DOI 10.26886/2414-634X.3(22)2018.5

UDC: 001-004.7

ANALYSIS OF THREATS FOR VEHICLE ELECTRONIC CONTROL UNITS IN CAN NETWORK

O. Chekanin

O. Zhdanova, PhD in Technical Sciences

National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” Ukraine, Kyiv

The security issues of the information exchange protocol CAN for vehicle electronic control units, the general scheme of attacker’s actions for attack performing against the car is considered, and car safety standards are considered. The methodology of threat modeling is described. Descriptions of practical attacks are collected and the classification of attacks is given. The assessment of threats of practical attacks based upon five criteria is given, the most important of which are driver’s life safety and ability to cope with consequences of the attacker’s actions. Calculated estimates allow one to compare attacks on potential damage and identify the most critical one. Weight coefficients for the threats assessment are provided. The threat modeling methodology for vehicles is applied with results of practical attacks.

Keywords: vehicle security, cyberattack, threat, vulnerability, threat modeling, attacks analysis, attacks assessment, assessment of severity and controllability.

Чеканін О. Ю., кандидат технічних наук, доцент, Жданова О. Г. Аналіз загроз для електронних компонентів управління автомобіля в мережі CAN / Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Україна, Київ.

Метою роботи є аналіз практично виконаних атак на електронні компоненти управління автомобіля та визначення кількісних оцінок для загроз. Методологія моделювання загроз полягала в оцінюванні загроз за п'ятьма параметрами наслідків загрози та в виборі вагових коефіцієнтів для кожного параметру. До параметрів належать безпека водія, експлуатаційні характеристики автомобіля, приватність даних водія, фінансові ризики та керованість ситуації. Найважливишими параметрами були безпека водія та керованість ситуації. Був зібраний опис здійсненних атак, для кожної з них за обраними параметрами надані оцінки та розрахована загальна оцінка. Отримані результати мають цінність для експертів з інформаційної безпеки та виробників транспортних засобів. Проаналізовані атаки мають широкий діапазон оцінок, що свідчить про значну кількість можливостей для зловмисника, найнебезпечнішими атаками виявилися ті, що впливають на рух автомобіля та здатність водія керувати.

Ключові слова: інформаційна безпека автомобіля, кібератака, загроза, вразливість, моделювання загроз, аналіз атак, оцінка атак, оцінка строгості та керованості.

Вступ. Починаючи з середини 90-х років автомобільні виробники стали активно використовувати спеціалізовані комп'ютери з зв'язками між собою, що контролюють функції автомобіля. Сучасні автомобілі мають багато різних комп'ютерних компонентів, які називаються електронні компоненти управління (ЕКУ). Кожен автомобіль містить від 20 до 100 таких пристроїв причому кожен ЕКУ несе відповідальність за одну або декілька функціональних особливостей транспортного засобу.

Сучасні автомобілі контролюються складними комп'ютеризованими системами. Все це дозволяє забезпечити ту

функціональність, що можна зустріти в автомобілях: починаючи від вбудованого LTE та Wi-Fi модулів і закінчуючи автопілотом. Ще донедавна транспортні засоби не були об'єктами інформаційних атак і виробникам не доводилося приймати це до уваги. Проте сучасні автомобілі привертають увагу кіберзловмисників або хакерів, для яких автомобіль принципово не відрізняється від стаціонарного комп'ютера, банкомата чи смартфона. Тепер недостатньо забезпечити нормальну роботу усіх компонентів автомобіля та захищати водія разом з пасажирами від ДТП. Зусилля дослідників[1-6] зосереджені на знайденні вразливостей та здійсненні атак, при цьому виникає необхідність в класифікації та порівнянні цих атак за можливими наслідками.

Найбільш поширеним протоколом обміну інформацією між ЕКУ є протокол Controller Area Network (CAN), який можна вважати стандартом де-факто для індустрії [7]. Цей протокол було створено ще в середині 1980-х компанією Bosch. Зазвичай в автомобілі присутні дві або три окремі CAN мережі, що працюють з різною швидкістю передачі даних. Особливістю протоколу є те, що ЕКУ з'єднані послідовною шиною, використовується широкомовна передача даних і кожен компонент "бачить" кожне повідомлення в мережі. Цей протокол забезпечує для ЕКУ виконання своїх обов'язків, проте є вкрай вразливим для здійснення атак.

