УДК 629.05+681.5+004.32

ІНФОРМАЦІЙНА БЕЗПЕКА НА АВТОМОБІЛІ ТА АВТОМОБІЛЬНОМУ ТРАНСПОРТІ

Кривошапов Сергій Іванович, канд. техн. наук, доцент кафедри «Технічної експлуатації та сервісу автомобілів ім. проф. Говорущенко М.Я.», Харківський національний автомобільно-дорожній університет

Анотація. Вказано на широке використання мікропроцесорних систем керування у сучасному автомобілі. Розглядаються різні канали передачі в цифрових системах управління, які можуть передавати дані всередині системи управління, між системами всередині транспортного засобу чи зв'язувати автомобіль із зовнішніми системами. Наведено основні причини порушення роботи системи керування автомобілем під внутрішнім та зовнішнім впливом. Вказано основні шляхи інформаційних загроз для персональних комп'ютерів та серверів, які використовуються для управління діяльністю підприємства автомобільного транспорту.

Ключові слова: транспорт, автомобіль, інформаційні технології, мережа, система управління, передача даних, кібербезпека, програмне забезпечення

Конструкція сучасного автомобіля все більше використовує електронні компоненти, що базуються на мікропроцесорних системах обробки даних, мережевих технологій прийому та передачі сигналів, комунікаційних систем загальної взаємодії елементів інформаційної системи [1]. В автомобіль широко використовуються мультимедійні технології, взаємодії з хмарними сестрами, телефонні та супутникові канали радіозв'язку, що дозволяють взаємодіяти з дорожньою інфраструктурою та центрами управління.

Для керування двигуном, трансмісією, підвіски, гальмівної системи та рульового керування, освітлення та комфорту використовуються електронні блоки управління (ЕБУ), з'єднані між собою різними каналами передачі даних:

- Controller Area Network (CAN) – об'єднана промислова мережа виконавчих пристроїв та датчиків, розроблена фірмою Bosch у середині 1980-х років;
- FlexRay – високошвидкісна мережа для автомобілів, заснована компаніями Philips спільно з BMW, Daimler, Bosch, General Motors та Volkswagen у 2004 році;
- Local Interconnect Network (LIN) – мережа для управління автомобільними системами низької відповідальності, розроблена консорціумом європейських автовиробників: Audi, BMW, Daimler Chrysler, Motorola, Volkswagen, Volvo та ін. у 1999 році;
- Media Oriented Systems Transport (MOST) – високошвидкісна мультимедійна автомобільна мережа, розроблена Microchip Technology;
- Ethernet – сімейство провідних мереж (LAN, MAN, WAN) передачі даних між комп'ютерами, яка розроблена фірмою Xerox 1973 року;
- Wi-Fi (Wireless Fidelity) – бездротова локальна мережа між пристроями, розроблена CSIRO у 1997 році.

Із зовнішнім світом сучасний автомобіль спілкується через канали супутникового зв'язку, використовує систему глобального позиціонування GPS (Global Positioning System), підтримує стандарти цифрового мобільного зв'язку GSM (Global System for Mobile Communications) та GPRS (General Packet Radio Service), протоколи радіозв'язку Wi-Fi та Bluetooth.

Сигнали від датчиків до мікропроцесора також можуть передаватися за

стандартними протоколами зв'язку:

- I²C (Inter-Integrated Circuit) - послідовний асиметричний канал для зв'язку між інтегральними схемами всередині електронних приладів, розроблений фірмою Philips;
- 1-Wire – двонаправлений однопровідний канал зв'язку для пристроїв із низькошвидкісною передачею даних, розроблений фірмою Maxim Integrated;
- SPI (Serial Peripheral Interface) - послідовний синхронний канал передачі в режимі повного дуплексу;
- UART (Universal Asynchronous Receiver-Transmitter) - двонаправлений канал зв'язку між цифровими пристроями.

Розвиток різних систем комунікації дозволяє оперативно отримувати та передавати інформацію про режим функціонування систем на автомобілі, дані про стан виконавчих елементів, відомості про місцезнаходження автомобіля та ін.

Використання стандартизованих каналів (протоколів) зв'язку дозволяють розширювати можливості інформаційної системи автомобіля без значних витрат на проектування архітектури, використовувати розподілену систему для збору та обробки даних, залучати різних розробників та технології.

Однак через канал зв'язку можуть передаватися помилкові або спотворені дані, які заважатимуть надійній роботі системи керування автомобілем. Порушення можуть відбуватися на сигнальному (невідповідність рівня напруги на лінії), логічному (порушення послідовності передачі даних та сигналів, що управляють передачею) або інформаційному (передача неправильних даних) рівні.

Канали зв'язку можуть бути використані для несанкціонованого доступу до даних, з метою їх перехоплення або цілеспрямованої зміни [2]. Основні види ризику з порушення кібербезпеки на транспортному засобі відображено у документі [3].

