому можуть розміщуватися ЕБК та інші охоронювані компоненти. Замки бувають механічними та електромеханічними. Перші відкриваються й закриваються вручну за допомогою окремого ключа, другі можуть підключатися до автомобільної сигналізації. Кількість і розташування точок замикання визначаються конструкцією. При виборі враховуються:

- стійкість механізму й циліндра до несанкціонованого відкривання;
- міцність кріплення та обмеження доступу до приводу замка;
- працездатність за відмови електроживлення та передбачений порядок аварійного відкривання;
- сумісність із конструкцією капота й зручність регламентного обслуговування.

Спеціальні шини запропоновано для протидії використанню пневматичної подушки біля замків капота. Цю пропозицію не можна подавати як загальну рекомендацію без перевірки конструкції, ризику травмування та наслідків для аварійного доступу. Практичним завданням залишається посилення захисту замка й його кріплення.

Додатковий іммобілайзер може формувати окрему умову дозволу запуску двигуна. Установлення розподілених реле або інших виконавчих компонентів потребує перевірки того, які кола вони контролюють і як поведуться за відмови. Кількість реле сама по собі не доводить ефективності захисту.

Діагностичний роз'єм може захищатися засобом контролю доступу, який обмежує несанкціоновані



діагностичні операції в режимі охорони. Після авторизованого переходу до сервісного режиму повинна зберігатися можливість належного обслуговування. Конкретний спосіб блокування визначається архітектурою автомобіля.

Окремою технічною пропозицією є ускладнення запуску через *керовані реле у колах датчиків колінчастого й розподільчого валів*. Її практична реалізація потребує окремих випробувань: не можна без перевірки стверджувати, що втручання не діагностується або не впливає на безпечну роботу двигуна. Для протигугінної функції пріоритетним є керований дозвіл запуску; створення нестабільної роботи чи зупинки двигуна під час руху не розглядається тут як підтверджений безпечний спосіб захисту.

Викрадення за наявності ключів. Втрата або викрадення штатного ключа потребує окремого розгляду: справжній ключ може задовольняти штатну перевірку доступу. Додаткова авторизація здатна створити ще одну умову дозволу запуску. Функції «Антипограбування» та «Паніка» залежать від конкретної системи; звукове оповіщення, заборона наступного запуску й керування вже працюючим двигуном є різними діями. Негайне заглушення двигуна під час руху не слід рекомендувати без документованих умов безпечного виконання.

Маяк глобальної системи позиціонування (GPS, Global Positioning System) або трекер є додатковим засобом пошуку автомобіля. Пристрій розміщується приховано, а режим передавання координат визначається його налаштуваннями. «Сплячий» режим може знижувати активність передавача, проте не гарантує неможливості виявлення. Отримання координат залежить від живлення, доступності супутникового сигналу й каналу зв'язку. Такий засіб підтримує реагування після події, але не замінює заборону несанкціонованого запуску.

Викрадення за допомогою евакуатора. Якщо до захисту автомобіля підходить комплексно, слід враховувати і його примусове переміщення без запуску двигуна. Якщо сигналізація оснащена датчиком нахилу, він може спрацювати при завантаженні, після чого система формує сигнал тривоги за умови доступного каналу зв'язку. Для визначення координат і маршруту може використовуватися GPS-трекер, приховано розміщений у салоні або в іншому придатному місці. Це підтримує пошук після переміщення, але не гарантує повернення автомобіля.

Переваги й обмеження механічних заходів. Фізичний бар'єр не потребує довіри до радіокоманди та може ускладнювати доступ до блоків і проводки навіть після електронного відмикання. Його недоліки — можливість силового руйнування, потреба в коректному монтажі та обслуговуванні, а для ручних пристроїв — залежність від дій власника. Окреме блокування запуску не усуває переміщення евакуатором.

Технічне рішення вдосконалення механічного захисту — узгоджене захищення підкапотного доступу, електронного блока та доступних ділянок проводки. Захисні елементи слід розміщувати так, щоб обхід одного не відкривав одразу всі критичні вузли. Перевіряти потрібно доступність обхідних шляхів, надійність кріплень і можливість штатного обслуговування. Це пропозиція до конструкції конкретного комплексу, а не універсальна схема монтажу.

2. Електронні заходи захисту від викрадення та їх удосконалення

Електронні заходи охоплюють сигналізації, іммобілайзери, штатний і додатковий контроль доступу та запуску. Їх перевага — можливість автоматично контролювати умови дозволу й повідомляти про подію. Обмеження пов'язані з живленням, радіозавадами, обхідними шляхами авторизації та залежністю додаткових систем від штатного підтвердження. Далі розглянуто характерні способи втручання та напрями вдосконалення. До цього типу належать також перевірка цифрових підтверджень і захист програмного забезпечення охоронних систем.

2.1. Радіоканали та електронна авторизація

У цьому підрозділі розглянуто вплив на радіоканали та штатну авторизацію. Глушіння перешкоджає обміну, перехоплення використовує особливості передавання команд, а ретрансляція переносить обмін зі справжнім ключем за межі дозволеної зони.

Глушіння сигналів. Радіозавади можуть перешкоджати доставленню команди замикання або повідомлення тривоги. Якщо власник не перевіряє фактичний стан охорони, недоставлена команда створює небажану невизначеність. Глушіння стільникового або іншого каналу також може обмежити дистанційне сповіщення. При цьому відсутність зв'язку не є доказом зняття охорони: результат залежить від автономної логіки системи.

Режим «активної охорони» може передбачати контроль зв'язку та повідомлення про його втрату. Проте сповіщення має діяти доступним каналом; система не може гарантувати push-повідомлення через той самий заглушений канал. Практичними заходами є перевірка фактичного замикання, автономне виявлення подій і оцінка можливостей резервного зв'язку.

Режим сигналізації Slave. Керування додатковою охоронною системою від штатного ключа зручне для власника. Однак якщо зняття додаткової охорони цілком залежить від штатного підтвердження,



компрометація цього підтвердження може вплинути на обидві системи. Додаткова мітка, персональний ідентифікаційний номер (PIN, Personal Identification Number) або інший засіб авторизації мають формувати окрему перевірку дозволу. Саму наявність двох пристроїв не слід без оцінки реалізації називати двофакторною автентифікацією.