Формулювання мети статті та завдань.

Разом з новими можливостями ЕКУ відкрили також і додаткові можливості для атак на інформаційні системи автомобіля. Дослідниками цієї проблеми [1-6] були показані реальні можливості атакувати автомобілі, які присутні на ринку. Ці роботи зосереджені виключно на пошуку успішних сценаріїв атак та їх практичної

спроможності. Але вони не відповідають на питання: яким чином можна класифікувати атаки з точки зору їх впливу на безпеку автомобіля.

Метою статті є аналіз результатів практично виконаних атак та на їх основі застосування методології оцінки загроз для автомобіля. Оцінювання загроз відбувається за п'ятьма параметрами і в роботі визначаються пріоритети для кожного параметру, що відображено значеннями відповідних вагових коефіцієнтів. Отримані результати дозволять порівняти атаки за ступенем наслідків.

Кожна атака експлуатує вразливості та намагається здійснити можливі загрози. В цій роботі виявлені та проаналізовані практично виконані атаки та надана класифікація для загроз, що є основою цих атак. Перелік та аналіз загроз разом утворюють модель загроз, що і є головною темою цієї роботи.

Приведемо визначення основних термінів, що використовуються в роботі. *Кібератака* - напад на безпеку системи, що випливає з використання загрози, тобто інтелектуальної дії, що є навмисною спробою уникнути служб безпеки та порушити політику безпеки системи [8]. *Загроза* - можлива причина інциденту, що може призвести до шкоди системам і організації [9]. *Вразливість* - вада або недолік в дизайні системи, реалізації, або операція та управління, які можуть бути використані для порушення політики безпеки системи [8].

Проблеми безпеки протоколу CAN. Протокол CAN має ряд властивих слабких місць, які є загальними для будь-якої реалізації. Розглянемо ключові серед них [3].

Широкомовна передача. Оскільки пакети CAN передаються фізично та логічно для всіх вузлів, зловмисник, який отримав доступ до мережі може легко переглянути всі повідомлення або відправляти пакети до будь-якого іншого вузла мережі.

Вразливість до атаки «відмова в обслуговувані». Протокол CAN надзвичайно уразливий для атак на відмову в обслуговуванні. Кожен ЕКУ має власний ідентифікатор, що представлений числом. Чим менше це число, тим більший пріоритет мають пакети від цього ЕКУ. Схема арбітражу CAN на основі пріоритетів дозволяє вузлу встановлювати "домінуючий" стан на шині і викликати відмову всіх інших вузлів шини CAN. Тобто зловмисник може надсилати пакети з найменшим можливим ідентифікатором і дані від інших ЕКУ не будуть пересилатися взагалі.

*Відсутність відміток про аутентифікацію***.** Пакети протоколу CAN не містять поля аутентифікації або навіть будь-якого поля ідентифікатора джерела пакета. Це означає, що будь-який компонент може надіслати пакет з ідентифікатором будь-якого іншого компонента. Будь-який скомпрометований компонент може використовуватися для управління всіма іншими компонентами в мережі.

Слабкий контроль доступу. ЕКУ використовують протоколи безпеки, де спочатку відбувається обмін даними для створення спільного криптографічного ключа. Проте було показано, що не всі ЕКУ використовують випадкові значення кожного разу або взагалі вимагають наявності ключа. Також в якості ключа можуть бути використані звичайні слова або вирази замість випадкових значень.

Загальний алгоритм виконання атаки через мережу CAN. Критичні з точки зору безпеки атаки проти автомобіля складаються з трьох етапів.

Перший етап полягає в тому, що зловмисник отримує доступ до внутрішньої автомобільної мережі. Це дозволяє зловмиснику вводити повідомлення в мережу автомобіля, прямо чи опосередковано контролюючи бажаний ЕКУ. Дослідники з Університету Вашингтона та університету Каліфорнії Сан-Дієго змогли отримати віддалене

виконання коду в модулі телематики автомобіля, використовуючи вразливість в програмному забезпеченні Bluetooth-модуля та скомпрометувати стільниковий модем [2].