Джерелом загрози безпеці може бути внутрішні елементи автомобіля. До автомобіля можуть бути підключені пристрої, які порушують роботу системи керування автомобілем. Також до автомобіля можуть бути підключені пристрої, які виконують, крім основної заявленої функції, приховані функції, які спрямовані на збір даних або порушення роботи систем на автомобілі. Шкідлива програма може видаляти чи спотворювати дані, які передаються між різними блоками керування по шині. Програма може блокувати певні блоки керування або генерувати нові дані, імітуючи роботу блоків керування, яких фізично немає в автомобілі.

Загрозою безпеки може бути зовнішній вплив, спрямований на канал зв'язку транспортного засобу із зовнішнім світом. Зловмисниками може бути організована DoS атака – надходження великої кількості запитів на обслуговування, як правило, з різних джерел, що призводить до порушення роботи сервісу, якій відповідає за обробку повідомлень по каналах зв'язку.

Основна мета зловмисника – отримати привілейований доступ до ядра програмного забезпечення. Тоді шкідлива програма матиме доступ до всіх даних, які не можуть бути виявлені системою безпеки. Шкідлива програма може керувати системою безпеки і змінювати логіку роботи ядра. За певною подією або часом, шкідлива програма може включити свій алгоритм управління, який може призвести до катастрофи.

Розробники шкідливих програм можуть аналізувати та використовувати вразливості програмного забезпечення, встановленого виробником обладнання. Також використовуються вразливість неякісного оновлення, особливо якщо таке оновлення виконується каналами спільного зв'язку.

Передача даних по широкомовних каналах, до яких належить радіозв'язок та Інтернет, може бути перехоплена стороннім програмними або апаратними засобами, які знаходяться в зоні дії мережі. Шляхом запису та подальшого аналізу всього або вибіркового трафіку, зловмисник може отримати відомості про приховану інформацію.

Інтерес представляє коди доступу, паролі та ключі до шифрування даних. Частина даних може бути записана та згодом відтворена у необхідний для зловмисника час.

На інформаційну безпеку впливає людський фактор, який може вносити зміни до електричної схеми плати контролера, перепрограмувати пам'ять блоку управління, встановлювати неперевірені прошивки, підключати сумнівне обладнання та ін.

Аналізуючи дані, отримані шляхом несанкціонованого доступу до каналу передачі, зловмисник може отримати інформацію про транспортний засіб. Інтерес представляють ідентифікатори автомобіля, версії програм і прошивок, режим використання (пробіг, швидкість та напрямок руху), дані з датчиків, журнал відмов, дані поточного стану, параметри конфігурації, дані моніторингу тощо. Метою несанкціонованого доступу може бути конфіденційна інформація про власника: особисті дані, режим роботи та відпочинку, інформація про рахунки, дані про контакти, інформація про місцезнаходження, особисті уподобання та ін.

Часто кібератака на автомобіль здійснюється для його несанкціонованого заволодіння шляхом відключення системи охорони або іммобілайзера, а також інших систем, які дозволяють відстежити або вплинути на роботу викраденого автомобіля.

Впроваджене шкідливе програмне забезпечення може негативно впливати на роботу водія, викликаючи збої в роботу систем автомобіля, виконуючи виведення незрозумілої або неправдивої інформації на панель приладів, зміни налаштування системи забезпечення комфорту, записувати або видаляти коди несправності бортової системи самодіагностики. Небезпечно, якщо порушуватиметься робота тих систем автомобіля, які відповідають за безпеку: система гальмування, кермового керування, світлової сигналізації тощо.

Інформаційна безпека поширюється не тільки на транспортний засіб, але й на сервери та комп'ютери, на яких проводиться обробка транспортної, логістичної та діагностичної інформації. В даний час найкращий захист мають хмарні сервери. Погано можуть бути захищені комп'ютери, які знаходяться на підприємстві автомобільного транспорту, особливо якщо один комп'ютер виконує кілька сервісних функцій (база даних, Веб-сервер, файловий сервер, поштовий сервер і т.п.). На таких підприємствах рідко працюють професійні адміністратори та фахівці кібербезпеки. Тому такі комп'ютери вразливі до поширення вірусів, можуть мати низький захист мережі, на них може бути встановлено не ліцензійне програмне забезпечення, нерідкі випадки поширення шкідливих програм через USB або Інтернет. Метою шахраїв – це персональні та фінансові дані, впровадження модулів для проведення DoS атак, віддалене керування комп'ютером тощо [4].

Широке впровадження інформаційних технологій у всі сфери діяльності, включаючи транспорт, вимагає професійного підходу до забезпечення кібернетичної безпеки на всіх рівнях.

Література

1. Мигаль В.Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Х.: Майдан, 2018. 262 с.
2. Колодяжний В.М., Левтеров А.І., Малащук Є.В. Кібербезпека автомобілів: історія цифровізації автомобілів, поточний стан проблеми, цілі сталого розвитку та стандарти, Вісник ХНАДУ, Вип. 96, 2022, С. 59-65.
3. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, UN Regulation No. 155. URL: https://eur-lex.europa.eu/eli/reg/2021/387/oj.
4. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны, ДМК Пресс, 2020, 326 с.