УДК 629.3

ЕЛЕКТРОМОБІЛЬ ЯК КІБЕРФІЗИЧНА СИСТЕМА

Смирнов Олег Петрович, докт. техн. наук, професор кафедри автомобільної електроніки, Харківський національний автомобільно-дорожній університет, e-mail: smirnov1oleg@gmail.com, ORCID: 0000-0003-4881-9042
Борисенко Анна Олегівна, канд. техн. наук, доцент кафедри автомобільної електроніки, Харківський національний автомобільно-дорожній університет, e-mail: anutochka2111@gmail.com, ORCID: 0000-0001-5992-8274
Думчіков Дмитро Васильович, магістрант, Харківський національний автомобільно-дорожній університет

Сучасні електромобілі – це складні кіберфізичні системи, що інтегрують телематику, інтерфейси зв'язку від транспортного засобу до всієї інтелектуальної транспортної інфраструктури V2X (Vehicle-to-Everything (V2X)), системи управління силовою установкою, акумуляторними батареями, тощо [1]. Він містить до сотень електронних блоків керування, з'єднаних в мережу через бортові шини. Електронні блоки керують критично важливими функціями електромобіля, такими як заряджання акумулятора, керування двигуном, функції автономного водіння та інформаційно-розважальна система. Тісна інтеграція кібер- та фізичної областей означає, що кібератаки можуть мати прямі фізичні наслідки для безпеки та надійності як окремих транспортних засобів, так і інтелектуальної транспортної системи в цілому [2].

Останні роки виявили численні автомобільні вразливості та інциденти, які демонструють, що електромобілі не застраховані від кіберзагроз. Наприклад, відсутність шифрування або автентифікації в шині CAN дозволяє зловмисникам впроваджувати шкідливі повідомлення, які можуть порушити або взяти під контроль функції транспортного засобу. Тому забезпечення кібербезпеки електромобілів, як кіберфізичних систем, має першорядне значення.

Шина CAN наразі не має вбудованої кібербезпеки. Надсилання кожного повідомлення до кожного електронного блока керування та дозвіл на появу «нових» систем без будь-якого адміністративного підтвердження є критичним ризиком. Взаємозв'язок кожного бездротового пристрою з шиною CAN створив багато точок атаки на цю критично важливу кіберфізичну систему. Доступ до шини CAN, підключеної до критично важливих компонентів транспортного засобу, може призвести до небезпечних ситуацій на дорозі. Хоча заходи щодо пом'якшення деяких виявлених загроз були застосовані, кібербезпека має бути включена до всіх майбутніх проектів. Якщо сама шина CAN не буде перероблена для забезпечення кращої кібербезпеки, то мережева конструкція транспортного засобу повинна враховувати захист критично важливих компонентів, підключених до шини CAN. Прогнозується, що мережі транспортних засобів лише ускладняться, а кібератака на автомобіль може поставити під загрозу людські життя.

Електромобілі, що підключаються до зовнішньої інфраструктури V2X (зарядних станцій, інтелектуальних транспортних систем, електричних мереж, хмарних сервісів тощо) за допомогою таких протоколів, як OBD-II, ISO 15118 та технології транспортний засіб – електрична мережа V2G (Vehicle-to-Grid (V2G)), ще більше розширює можливість кібератаки [3]. Хоча такі підключення дозволяють надавати інноваційні послуги, вони також вводить нові шанси для кібервторгнень.

Можливі вектори кібератаки на електромобіль наведені на рисунку 1.