Кібер-фізичні напади (атаки, що приводять до фізичного контролю різних аспектів автомобіля), з іншого боку, вимагатимуть взаємодії з іншими ЕКУ. Кібер-фізична атака, як правило, вимагає *другого етапу*, який передбачає ін'єкцію повідомлень у внутрішню автомобільну мережу, в спробі взаємодіяти з критично важливими ЕКУ, такими що відповідальні за керування, гальмування, прискорення, тощо.

Третій крок полягає в тому, щоб атакований ЕКУ здійснив певну поведінку, що погіршує безпеку автомобіля. Це передбачає реверс-інженірінг повідомлень у мережі та виявлення точного формату для виконання певних дій.

Моделювання загроз. Моделювання загроз - це процедура оптимізації безпеки мережі шляхом визначення цілей зловмисника та вразливостей, з подальшим визначенням контрзаходів для запобігання чи пом'якшення наслідків загроз для системи. У цьому контексті загроза являє собою потенційну або фактичну побічну подію, яка може бути шкідливою (наприклад, атакою на відмову в обслуговуванні) або випадковою (наприклад, збою пристрою зберігання даних), що може спричинити небезпеку для захищуваної системи.

Ключовий момент моделювання загроз полягає в тому, щоб визначити, де слід застосувати найбільше зусиль для забезпечення безпеки системи. Цей показник змінюється, коли додаються нові фактори, додається, видаляється або оновлюється програмне забезпечення, та розвиваються вимоги користувачів. Моделювання загрози - це ітеративний процес, який полягає у визначенні захищуваних активів, визначення того, що кожна програма робить щодо цих активів, створення профілів безпеки для кожної програми,

визначення потенційних загроз, визначення пріоритетів потенційних загроз та документування побічних явищ та дій, здійснених у кожній із них.

Стандарти безпеки автомобіля. Разом з все більшим використанням ЕКУ та більшої інтеграції інформаційних технологій в транспортний засіб, збої більше не стосуються зносу або порушенням електричних мереж, а помилкам програмування. Той факт, що електронні компоненти можуть впливати на фізичний світ, змусили виробників транспортних засобів та урядові організації визначити стандарт, згідно з яким виробники автомобілів повинні здійснювати роботу з ризиками. З цією метою в 2011 році стандарт ISO 26262 був прийнятий на базі вже існуючого стандарту IEC 61508, який був розроблений для кібер-фізичних систем та був змінений, щоб бути більш придатним для транспортних засобів [10].

ISO 26262 визначає функціональну безпеку електричних та електронних систем у транспортних засобах і вважається стандартом для функціональної безпеки автомобіля. Оцінка ризиків небезпеки відбувається з урахуванням трьох аспектів:

- *ступінь тяжкості* - ступінь тяжкості небезпеки, наприклад, чи є небезпека життю людей;
- *вплив* - вплив небезпеки або наскільки імовірною є небезпека;
- *контрольованість* - контрольованість небезпеки, чи здатен водій запобігти небезпеці шляхом, наприклад, гальмування.

Методологія моделювання загроз. В цій роботі використовується методологія моделювання загроз [4], розроблена саме для автомобілів. Вона сфокусована на виявлені загроз за умови, що зловмисник вже отримав доступ до системи або має можливість здійснити неправомірні дії. Це є доцільним, оскільки далі будуть розглянуті атаки, виконання яких було практично підтверджено. Згідно

з запропонованою методологією моделювання загроз складається з трьох етапів.

Етап 1. Визначення критичного програмного забезпечення (ПЗ) / програмної системи (ПС)

Критичними вважаються програми, які швидше за все призведуть до серйозних загроз і тому мають бути досліджені в першу чергу. В межах методології критична програма або система - це функціональність, яка будучи скомпрометованою, може призвести до серйозних наслідків, пов'язаних з безпекою або іншими способами. Далі для всіх ідентифікованих застосувань та систем застосовуються етапи 2 та 3.