Кодграббери. Цим терміном у практичному описі позначають пристрої, які перехоплюють радіокоманди та використовують особливості конкретної схеми доступу для їх відтворення або формування. Простий запис раніше переданої команди не є достатнім для подолання будь-якої системи зі змінним кодом. Дослідження Garcia та співавторів показує вразливості окремих реалізацій дистанційного доступу [7]. Стійкість залежить від протоколу, ключів і перевірки актуальності; позначення «діалоговий код» саме по собі не підтверджує абсолютної захищеності.

Ретранслятори («вудки»). На відміну від компрометації коду, ретрансляція переносить обмін між автомобілем і справжнім ключем, який перебуває поза очікуваною зоною близькості. Криптографічна перевірка може бути успішною, оскільки відповідає справжній ключ. У дослідженні Francillon, Danev та Саркун продемонстровано доступ і запуск у досліджених PKES-системах [6]. Системи безключового доступу мають різні комерційні назви — Keyless Go, Keyless Entry, Smart Key, Comfort Access тощо; стійкість слід оцінювати за реалізацією, а не за назвою. У Правилах ООН № 155, додатку 5, таблиці B4, загроза 16.1 прямо охоплює дистанційний ключ та іммобілайзер; захід M20 передбачає захист систем дистанційного доступу [12].

На поширення радіосигналу впливають відстань, стіни, металеві конструкції та розміщення ключа. Тому умови ретрансляції біля магазину й житлового приміщення можуть відрізнитися. Перевірка захисту має враховувати реальні умови зберігання ключа. Непідтверджені твердження про гарантовану дальність, прихованість пристрою чи неможливість довести його призначення не є підставою для технічного висновку.

Одним із практичних напрямів є обмеження штатного радіоканалу в режимі охорони та додаткова авторизація окремою міткою або іншим засобом. Така система може бути додатковою сигналізацією чи нештатним іммобілайзером. Розглянемо кілька варіантів інтеграції, застосовність яких залежить від електричної схеми:

- керований вплив на передавання дозволу до модулів штатного доступу; фізичне шунтування цифрової шини не слід трактувати як універсальний спосіб через можливі наслідки для інших вузлів;
- керування живленням штатного трансивера лише в режимах і конфігураціях, для яких підтверджено сумісність;
- обмеження роботи сенсорів контактних зон із перевіркою всіх альтернативних шляхів авторизації.

Поеднання додаткового іммобілайзера з належно встановленим електромеханічним замком капота створює різні за призначенням бар'єри. Проте заборона запуску не тотожна захисту майна в салоні й не запобігає переміщенню евакуатором.

Для автомобілів із пасивним безключовим доступом розглянемо сім напрямів протидії ретрансляції. Їх вибір залежить від конструкції ключа, функцій автомобіля та прийнятного рівня зручності.

1. Для відключення відповіді автомобільного ключа може використовуватися керування його електроживленням. Одним із варіантів є мікровимикач батарейки на час відсутності власника біля автомобіля. Втручання у конструкцію ключа потребує перевірки працездатності та надійності; пріоритет слід надавати передбаченим виробником режимам.

2. Одним із напрямів протидії ретрансляторам стало впровадження можливості відключення безконтактного доступу штатним способом. Для окремих реалізацій така функція активується комбінацією натискань на ключі або діями з органами керування автомобіля. Процедура потрібно звіряти з інструкцією конкретної моделі.

Наприклад, в інструкції Volkswagen Nivus (код документа 25A.5L1.NIV.20) описано тимчасове вимкнення Keyless Access: після замикаання кнопкою ключа протягом п'яти секунд натискають кнопку на зовнішній частині ручки. Після наступного відмикання функція активується знову [13, с. 58]. Це послідовність дій для керування режимом, а не «двофакторна деактивація». Інструкція Mercedes-Benz CLA 2016 року передбачає деактивацію KEYLESS-GO двома швидкими натисканнями кнопки замикаання на SmartKey. Підтвердженням є світлова індикація на ключі, а не два короткі та один довгий звукові сигнали [14, с. 78]. Процедура не слід автоматично переносити на інші моделі й покоління ключів. Для Range Rover спосіб керування пасивним доступом слід визначати за інструкцією відповідної моделі, року та комплектації. Комбінації натискань, наведені для іншого покоління ключа або іншої моделі, не слід переносити без перевірки.

3. Екранування ключа. Чохол Фарадея, металевий контейнер або інша екранувальна оболонка можуть обмежувати радіообмін. Результат залежить від матеріалу, конструкції, закриття та робочих частот



конкретного ключа. Тому потрібна перевірка, чи автомобіль реагує на ключ, який перебуває всередині оболонки. Номінальний частотний діапазон або рекламна назва не доводять повного блокування; пошкодження й неповне закриття можуть знижувати захисну функцію [6].

4. Автоматичне керування живленням за рухом. Прикладом є Keyless Protector — вставка до батарейного відсіку ключа. За описом постачальника RMS, вона використовує мікропроцесор і датчик руху для керування живленням [15]. Це опис принципу конкретного виробу; сумісність, режими спрацювання й ефективність потребують окремої перевірки.

Перші чотири розглянуті способи можуть обмежувати зручність користування безконтактним доступом: від відкривання багажника, коли водій підходить до автомобіля з кількома пакетами із супермаркету, до пошуку ключа у кишені для відкриття дверей. Тому вибір захисту має враховувати готовність власника регулярно виконувати потрібні дії.

5. Додаткові системи авторизації для захисту штатного радіоканалу. Ідентифікаторами в цьому випадку є додаткові радіомітки, які можуть зберігатися в гаманці, або застосунок на мобільному телефоні. Під час установлення охоронної системи може здійснюватися підключення до цифрової шини CAN. Необхідно з'ясувати, чи формується окрема умова дозволу, а не лише повторюється штатне підтвердження.

Підтримка штатного радіоканалу (на професійному сленгу інсталяторів охоронних систем — «підпір штатки») — ще один спосіб посилити штатні охоронні системи та обмежити несанкціонований доступ і подальший запуск автомобіля. Його розглядають для автомобілів із пасивним доступом та кнопкою START-STOP. Окремий засіб авторизації має доповнювати штатний дозвіл. Такий підхід спрямований на обмеження таких сценаріїв:

- ретрансляцію обміну зі штатним ключем за відсутності окремого дозволу;
- зняття додаткової охорони лише на підставі штатного радіопідтвердження;
- використання викраденого штатного ключа без додаткової авторизації;
- використання несанкціоновано зареєстрованого ключа, якщо окрема умова дозволу не виконана.

Результат залежить від того, які саме дії блокує додаткова система: відмикання, зняття охорони чи запуск. Захист не слід вважати підтвердженням лише за фактом установлення мітки або підключення до CAN.