Етап 2. Декомпозиція ПЗ / ПС

2.1 Створення діаграм взаємозв'язків в транспортному засобі (визначаються усі елементи, підсистеми та шини даних, які підключені до розглянутої системи, а також зовнішні з'єднання, такі як Wi-Fi, OBD-II, Bluetooth або стільниковий зв’язок)

2.2 Визначення високорівневих потоків даних в діаграмі взаємозв’язків

Етап 3. Виявлення та аналіз загроз

3.1 Ідентифікація загрози за допомогою класифікації загроз STRIDE. Під час першого кроку всі загрози ідентифікуються за допомогою класифікації загроз STRIDE [11]. Це означає, що для кожного ЕКУ, потоку даних та зовнішнього об'єкта по відношенню до мережі використовуються відповідні класи STRIDE для ідентифікації можливих загроз, в результаті чого з'являється список загроз для всіх компонентів системи.

3.2 Визначення тяжкості загроз.

Оцінювання тяжкості загроз. На етапі 3 кожна загроза оцінюється за двома критеріями: строгістю та керованістю. Для

визначення строгості (ступеня тяжкості наслідків) загрози використовується класифікація[5]. Ця класифікація наведена в таблиці 1 і дає чітке розмежування між наслідками для одного або декількох транспортних засобів та

Таблиця 1

Класифікація загроз для визначення ступеня строгості

Рівень	Ступінь впливу на			
	Безпека водія	Експлуатаційні характеристики автомобіля	Приватність даних водія	Фінансові ризики
0	Жодного впливу	Жодного впливу на експлуатаційні показники	Жодного неавторизованого доступу до даних	Жодних збитків
1	Незначний вплив	Непомітний для водія вплив	Доступ до даних, що не дозволяють ідентифікувати водія або автівки	Незначні збитки (до 10$)
2	Ризик для життя (з можливістю вижити) або помірні пошкодження для багатьох автомобілів	Водій помічає погіршення експлуатаційних показників або непомітний вплив на декілька автомобілів	Ідентифікація водія або автомобіля або деанонімізовані дані з декількох автомобілів	Помірні збитки (до 100$) або незначні збитки для багатьох автомобілів
3	Ризик для життя (з малою ймовірністю вижити) або суворі пошкодження для багатьох автомобілів	Значний вплив на експлуатаційні показники або помітний вплив на декілька автомобілів	Відстежування водія або автомобіля або ідентифікація багатьох водіїв або автомобілів	Значні збитки (до 1000$) або помірні збитки для багатьох автомобілів
4	Пошкодження з загрозою для життя та фатальними наслідками для багатьох автівок	Значний вплив на чисельні автомобілі	Відстежування багатьох водіїв або автомобілів	Значні збитки для багатьох автомобілів

сфокусована на наступних аспектах: безпека водія; експлуатаційні характеристики автомобіля; приватність даних; фінансові ризики.

Визначення того, якого з названих аспектів стосується кожна загроза, зазвичай робиться групою експертів. Стандарт ISO 26262 дає опис вимірювання керованості (таблиця 2).

Таблиця 2

Класифікація загроз за ступеню керованості

Рівень	Опис
0	Повністю контрольована ситуація
1	Легко контролюється водієм
2	Помірно контролюється (більшість водіїв можуть впоратися)
3	Водію важко контролювати ситуацію або непідконтрольне
4	Не може бути контрольованою

Використовуючи значення строгості та керованості, загальний рівень загрози вимірюється наступним чином [6]:

$$T = w_C C \cdot w_S S + w_O O + w_P P + w_F F \quad (1)$$

де T – кількісна оцінка загрози, C – оцінка керованості, S – оцінка безпеки, O – оцінка експлуатації, P – оцінка приватності, F – оцінка фінансових ризиків, w_C, w_S, w_O, w_P, w_F – відповідні вагові коефіцієнти, що обираються експертами.

Слід зауважити, що керованість має відношення лише до безпеки, оскільки інші категорії не контролюються водієм повністю або частково, тому значення для безпеки та керованості перемножуються.

Вибір вагових коефіцієнтів. Для обчислення оцінок загроз обираються вагові коефіцієнти для кожного аспекту згідно з пріоритетами при складанні моделі загроз. В даній роботи пріоритетом

є безпека і життя водія та пасажирів, а також вплив на експлуатаційні характеристики, оскільки вони також можуть мати вплив на безпеку водія під час руху. Приватність та фінансові ризики мають меншу пріоритетність, оскільки не пов'язані з фізичними загрозами для життя людини.

З огляду на це, далі використовуються наступні коефіцієнти:

$$w_C = w_S = 10,\ w_O = 7,\ w_P = w_F = 5 \qquad (2)$$

Модель класифікації загроз STRIDE. Класифікація загроз STRIDE була розроблена корпорацією Microsoft і використовувалась як частина їх концепції життєвого циклу безпечної розробки [12] для класифікації та виявлення потенційних загроз. Це акронім для наступних шести категорій загроз:

- підроблення ідентичності (**Spoofing identity**);
- порушення даних (**Tampering with data**);
- відмова від обов'язків (**Repudiation**);
- розкриття інформації (**Information disclosure**);
- відмова в обслуговуванні (**Denial of service**);
- перевищення привілеїв (**Elevation of privilege**).

Ідея методології STRIDE полягає в тому, щоб надати експертам із питань безпеки або тим, хто не є спеціалістом з питань безпеки інструменти для аналізу загроз безпеці.

Аналіз атак на ЕКУ автомобіля. Перед описом проаналізованих атак необхідно зазначити, що їх можна поділити за одним критерієм — чи необхідна була діагностична сесія для виконання атаки. За дизайном вона необхідна майстрам з авто центру для виявлення проблем в автомобілі та дозволяє робити операції, що недоступні звичайному користувачу. Тому неавторизований доступ відкриває значний простір для здійснення атак.

Оскільки відкриття діагностичної сесії зловмисником є

зловживанням, то згідно класифікації STRIDE усі атаки, що здійснюються з використання діагностичних команд, мають клас "Перевищення привілеїв".

Пакети, що використовуються ЕКУ при звичайних обставинах називаються нормальними. Їх використання зловмисником під час роботи автомобіля не може бути виявлено існуючими методами захисту. Виробники не надають формат пакетів у відкритому доступі, тому зловмисник вимушений спочатку виявити пакети та розібрати формат даних в кожному з них.

Використання методології моделювання загроз. Атаки, що розглянуті далі, виконані для Ford Escape 2010 та Toyota Prius 2010 [1] і проводились за допомогою нормальних пакетів. Атаки передбачають надсилання пакетів, що формуються та очікуються ЕКУ в мережі автомобіля, тому кожна атака має позначку про підроблення ідентичності (позначається літерою S).

Показ довільних значень на спідометрі (Форд). Атака дозволяє показати будь-які значення швидкості та обертів двигуна на приладовій панелі.

Показ довільних значень одометра (Форд). Ця атака проводиться так само, як і попередня.

Обмежена можливість керування (Форд). Атака являє собою відмову в обслуговувані. Цільовим є ЕКУ модуль керування рульовим управлінням (Power Steering Control Module). В результаті здійснення атаки автомобіль не допомагає під час керування, що робить складним поворот колес, а саме неможливо повернути колесо більш, ніж на 45% порівняно з нормальною роботою.

Показ довільних значень на спідометрі (Тойота). Атака проводиться так само, як і для Форда. Пакет з недійсними значеннями

швидкості необхідно надсилати безперервно, оскільки оригінальний пакет постійно надсилається.

Спрацювання гальм (Тойота). Атака експлуатує систему передбачування зіткненнь (Pre-Collision System), яка допомагає водію уникнути зіткнення з іншим автомобілем. Ця система має можливість змусити автомобіль загальмувати. Здійснення атаки призводить до зменшення швидкості або повного гальмування автомобіля. Результатом атаки є те, що автомобіль буде стояти, навіть якщо натиснути на педаль газу повністю.

Керування автомобілем (Тойота). Тойота має систему Intelligence Park Assist System (IPAS), яка допомагає водію під час паркування. Ця система має можливість змінювати напрямок руху автомобіля, проте лише при швидкості менш, ніж 4 миль/г. Атака полягає в підробці значень від ЕКУ, на дані від яких очікує система IPAS. Атака призводить до можливості повертати на будь-якій швидкості, але ці повороти є доволі різкими, що може спричинити додаткову небезпеку.