Для пояснення принципу розглянемо типовий варіант PKES з низькочастотним запитом близько 125 кГц та відповіддю ключа в іншому радіодіапазоні; конкретні частоти й послідовність визначаються реалізацією [6]. Для відповіді ключа, зокрема, може використовуватися діапазон 433 МГц [6].

Реалізація обмеження радіоканалу потребує професійного інтегрування. Одним із варіантів є втручання в приймальний вузол, проте спосіб його виконання має визначатися електричною схемою та перевіркою наслідків для інших функцій автомобіля.

Після коректної інтеграції додаткове підтвердження може дозволяти відповідну дію власнику. Якщо використовується мобільний застосунок, потрібно враховувати налаштування й доступність Bluetooth, а також живлення телефона. Аналогічно враховуються умови роботи додаткової мітки й аварійний порядок авторизованого доступу.

6. Часові перевірки близькості. Основна авторська пропозиція — скоротити заводський тайм-аут так, щоб відхиляти ретрансльовану відповідь і зберегти штатну авторизацію. Умову вибору порога та межі застосування розглянемо далі (в підрозділі 2.3). Для відстані 300 м і швидкості поширення близько 3×10^8 м/с проходження сигналу становить приблизно 1 мкс в один бік і 2 мкс в обидва боки. Це розрахунок лише складової поширення, а не вимірний час повної авторизації. За даними Francillon та співавторів [6, підрозд. 3.4, табл. 3], затримки передавальних і приймальних електронних схем бездротового ретранслятора становили приблизно 15–20 нс, тоді як виміряна затримка низькочастотного каналу (LF, Low Frequency) на відстані 30 м — 120 ± 20 нс; для загальної затримки ретрансляції враховується також зворотний ультрависокочастотний канал (UHF, Ultra High Frequency). У таблиці 5 цієї праці найбільша допустима додаткова затримка для перевірених систем становила від 35 мкс до 10–20 мс. Це результати експериментів Francillon та співавторів для досліджених реалізацій, а не універсальні заводські тайм-аути або вимірювання автора. Вони підтверджують можливість значно меншої додаткової затримки ретрансляції порівняно з допустимою затримкою відповіді, але самі по собі не доводять наявності порога, який розділяє штатний і ретрансльований обмін у конкретному автомобілі.

7. Надширокопasmовога технологія UWB. Ultra-Wideband використовується для визначення відстані та може підтримувати перевірку близькості ключа. Jaguar Land Rover описує застосування UWB як засобу протидії ретрансляційним атакам [16]. Водночас дослідження Ghost Peak демонструє маніпуляції з виміряною відстанню в окремих реалізаціях UWB із високою частотою повторення імпульсів (HRP, High-Rate Pulse Repetition Frequency) [9]. Це не доводить вразливості всіх автомобільних UWB-систем, але



показує необхідність перевірки конкретного протоколу й реалізації. Захист визначається не лише швидкістю обміну чи заявленою точністю.

Технічне рішення вдосконалення електронного захисту — розділити штатне відмикання й додатковий дозвіл запуску: штатна команда сама по собі не повинна знімати всі рівні охорони. Поєднання окремої авторизації, блокування запуску й захищення доступу до блокувального вузла зменшує залежність від єдиного каналу. Перевірці підлягають запуск без додаткового дозволу, зникнення живлення, втрата мітки й сервісний режим. Реакція має бути безпечною та не спричиняти довільної зупинки автомобіля під час руху.

2.2. Втручання в CAN та захист внутрішнього обміну

Захист цифрового обміну має запобігати використанню підробленого цифрового підтвердження як підстави для відмикання або запуску. Фізичне підключення до проводки є шляхом доступу, а введення повідомлень CAN — втручанням у цифровий обмін. Захист внутрішнього обміну доповнює захист радіоканалів; фізичні бар'єри ускладнюють доступ до відповідних вузлів.

Одним зі способів несанкціонованого впливу є фізичний доступ до CAN-мережі автомобіля. Кількість і призначення підключених блоків залежать від моделі та комплектації. Бортіві повідомлення забезпечують узгоджене виконання функцій керування й моніторингу, тому їх підміна може мати наслідки для роботи відповідних систем [8].

CAN було розроблено для обміну даними між електронними компонентами автомобіля; протокол набув застосування також у промисловості [10]. CAN та Ethernet є різними технологіями мережного обміну. Для кіберзахисту принципове значення має перевірка того, чи доповнена передача CAN-повідомлень засобами криптографічної автентифікації та захисту від повторного використання.

У високошвидкісних реалізаціях CAN диференціальна передача через CAN High і CAN Low сприяє завадостійкості. Колір проводів і схема їх розміщення визначаються документацією конкретного виробника, тому універсальна ідентифікація лише за кольором некоректна. Фізична завадостійкість лінії не є засобом перевірки походження повідомлення.

CAN-шина є засобом зв'язку між пристроями автомобіля. За наявності доступу до відповідного сегмента та недостатньої перевірки повідомлень можливий вплив на рішення підключених блоків. Для аналізу протигінного захисту важливо встановити, чи бере конкретний сегмент участь у передачі підтвердження доступу або дозволу запуску [8].

Розглянемо приклади спеціалізованих пристроїв у корпусах портативної акустики або телефона Nokia 3310. Зовнішній вигляд не визначає механізму атаки: пристрій для CAN injection не є звичайним телефоном чи ретранслятором сигналу ключа. Підміна внутрішнього повідомлення та ретрансляція обміну зі справжнім ключем є різними способами несанкціонованого впливу [8], [6].

У технічному описі К. Tindell розглянуто випадок Toyota RAV4, де доступ до мережі був пов'язаний із вузлом передньої фари. Це демонструє необхідність оцінки доступності зовнішніх електронних компонентів, але не означає однакової архітектури фар і мереж у всіх автомобілях [8].

При CAN injection до відповідної мережі вводяться повідомлення, які система може прийняти як підтвердження від штатного вузла перевірки ключа. У розглянутому технічному описі це пов'язано з обходом внутрішнього механізму довіри, а не з розкриттям секрету справжнього ключа [8]. Тому захист лише радіоканалу ключа не охоплює цей шлях. Наведений приклад не дає підстав переносити висновки на всі моделі згаданих у вихідному тексті брендів або встановлювати універсальний час викрадення.

До напрямів захисту CAN-мережі від стороннього втручання належать такі заходи, застосовність яких потрібно оцінювати для конкретної архітектури.