Для наступних атак автори роботи [3] не зазначили модель автомобіля з міркувань безпеки:

– *збільшення гучності радіо.*

– *віддалений старт автомобіля.*

– *вимикання двигуна* (атака була виконана на швидкості 40 миль/г, що призводить до раптової зупинки).

– *визначення автомобіля* [11] завдяки ідентифікаторам датчиків тиску повітря в шинах (кожен датчик має власний унікальний ідентифікатор).

– *запис розмов в салоні автомобіля* [2] завдяки доступу до вбудованого мікрофона через вразливість в ПЗ модуля телематики.

– *визначення положення автомобіля* [2] завдяки отриманню даних системи GPS через вразливість в ПЗ модуля телематики.

В таблиці 3 наведені числові оцінки строгості та керованості, а також значення загальної оцінки рівня розглянутих атак під час звичайної роботи автомобіля.

Таблиця 3

Значення оцінок строгості і керованості та загальної оцінки рівня атак під час звичайної роботи автомобіля

STRIDE	Безпека водія	Експлуатаційні характеристики	Приватність даних водія	Фінансові ризики	Керованість автомобіля	Оцінка загрози
1	**2**	**3**	**4**	**5**	**6**	**7**
Показ довільних значень на спідометрі						
S T	1	0	0	1	1	105
Показ довільних значень одометра (Форд)						
S T	0	0	0	2	0	10
Обмежена можливість керування (Форд)						
D	2	2	0	2	2	424

Продовження таблиці 3

1	**2**	**3**	**4**	**5**	**6**	**7**
Показ довільних значень на спідометрі (Тойота)						
S T	1	0	0	1	1	105
Спрацювання гальм (Тойота)						
S T R	2	3	0	3	3	636
Керування автомобілем (Тойота)						
S T R D	3	3	0	3	3	936
Збільшення гучності радіо						
S T	1	0	0	0	1	100
Віддалений старт автомобіля						
S T	0	0	0	3	4	15
Вимикання двигуна						
S T R	4	3	0	3	3	1236
Визначення автомобіля						
I	0	0	3	0	0	15

Запис розмов в салоні автомобіля						
I E	0	0	3	0	0	15
Визначення положення автомобіля						
I E	0	0	3	0	0	15

Атаки за допомогою діагностичних команд. Кожна атака з перелічених нижче здійснюється після встановлення діагностичної ситуації, що є перевищенням привілеїв. Тому кожна атака має відповідний клас в стовпчику для класифікації STRIDE. Опис та результати атак [1] зроблені для Ford Escape 2010 та Toyota Prius 2010.

*Спрацювання гальм (Форд). А*така можлива лише, коли авто припарковано, жодної загрози для життя водія немає. Неможливість розпочати рух унеможливлює найважливішу функцію автомобіля. Після проведення атаки рух стає неможливим, незалежно від того як водій тисне на педаль газу.

Блокування гальм (Форд). Результатом є неможливість зупинити авто при швидкості 5 миль/г та менше. Водій вимушений шукати можливість зупинити шляхом зіткнення з найменшими наслідками для нього та оточуючих автомобілів і людей.

Вимкнення фар та освітлення (Форд). Існує діагностична команда яка змушує ЕКУ Smart Junction Box вимкнутися. Разом з цим перестають працювати усі пристрої, що залежать від його роботи. Це фари, внутрішнє освітлення, радіо і т. д. Ця атака стає вкрай небезпечною для водія в умовах обмеженої видимості (під час дощу, туману).

Вимикання двигуна (Форд). Вимикання двигуна на довільній швидкості призведе до зупинки шляхом зіткнення. У разі, коли поруч

знаходяться інші автомобілі, вони можуть зіткнутися з атакованим автомобілем, що становить загрозу і для їх безпеки.

Вимикання двигуна (Тойота). На відміну від попередньої, ця атака можлива лише, коли автомобіль припаркований, тому вона не становить загрозу для водія.

Вмикання/вимикання гудка (Тойота). Постійний звук гудка зменшує зосередженість водія на ситуації на дорозі, також становить стресову ситуацію, що негативно впливає на здатність адекватно та вчасно реагувати на події під час їзди.

Відкривання /замикання дверей – Тойота. В першу чергу атака забезпечує фізичний доступ до салону та багажника автомобіля. Закриття дверей водієм або пасажиром не допоможе впоратися з атакою, оскільки повторне виконання атаки знову відчинить двері.

Показ довільних значень на індикаторі палива (Тойота). Атака приводить до того, що водій бачить, що палива вдосталь, хоча воно закінчується. Це може призвести до раптової зупинки під час руху.

А тепер наведемо перелік атак для ЕКУ Body Control Module [3]:

- постійна активація реле блокування дверей;
- безперервна робота склоочисників;
- відкриття багажника;
- відміна блокування положення дросельної заслінки (результатом атаки є вплив на дросельну заслінку, яка регулює постачання палива до двигуна і зміна швидкості без дій з боку водія);
- відкриття усіх дверей;
- постійна робота гудка;
- вимикання усього допоміжного освітлення - найбільший ризик атака завдає в умовах обмеженої видимості;
- безперервна подача рідини для склоочисників.

Атаки на ЕКУ модуль керування двигуном [3]:

– тимчасовий приріст кількості обертів двигуна;

– вимикання циліндрів двигуна, рульового управління, гальм – особливістю є те, що водій має можливість скасувати результат атаки (наприклад, завести двигун), що значно збільшує ймовірність того, що водій впорається з ситуацією;

– вимикання двигуна – водій може завести повторно двигун, що зменшує негативні наслідки атаки;

– збільшення кількості обертів двигуна в режимі спокою.

В таблиці 4 наведені числові оцінки строгості та керованості, а також значення загальної оцінки рівня розглянутих атак, що можуть мати місце під час діагностики.

Таблиця 4

Значення оцінок строгості і керованості та загальної оцінки рівня атак за допомогою діагностичних команд

STRIDE	Безпека водія	Експлуатаційні характеристики	Приватність даних водія	Фінансові ризики	Керованість автомобіля	Оцінка загрози
1	**2**	**3**	**4**	**5**	**6**	**7**
Спрацювання гальм (Форд)						
S T R	0	3	0	0	4	15
Блокування гальм (Форд)						
S T R	2	3	0	2	3	631
Вимкнення фар та освітлення (Форд)						
S T R	2	2	0	3	2	429
Вимикання двигуна (Форд)						
S T R	0	3	0	0	4	21
1	**2**	**3**	**4**	**5**	**6**	**7**
Вмикання/вимикання гудка (Тойота)						
S T R	1	0	0	0	3	300
Відкривання /замикання дверей (Тойота)						
S T R	2	2	0	3	2	429
Показ довільних значень на індикаторі палива (Тойота)						

S T R	2	1	0	3	2	422
Постійна активація реле блокування дверей						
R E	1	2	0	0	1	114
Безперервна робота склоочисників						
R E	1	0	0	0	1	100
Відкриття багажника						
S T E	0	0	0	3	3	15
Відміна блокування положення дросельної заслінки						
R E	2	2	0	0	2	400
Відкриття усіх дверей						
R E	1	2	0	3	2	229
Постійна робота гудка						
S R E	1	0	0	0	1	100
Вимикання усього допоміжного освітлення						
S R E	2	2	0	3	4	829
Безперервна подача рідини для склоочисників						
S R E	2	2	0	3	3	629
Тимчасовий приріст кількості обертів двигуна						
S R E	2	3	0	2	3	631
Вимикання циліндрів двигуна, рульового управління, гальм						
S R E	3	3	0	3	3	921
Збільшення кількості обертів двигуна в режимі спокою						
S R E	2	2	0	2	2	424
Спрацювання гальм для передніх колес						
S R E	3	4	0	4	4	1248
Розблокування гальм, запобігання гальмуванню						
S R E	4	4	0	4	4	1648

Результати оцінювання. Отримані оцінки знаходяться в широкому діапазоні, що свідчить про значну кількість атак, що можуть бути здійснені. Оцінювання загроз дозволяє порівняти загрози між собою та виявити ті, що являють собою найбільшу небезпеку. Ось перелік загроз, що мають найвищі оцінки: розблокування гальм,

запобігання гальмуванню (1648); спрацювання гальм для передніх колес (1248); вимикання двигуна (1236). Тоді як найменші оцінки мають показ довільних значень одометра (10); відкриття багажника (15) та загрози, що можуть бути здійснені лише тоді, коли автомобіль припаркований: вимикання двигуна (Тойота) (21) та спрацювання гальм (Форд) (15). Найбільш вплив на оцінку має факт можливості здійснення неавторизованих дій під час руху автомобіля, чи існує загроза для інших транспортних засобів на дорозі та наскільки важко водію впоратися з наслідками здійснення атаки.