Захист фізичними бар'єрами: захисні корпуси й спеціальні кронштейни для джгутів проводів, обмеження доступу до роз'ємів та електронних блоків. Їх призначення — ускладнити демонтаж або несанкціоноване підключення.

Шифрування даних може забезпечувати конфіденційність за умови підтримки відповідної схеми учасниками обміну. Саме шифрування не слід ототожнювати з перевіркою походження чи актуальності повідомлення.

Використання фільтрів для блокування небажаних повідомлень у CAN-мережах. Правила фільтрації мають відповідати функціям конкретного сегмента та не порушувати легітимний обмін.

Контрольні суми виявляють певні помилки передавання. Звичайну контрольну суму не можна використовувати як доказ криптографічної справжності повідомлення або захист від навмисної підміни.

Використання автентифікації для перевірки справжності повідомлень і контролю їх актуальності для протидії повторному використанню. Захист внутрішнього обміну й розмежування доступу розглядаються в рекомендаціях Національної адміністрації безпеки дорожнього руху США (NHTSA, National Highway Traffic Safety Administration) [17]. Додаток 5 Правил № 155 містить перевірку справжності й цілісності повідомлень (M10) та розгляд засобів виявлення шкідливого внутрішнього



обміну CAN (M15). Згаданий replay означає повторне відтворення, а не ретрансляцію поточного обміну зі справжнім ключем [12].

Маркування й контроль стану проводки можуть допомагати виявляти втручання під час огляду або обслуговування. Позначення проводів саме по собі не унеможливує їх пошкодження чи підміну.

Контроль зовнішніх інтерфейсів і мережних шлюзів має обмежувати несанкціонований вплив на CAN із бездротових або інших зовнішніх компонентів. Це точніше, ніж загальна вимога «відключити бездротові підключення до CAN», оскільки доступ зазвичай опосередковується окремими блоками.

2.3. Часова перевірка авторизації як основна пропозиція протидії ретрансляції

На відміну від розглянутого втручання в CAN, ретрансляція зберігає обмін зі справжнім ключем [6]. Для цього сценарію розвиваємо часову пропозицію, наведену в пункті 6 підрозділу 2.1: визначаємо допустимий інтервал тайм-ауту, вимоги до точності й межі застосування.

Умова розділення часових характеристик:

$$t_{\text{штатний, max}} + \varepsilon < T_{\text{тайм-аут}} < t_{\text{ретрансльований, min}} - \varepsilon \quad (1)$$

де $t_{\text{штатний, max}}$ — найбільший час від запиту до завершення відповідної перевірки за штатної роботи ключа в дозволений зоні; $t_{\text{ретрансльований, min}}$ — найменший повний час тієї самої перевірки через ретранслятор у розглянутих сценаріях; $T_{\text{тайм-аут}}$ — допустимий час очікування; ε — запас на похибку вимірювання та невраховані коливання. Обидва часи потрібно вимірювати між однаковими подіями протоколу. Додаткова затримка ретранслятора є лише складовою повного часу обміну й не може безпосередньо підмінити його в цій нерівності.

За наявності такого інтервалу скорочення тайм-ауту може відхиляти розглянуті ретрансляційні сценарії. Якщо діапазони перекриваються, одного налаштування загального тайм-ауту недостатньо: потрібен швидкий автентифікований обмін із контрольованим часом оброблення та точним вимірюванням затримки. Протоколи обмеження відстані (distance bounding) реалізують цей принцип; дослідження [6] пояснює значення стабільності часу відповіді та захищеності обміну від попереднього формування відповіді. У цій статті не заявляється розроблення нового протоколу обмеження відстані.

Технічна реалізація й перевірка. Спочатку слід визначити часові характеристики штатної авторизації за різних допустимих умов роботи, точність вимірювання та найменші затримки розглянутих способів ретрансляції. Далі обирають поріг із запасом і перевіряють відмови законному користувачу та пропуск ретрансльованих відповідей. За недостатньої точності потрібне вдосконалення протоколу й апаратних засобів вимірювання на рівні виробника. Відхилення простроченої відповіді має забороняти відповідну авторизацію доступу або запуску, зберігаючи безпечні функції автомобіля. Довільне зменшення параметра без таких перевірок не є обґрунтованою реалізацією пропозиції. Пункт 7.3.6 Правил № 155 вимагає випробувати ефективність захисту; п. 5.1.2 передбачає перевірку реалізації заявлених заходів випробуваннями автомобіля [12]. Вибір часового порога є технічною пропозицією цієї статті: числового тайм-ауту безключової авторизації в опрацьованому тексті № 155 не встановлено.

Межі застосування. Часова перевірка спрямована на ретрансляцію справжнього ключа поза дозволеною зоною. Вона не усуває використання викраденого ключа поруч з автомобілем, введення підроблених CAN-повідомлень в обхід перевірки або переміщення евакуатором. Тому її слід поєднувати з фізичними бар'єрами та незалежною авторизацією. Захист команд, які можуть обійти перевірку ключа, розглянуто в наступному підрозділі.

Інтервальна модель та припущення. Нехай $s_{\min}$ і $s_{\max}$ задають нижню й верхню межі істинної повної тривалості штатного обміну, а $r_{\min}$ — нижню межу повної тривалості ретрансльованого обміну для явно визначеної множини сценаріїв. Час відлічується між однаковими подіями протоколу. Абсолютні похибки оцінювання часу не перевищують ε_s і ε_r відповідно; вони охоплюють невизначеність фіксації подій, тоді як допустимі зміни режиму роботи вже включено до часових меж. Повторно враховувати одну й ту саму складову невизначеності не потрібно. Справжність та актуальність відповіді перевіряються незалежно від часу. Модель не допускає успішного передбачення відповіді або зміни подій відліку; за таких можливостей наведені межі потребують перегляду.

$$S = s_{\max} + \varepsilon_s; R = r_{\min} - \varepsilon_r; W = R - S \quad (2)$$

Тут S — найбільший час штатної відповіді з урахуванням похибки, R — найменший час ретрансльованої відповіді з урахуванням похибки, W — ширина інтервалу розділення. Система дозволяє операцію лише за справжньої актуальної відповіді та виконання часової перевірки. Розглядаємо пороги $S < T < R$, які забезпечують додатний запас з обох боків; вимоги до оброблення точного збігу з порогом не



впливають на цей інтервал.

Твердження 1. У заданій моделі неперервний поріг із додатним запасом існує тоді й лише тоді, коли $W > 0$. Для будь-якого T усередині цього інтервалу найбільша спостережувана штатна тривалість не перевищує $S < T$, а найменша ретрансльована тривалість не менша за $R > T$. Якщо $W \leq 0$, немає значення, яке одночасно перевищує S та є меншим за R . Це доведення стосується розділення гарантованих меж, а не оцінки частоти хибних рішень.

$$g(T) = \min(T - S, R - T); \quad T^* = (S + R)/2; \quad g(T^*) = W/2 \quad (3)$$

Величина $g(T)$ — мінімальний часовий запас. Оскільки сума двох запасів дорівнює W , менший із них не може перевищувати $W/2$. Рівність досягається в середині інтервалу, що обґрунтовує формулу (3). Це оптимум лише за прийнятим критерієм: він не означає оптимальної вартості, зручності чи ймовірності викрадення. Скорочення заводського параметра можливе лише за $T^* < T_0$, де T_0 — початковий тайм-аут; коли ця умова не виконана, саме T^* не є скороченням. Якщо потрібне інше допустиме значення $T < T_0$, слід також перевірити наявність порога в перетині інтервалів (S, R) та $(-\infty, T_0)$.

Дискретність налаштування. Нехай доступні пороги утворюють сітку $T_k = T_{\text{ref}} + kq$, де $q > 0$ — крок налаштування, T_{ref} — відома опорна величина, k — ціле число. Діапазон дозволених значень параметра враховується додатковим перетином; для скорочення використовуємо верхню межу $U = \min(R, T_0)$. Умова $S < T_k < U$ дає такі межі індексу:

$$\begin{aligned} k_{\min} &= \text{floor}((S - T_{\text{ref}})/q) + 1 \\ k_{\max} &= \text{ceil}((U - T_{\text{ref}})/q) - 1 \end{aligned} \quad (4)$$

Твердження 2. Без апаратного обмеження допустимий дискретний скорочений поріг із додатним запасом існує тоді й лише тоді, коли $k_{\min} \leq k_{\max}$. Якщо дозволени індекси обмежено цілими a і b , точний критерій має вигляд $\max(k_{\min}, a) \leq \min(k_{\max}, b)$. Функції floor і ceil означають округлення вниз та вгору. Строгість часових нерівностей враховано додаванням і відніманням одиниці, зокрема коли межа точно збігається з вузлом сітки. Додатне W саме по собі не гарантує виконання цієї умови.

Серед допустимих вузлів сітки найбільше $g(T_k)$ має вузол, найближчий до середини $(S + R)/2$. Якщо середина поза множиною дозволених скорочених порогів, обирається найближчий допустимий крайній вузол. Доведення випливає з того, що $g(T)$ зростає до середини інтервалу та спадає після неї. За двох рівновіддалених вузлів їх мінімальні запаси однакові. Інтервал шириною понад q обов'язково містить вузол необмеженої сітки, але це лише достатня умова; точний критерій задає формула (4).

У таблиці 1 наведено умовні приклади для $T_{\text{ref}} = 0$ та $T_0 > R$, без додаткового апаратного обмеження. Усі величини нормовано на q . Ці числа обрано для перевірки граничних випадків; вони не походять із вимірювань автомобіля й не є рекомендованими заводськими налаштуваннями.

Таблиця 1

Розрахункові приклади існування дискретного порога

S/q	R/q	W/q	Допустимі k	T/q	g/q
10,2	10,8	0,6	немає	—	—
10,2	11,8	1,6	11	11	0,8
10,2	12,2	2,0	11, 12	11	0,8
10,8	11,2	0,4	11	11	0,2

Перший рядок показує інтервал із $W > 0$, який не містить жодного допустимого дискретного порога. Друга й третя підтверджують правило вибору найближчого до середини вузла; у третьому рядку для $k = 12$ запас становив би лише $0,2q$ замість $0,8q$ для $k = 11$. Четверта показує, що навіть інтервал завширшки $0,4q$ може містити допустимий вузол залежно від розташування меж. Отже, оцінювати потрібно і ширину інтервалу, і його положення відносно сітки.

Зв'язок із додатковою затримкою. Лише за окремого припущення, що ретрансляція додає затримку $\Delta \geq \Delta_{\min}$ до штатного обміну і не скорочує інші його складові, маємо $r_{\min} \geq s_{\min} + \Delta_{\min}$. Позначимо $v = s_{\max} - s_{\min}$. Тоді ширина інтервалу має нижню оцінку:

$$W \geq \Delta_{\min} - v - \varepsilon_s - \varepsilon_r \quad (5)$$

За цієї додаткової моделі нерівність $\Delta_{\min} > v + \varepsilon_s + \varepsilon_r$ є достатньою для існування неперервного порога. Умова $\Delta_{\min} > v + \varepsilon_s + \varepsilon_r + q$ гарантує наявність вузла необмеженої сітки, але не його входження



до апаратного діапазону чи скорочення відносно T_0 ; ці вимоги перевіряються окремо за формулою (4). Якщо нерівність не виконано, достатня гарантія не отримана, проте це саме по собі не доводить неможливості розділення за точнішими межами.

Розрахунок приблизно 2 мкс для проходження 300 м у двох напрямках характеризує лише поширення сигналу. Його не можна автоматично підставляти як $\Delta_{\min}$: потрібні визначені геометрія обох шляхів, штатна відстань, часові події й модель ретранслятора. Так само затримка електронних схем 15–20 нс із дослідження [6] не є універсальною нижньою межею для всіх можливих пристроїв. Відсутність обґрунтованої нижньої межі $r_{\min}$ означає, що універсальний тайм-аут на підставі цих чисел визначити неможливо.

Порівняння з відомими рішеннями та межі результату. Дослідження Francillon та співавторів [6] демонструє ретрансляцію та обґрунтовує перевірку близькості на основі часу. У цій роботі конкретизовано вибір загального порога за похибками й доступною сіткою налаштувань та обґрунтовано запас до часових меж. Протоколи distance bounding потребують захищеного швидкого обміну; налаштування загального тайм-ауту не замінює такий протокол. Результати Ghost Peak [9] додатково показують, що заявлена технологія вимірювання відстані потребує перевірки конкретної реалізації. Запропонований критерій не враховує такі атаки автоматично: відповідні сценарії мають входити до множини, за якою обґрунтовано $r_{\min}$. Аналітична процедура придатна для проєктування або сумісної модернізації, але не доводить, що наявний автомобіль допускає ефективну зміну лише програмного параметра.