Висновки. Відсутність механізмів безпеки проти інформаційних атак призвела до того, що зловмиснику здатен значно вплинути на роботу автомобіля та безпеку людей всередині. Зловмисник має можливість впливати на компоненти автомобіля починаючи з радіо і закінчуючи двигуном.

Це результат того, що автомобілі стали привертати увагу хакерів нещодавно і виробникам транспортних засобів не було потреби впроваджувати механізми інформаційної безпеки. ЕКУ автомобіля використовують протокол CAN для обміну даними між собою, який був представлений ще у 1980-х. На той час не було потреби в інформаційній безпеці і тому вона не бралася до уваги під час розробки протоколу. Все це свідчить про те, що існує потреба в кардинально нових рішеннях для автомобілів та урахування вимог інформаційної безпеки ще на етапі проектування.

В даній роботі була надана оцінка практично здійсненим атакам з урахуванням наступних критеріїв: безпека водія, вплив на експлуатаційні характеристики автомобіля, приватність даних водія, фінансові ризики та керованість автомобіля. Оцінка залежить від вагових коефіцієнтів, які визначають пріоритети під час оцінювання. Життю водія та його здатності впоратися з наслідками атаки в цій

роботі були надані найвищі пріоритети. Як результат, високі оцінки отримали атаки, що можуть бути здійснені під час руху автомобіля та ті, що суттєво впливають на можливість водія контролювати рух. Тоді як атаки, що дозволяють, наприклад, отримати фізичний доступ до салону автомобіля мають низькі оцінки.

Застосований підхід дозволяє порівнювати атаки між собою, особливо ті, що на думку експерта здаються однаковими за наслідками. Також це дозволяє виробникам транспортних засобів виявити найбільш серйозні за наслідками атаки та зосередитися саме на них, що призводить до грамотного планування ресурсів.

Література:

1. Dr. Charlie Miller, Chris Valasek, "Adventures in Automotive Networks and Control Units". [Електронний ресурс]: http://illmatics.com/car_hacking.pdf.

2. S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces". In Proceedings of the 20th USENIX Conference on Security, SEC'11.

3. K. Koscher et al., "Experimental security analysis of a modern automobile," in Proceedings — IEEE Symposium on Security and Privacy, 2010, pp. 447–462

4. Winsen, Stijn van, "Threat Modelling for Future Vehicles, On Identifying and Analysing Threats for Future Autonomous and Connected Vehicles", 2017. [Електронний ресурс]: http://essay.utwente.nl/71792/.

5. David Ward, Ireri Ibara, and Alastair Ruddle. "Threat Analysis and Risk Assessment in Automotive Cyber Security." In: SAE International Journal of Passenger Cars-Electronic and Electrical Systems 6.2 (2013), pp. 507–513. ISSN: 1946-4622. DOI: doi:10.4271/2013-01-1415

6. Ishtiaq Roufa et al., “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”. ISBN: 888-7-6666-5555-4.

7. ISO 11898-1:2003 - Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signaling.

8. RFC2828. Shirey, R., "Internet Security Glossary", RFC 2828, DOI 10.17487/RFC2828, May 2000.

9. ISO/IEC, "Information technology - Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008.

10. ISO. ISO 26262. Road vehicles – Functional safety. ISO 26262:2012. Geneva, Switzerland: Internation Organization for Standardization, 2012.

11. The STRIDE Threat Model. [Електронний ресурс]: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

12. The Trustworthy Computing Security Development Lifecycle. [Електронний ресурс]: https://msdn.microsoft.com/en-us/library/ms995349.aspx.

13. Ishtiaq Roufa et al., “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”. ISBN: 888-7-6666-5555-4.