2.4. Захист цифрових команд, діагностики та програмного забезпечення

Переваги й обмеження захисту цифрового обміну. Перевірка походження й актуальності повідомлення дає змогу відрізнити дозволена команду від підробленої або повтореної. Контроль цифрового обміну може також виявляти втручання, яке не помітне фізичним датчикам. Обмеження — залежність від можливостей блоків, захищення ключів, коректної конфігурації та оновлень. Додаткові перевірки потребують оцінювання затримок і навантаження; помилкове виявлення не має порушувати безпечне керування.

1. *Автентифікація критичних команд.* Для повідомлень, від яких залежить дозвіл запуску, пропонується перевірка криптографічного коду автентифікації та значення актуальності повідомлення, наприклад лічильника. Подібний принцип описано у специфікації захищеного бортового обміну (SecOC, Secure Onboard Communication) партнерства AUTOSAR (AUTomotive Open System ARchitecture — відкрита системна архітектура автомобіля); він потребує підтримки з боку відправника й одержувача [18]. Практичне завдання — визначити критичні команди, захищати відповідні ключі та перевірити відхилення підроблених і повторених повідомлень. Звичайна контрольна сума цього завдання не виконує. Таке рішення належить до проєктування або сумісної модернізації електронної архітектури, а не до встановлення універсального зовнішнього пристрою.

2. *Контроль діагностики й мережних ілюзій.* Пропонується дозволяти реєстрацію ключів і зміну охоронних налаштувань лише в авторизованій діагностичній сесії та обмежувати проходження команд із зовнішніх інтерфейсів до критичних сегментів. Політика доступу має зберігати необхідні сервісні функції [17]. Фізичний захист бортового діагностичного інтерфейсу (OBD, On-Board Diagnostics) із розділу 1 доповнює цей контроль. Перевіряти потрібно спробу реєстрації ключа без належного дозволу та штатне обслуговування після встановлення обмежень. Захід M22 у таблиці B4 додатка 5 Правил № 155 стосується захисту зовнішніх інтерфейсів, зокрема від атак через діагностичний доступ OBD [12].

3. *Виявлення втручань.* Як напрям удосконалення пропонується моніторинг неочікуваних послідовностей команд авторизації, частоти повідомлень і діагностичних звернень. Ознаки, пороги та правила реагування необхідно визначати для конкретної мережі, зіставляючи підозрілі події зі штатними режимами. Виявлення слід пов'язати з журналюванням, повідомленням власнику та перевіркою дозволу перед наступним запуском. Сам факт аномалії не є достатньою підставою для зупинки автомобіля під час руху. Критерії перевірки — виявлення заданих сценаріїв, частота хибних спрацювань і безпечність реакції. Пункт 7.3.7 Правил № 155 передбачає виявлення й запобігання атакам, підтримку моніторингу та аналізу даних про спроби втручання [12]. Запропоновані тут ознаки й реакції потребують окремого обґрунтування.

4. *Захищене оновлення програмного забезпечення.* Правила ООН № 156 у публікації 2021 року встановлюють захист справжності й цілісності оновлень (п. 7.2.1.1), визначення міжсистемних залежностей і перевірку сумісності (пп. 7.1.1.5, 7.1.1.7). Для ОТА передбачено відновлення попередньої версії або безпечний стан після невдалого оновлення (п. 7.2.2.1.1), достатнє живлення та технічне забезпечення безпечних умов установлення (пп. 7.2.2.1.2–7.2.2.1.3) [19]. Для протиугінного комплексу пропонується додатково перевіряти після оновлення взаємодію штатної авторизації з установленою охороною та збереження часового порога. Це рекомендація статті, а не дослівна вимога Правил. Критерії перевірки — відхилення зміненого пакета, сумісність блоків, відновлення після переривання та збереження заданих умов запуску.



2.5. Узгодження механічних та електронних заходів

Пропонується використовувати послідовність незалежних умов: фізичний бар'єр ускладнює доступ до вузлів; електронна система перевіряє справжність цифрових підтверджень і вимагає окремого дозволу запуску. Для протидії ретрансляції справжнього ключа потрібна також часова перевірка його близькості. Для кожного можливого обходу слід встановити, який інший засіб зберігає захисну функцію. Перевірку комплексу доцільно проводити за сценаріями викраденого штатного ключа, радіозавад, доступу до проводки, неавторизованої діагностики та програмного оновлення. Це запропонований спосіб перевірки взаємодії засобів; результати таких випробувань у статті не наведено.

Зв'язок нормативних вимог із технічними рішеннями. ISO/SAE 21434 задає рамку інженерного управління кіберризиками [3]. Пункт 7.3.4 Правил № 155 пов'язує вибір заходів із виявленими ризиками й вимагає іншого належного рішення, якщо перелічене недостатнє [12]. Для цієї статті це означає необхідність зіставляти спосіб викрадення, захисну функцію та результат її перевірки. Часова авторизація, захист CAN, діагностики й оновлень мають оцінюватися за відповідними сценаріями втручання. Використано публікацію № 155 від 2025 року, що включає доповнення 3, і базову публікацію № 156 від 2021 року; повноту охоплення подальших змін не заявлено.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В роботі зіставлено механічні та електронні заходи захисту автомобіля від викрадення. Перевагою механічних засобів є створення фізичної перешкоди доступу до охоронних вузлів і переміщенню автомобіля; їх обмеження пов'язані із силовим обходом, монтажем та обслуговуванням. Електронні засоби забезпечують перевірку дозволу доступу й запуску, виявлення втручань та захист цифрових команд, але залежать від живлення, каналів зв'язку й реалізації авторизації. Поєднання цих заходів слід визначати за сценаріями обходу та перевіряти на сумісність.

Центральна технічна пропозиція — скорочення заводського тайм-ауту безключової авторизації. Для її оцінювання побудовано інтервальну модель із похибками: вільний неперервний поріг із додатним запасом існує за $W > 0$. Для скорочення заводського тайм-ауту додатково потрібен поріг нижче його початкового значення. Для дискретного налаштування з апаратними межами індексу виведено точний критерій $\max(k_{\min}, a) \leq \min(k_{\max}, b)$, де межі індексу враховують вимогу скорочення початкового тайм-ауту, а a і b — апаратні межі. Обґрунтовано вибір допустимого порога, найближчого до середини інтервалу, для максимізації мінімального часового запасу. Умовні розрахунки показали, що додатний інтервал може не містити доступного значення параметра. За припущення про адитивну затримку отримано достатню умову через її нижню межу, діапазон штатного часу та похибки. Висновки чинні лише за заявлених припущень і гарантованих часових меж; часовий контроль не охоплює всі способи викрадення.

Для узгодженого застосування засобів запропоновано захищати доступ до електронних блоків і проводки, використовувати незалежний дозвіл запуску, перевіряти справжність і актуальність цифрових команд, контролювати діагностику та сумісність після оновлень. Сім розглянутих напрямів протидії ретрансляції відрізняються умовами застосування і впливом на зручність користування. Вибір має враховувати конструкцію конкретного автомобіля, незалежність додаткової авторизації та безпечність реакції охоронної системи.

Практичний результат — послідовність оцінювання: визначити сценарії та однакові події відліку; обґрунтувати часові межі, похибки й сітку налаштування; перевірити існування скороченого порога; обрати значення з найбільшим мінімальним запасом; оцінити сумісність із незалежним дозволом запуску та іншими захисними засобами. Власних вимірювань і кількісної оцінки зниження ризику викрадення не наведено. Подальший розвиток методу може стосуватися багаторежимної авторизації, часових меж для конкретних протоколів та змін після оновлень. Практичне впровадження потребує окремої валідації, яка виходить за межі цієї теоретико-аналітичної роботи.

Доступність даних. Первинні експериментальні дані в роботі не створювалися. Джерела опублікованих результатів наведено в бібліографії; умовні приклади повністю визначено формулами (2)–(4) та відповідними значеннями таблиці 1.

Декларація про використання штучного інтелекту. Під час підготовки рукопису використано ChatGPT для мовного редагування українського та англійського текстів, допомоги в опрацюванні аналітичної моделі, перевірці розрахунків, пошуку й перевірці бібліографічних відомостей та оформленні рукопису, а також сервіс Grammarly для автоматичного виправлення граматичних і пунктуаційних помилок.

Після використання зазначених технологій автор детально перевірів, критично оцінив та



відредагував весь отриманий текст. Автор несе повну особисту відповідальність за науковий зміст, висновки дослідження та оригінальність цієї публікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Клімушин, П., Світличний, В., Гнусов, Ю., & Онищенко, Ю. (2025). Автомобільна електроніка та кібербезпека: системний огляд атак на безпеку та заходів протидії. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 4(28), 115–136. <https://doi.org/10.28925/2663-4023.2025.28.760>
2. Світличний, В. А. (2020). Кібербезпека сучасного автомобіля. У *Сучасні тенденції розвитку автомобільного транспорту та галузевого машинобудування: матеріали міжнародної науково-практичної конференції* (с. 134–135). ХНАДУ.
3. International Organization for Standardization, & SAE International. (2021). *Road vehicles — Cybersecurity engineering* (ISO/SAE 21434:2021). <https://www.iso.org/standard/70918.html>
4. Світличний, В. А. (2023). Виклики та перспективи покращення кібербезпеки і захисту від викрадання сучасних автомобілів. У *Актуальні питання з розроблення й виготовлення спеціальних та спеціалізованих автотранспортних засобів в умовах воєнного стану: збірник тез доповідей Всеукраїнської науково-практичної конференції* (с. 166–169). ДНДІ МВС України.
5. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX Security Symposium*. USENIX Association. <https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces>
6. Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Internet Society. <https://www.ndss-symposium.org/wp-content/uploads/2017/09/franc.pdf>
7. Garcia, F. D., Oswald, D., Kasper, T., & Pavlidès, P. (2016). Lock it and still lose it—On the (in)security of automotive remote keyless entry systems. In *25th USENIX Security Symposium* (pp. 929–944). USENIX Association. <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia>
8. Tindell, K. (2023, April 3). *CAN injection: Keyless car theft*. Dr. Ken Tindell. <https://kentindell.github.io/2023/04/03/can-injection/>
9. Leu, P., Camurati, G., Heinrich, A., Roeschlin, M., Anliker, C., Hollick, M., Capkun, S., & Classen, J. (2022). Ghost Peak: Practical distance reduction attacks against HRP UWB ranging. In *31st USENIX Security Symposium* (pp. 1343–1359). USENIX Association. <https://www.usenix.org/conference/usenixsecurity22/presentation/leu>
10. CAN in Automation. (n.d.). *History of CAN technology*. <https://www.can-cia.org/can-knowledge/history-of-can-technology>
11. OnStar. (n.d.). *The history and evolution of OnStar*. <https://www.onstar.com/why-onstar/evolution-of-onstar-innovations>
12. United Nations Economic Commission for Europe. (2025). *UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system [2025/5]*. Official Journal of the European Union, L, 2025/5. <https://eur-lex.europa.eu/eli/reg/2025/5/oj/eng>
13. Volkswagen. (n.d.). *Nivus: Manual de instruções* (25A.5L1.NIV.20). https://www.volkswagen.com.pa/idhub/content/dam/onehub_pkw/importers/pa/manuales/25A.5L1.NIV.20%20-%20Manual%20de%20instrucoes.pdf
14. Mercedes-Benz. (2016). *CLA: Operator's manual*. https://www.mbusa.com/content/dam/mb-nafta/us/owners/manuals/2016/operators/MY16_CLA_Operator.pdf
15. RMS. (n.d.). *Keyless Protector*. <https://rms-tuning.pl/keyless-protector/>
16. Jaguar Land Rover. (n.d.). *Security & protection FAQs*. <https://www.landrover.co.uk/ownership/security-faqs.html>
17. National Highway Traffic Safety Administration. (2022). *Cybersecurity best practices for the safety of modern vehicles*.
18. AUTOSAR. (2023). *Specification of Secure Onboard Communication Protocol* (Foundation R23-11, Document ID 969).
19. United Nations Economic Commission for Europe. (2021). *UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388]*. Official Journal of the European Union, L 82, 60–74. <https://eur-lex.europa.eu/eli/reg/2021/388/oj/eng>

**Vitalii Svitlychnyi**

Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Cybercrime Counteraction
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID: 0000-0003-3381-3350
vit.svet@ukr.net

OPTIMIZATION OF VEHICLE THEFT PROTECTION CONSIDERING CYBERSECURITY REQUIREMENTS

Abstract. The study aims to substantiate the selection of a reduced factory timeout for passive keyless authentication within coordinated mechanical and electronic vehicle theft protection. The methods include analysis of scientific and regulatory sources, interval modelling of timing characteristics, analytical derivation of threshold feasibility conditions, and functional comparison of protective measures. Mechanical barriers to electronic control units and wiring, diagnostic port protection, independent start authorisation, and seven approaches to countering relay attacks are considered. The main theoretical result is a threshold selection model based on guaranteed bounds of complete legitimate and relayed exchanges, measurement errors, and the timeout adjustment step. For a continuous threshold, feasibility requires a positive separation interval. For a discrete threshold, an exact condition for the existence of an admissible setting is derived. A threshold that maximises the smaller clearance from the two timing boundaries is justified. Dimensionless illustrative calculations show that a positive separation interval may contain no admissible setting when the adjustment step is too large. Under the additional assumption of additive relay delay, a sufficient condition is derived from its lower bound and the legitimate response time range. Experimental findings reported by Francillon and colleagues explain the relationship between timing quantities; they are neither original measurements of this study nor universal vehicle parameters. The established principle of timing-based proximity verification is not claimed as a new protocol. The practical value is a procedure for assessing timeout feasibility and coordinating this decision with physical barriers, digital command verification, diagnostic access control and secure updates. Relevant provisions of UN Regulations Nos. 155 and 156 are mapped to protective functions. The study is theoretical and analytical, reports no original experiments, and does not claim a quantified reduction in vehicle theft probability. Model assumptions and application limits are specified. System-specific timing bounds and protocol behaviour require validation before deployment; the model alone cannot establish protection against every relay implementation.

Keywords: vehicle theft protection; mechanical measures; electronic measures; passive keyless entry; authentication; relay attack; timeout.

REFERENCES

1. Klimushyn, P., Svitlychnyi, V., Gnusov, Y., & Onyshchenko, Y. (2025). Avtomobilna elektronika ta kiberbezpeka: Systemnyi ohliad atak na bezpeku ta zakhodiv protydyi [Automotive electronics and cybersecurity: A systematic review of security attacks and countermeasures]. *Cybersecurity: Education, Science, Technique*, 4(28), 115–136. [In Ukrainian]. <https://doi.org/10.28925/2663-4023.2025.28.760>
2. Svitlychnyi, V. A. (2020). Kiberbezpeka suchasnoho avtomobilia [Cybersecurity of the modern vehicle]. In *Suchasni tendentsii rozvytku avtomobilnoho transportu ta haluzevoho mashynobuduvannia [Current trends in road transport and industrial mechanical engineering]* (pp. 134–135). Kharkiv National Automobile and Highway University. [In Ukrainian]. https://af.khadi.kharkov.ua/fileadmin/F-AUTOMOBILE/Конференції/2020/_тезы20п.pdf
3. International Organization for Standardization, & SAE International. (2021). *Road vehicles — Cybersecurity engineering* (ISO/SAE 21434:2021). <https://www.iso.org/standard/70918.html>
4. Svitlychnyi, V. A. (2023). Vyklyky ta perspektyvy pokrashchennia kiberbezpeky i zakhystu vid vykradannia suchasnykh avtomobiliv [Challenges and prospects for improving cybersecurity and theft protection of modern vehicles]. In *Aktualni pytannia z rozroblennia y vyhotovlennia spetsialnykh ta spetsializovanykh avtotransportnykh zasobiv v umovakh voiennoho stanu [Current issues in the development and manufacture of special and specialised vehicles under martial law: Proceedings of the All-Ukrainian scientific and practical conference]* (pp. 166–169). State Research Institute of the Ministry of Internal Affairs of Ukraine. [In Ukrainian].



- https://repositc.nuczu.edu.ua/bitstream/123456789/19696/1/36ірник_тез_2023%20конфер%20ВСТ.pdf
5. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX Security Symposium*. USENIX Association. <https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces>
 6. Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Internet Society. <https://www.ndss-symposium.org/wp-content/uploads/2017/09/franc.pdf>
 7. Garcia, F. D., Oswald, D., Kasper, T., & Pavlidès, P. (2016). Lock it and still lose it—On the (in)security of automotive remote keyless entry systems. In *25th USENIX Security Symposium* (pp. 929–944). USENIX Association. <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia>
 8. Tindell, K. (2023, April 3). *CAN injection: Keyless car theft*. Dr. Ken Tindell. <https://kentindell.github.io/2023/04/03/can-injection/>
 9. Leu, P., Camurati, G., Heinrich, A., Roeschlin, M., Anliker, C., Hollick, M., Capkun, S., & Classen, J. (2022). Ghost Peak: Practical distance reduction attacks against HRP UWB ranging. In *31st USENIX Security Symposium* (pp. 1343–1359). USENIX Association. <https://www.usenix.org/conference/usenixsecurity22/presentation/leu>
 10. CAN in Automation. (n.d.). *History of CAN technology*. <https://www.can-cia.org/can-knowledge/history-of-can-technology>
 11. OnStar. (n.d.). *The history and evolution of OnStar*. <https://www.onstar.com/why-onstar/evolution-of-onstar-innovations>
 12. United Nations Economic Commission for Europe. (2025). *UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system [2025/5]*. Official Journal of the European Union, L, 2025/5. <https://eur-lex.europa.eu/eli/reg/2025/5/oj/eng>
 13. Volkswagen. (n.d.). *Nivus: Manual de instruções* (25A.5L1.NIV.20). https://www.volkswagen.com.pa/idhub/content/dam/onehub_pkw/importers/pa/manuales/25A.5L1.NIV.20%20-%20Manual%20de%20instrucoes.pdf
 14. Mercedes-Benz. (2016). *CLA: Operator's manual*. https://www.mbusa.com/content/dam/mb-nafta/us/owners/manuals/2016/operators/MY16_CLA_Operator.pdf
 15. RMS. (n.d.). *Keyless Protector*. <https://rms-tuning.pl/keyless-protector/>
 16. Jaguar Land Rover. (n.d.). *Security & protection FAQs*. <https://www.landrover.co.uk/ownership/security-faqs.html>
 17. National Highway Traffic Safety Administration. (2022). *Cybersecurity best practices for the safety of modern vehicles*. <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>
 18. AUTOSAR. (2023). *Specification of Secure Onboard Communication Protocol* (Foundation R23-11, Document ID 969). https://www.autosar.org/fileadmin/standards/R23-11/FO/AUTOSAR_FO_PRS_SecOcProtocol.pdf
 19. United Nations Economic Commission for Europe. (2021). *UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388]*. Official Journal of the European Union, L 82, 60–74. <https://eur-lex.europa.eu/eli/reg/2021/388/oj/eng>

Отримано редакцією журналу / Received: 30.07.26

Прорецензовано / Revised: 14.08.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.