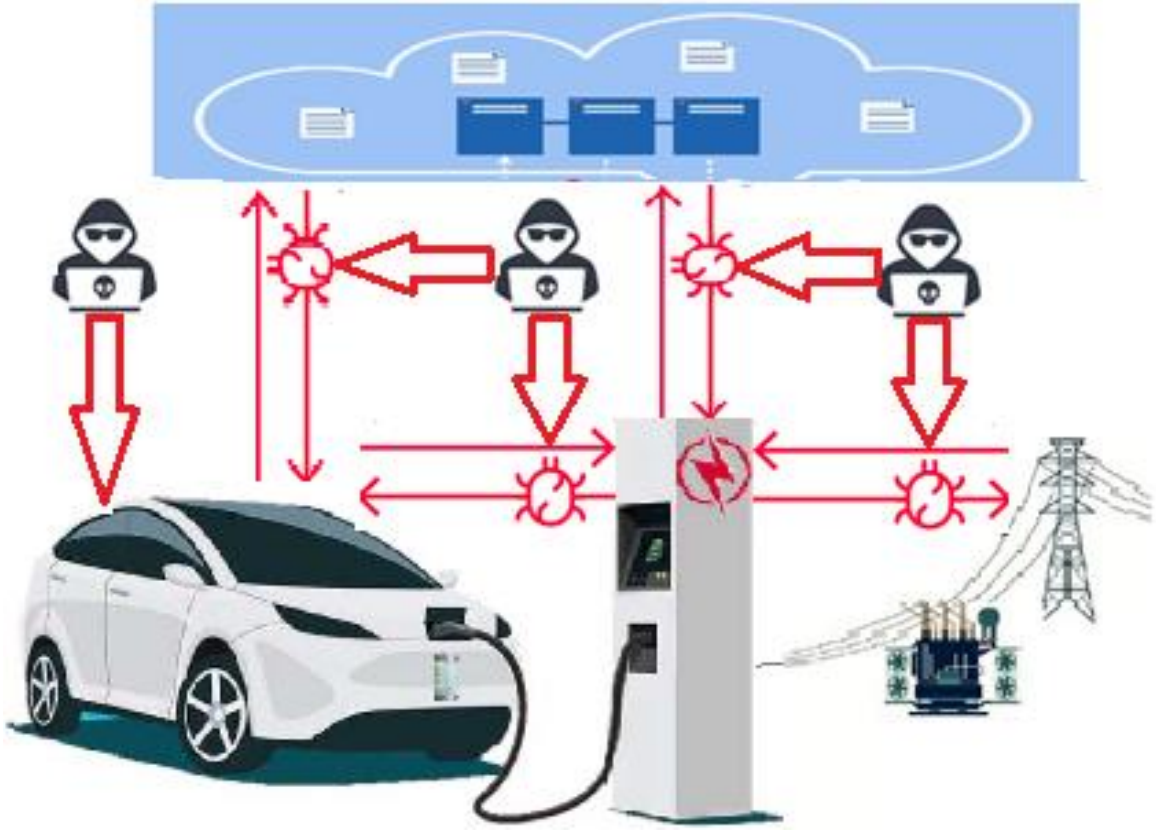

Рисунок 1 – Можливі вектори кібератаки

Загрози включають:

- впровадження шкідливого програмного забезпечення, коли зловмисники можуть впроваджувати шкідливий код у програмне забезпечення зарядної станції, який потім може заразити будь-який електромобіль, що підключається до неї;

- кібератаки типу «відмова в обслуговуванні», які можуть порушити доступність зарядних станцій;

- крадіжки конфіденційної інформації, при якої хакери можуть викрасти особисту та платіжну інформацію, перехоплюючи зв’язок між транспортним засобом, зарядним пристроєм та системою керування;

- кібератака на хмарні та серверні системи, які керують сеансами нарахування плати, автентифікацією та виставленням рахунків. Порушення цих систем може розкрити конфіденційні дані користувачів і дозволити злочинцям змінювати нарахування плати;

- кібератака на зарядні станції може створити штучні сплески або падіння попиту на енергію, потенційно дестабілізуючи електричну мережу та спричиняючи масові відключення електроенергії;

- кібератака при оновленні автомобільного програмного забезпечення по повітрю можна запровадити шкідливе програмне забезпечення, яке може привести до непередбачуваних аварійних ситуацій;

- кібератака на програмне забезпечення електромобіля.

Наприклад, шкідливе програмне забезпечення, впроваджене в бортові мережі транспортного засобу, може дозволити хакеру отримати контроль над життєва важливими функціями, такими як прискорення, гальмування та рульове керування, створюючи серйозну фізичну загрозу безпеці. Кібератака може перешкоджати роботі таких удосконалених системи допомоги водієві, як адаптивний круїз-контроль, утримання смуги руху та виявлення пішоходів, наражаючи на небезпеку пасажирів та інших учасників дорожнього руху. Зловмисні маніпуляції з акумуляторною батареєю та системами заряджання електромобіля можуть призвести до перегріву акумулятора, що потенційно може спричинити пожежу.

Прикладом сучасної системи виявлення та запобігання кібервторгненням електромобілів може бути система xCarbon від VicOne, яка забезпечує специфічні функції виявлення кібербезпек для архітектури електронних систем електромобілів. Система виявлення та запобігання вторгненням xCarbon адаптується до різних типів електронного обладнання, від звичайних мікроконтролерів до високоефективних складних комп’ютерних систем. Завдяки своїм гнучким перевагам xCarbon ефективно виявляє шкідливу активність системи, мережеві загрози та аномалії в CAN шині з мінімальним використанням процесора та пам'яті. Система xCarbon забезпечує самозахист інтелектуальних транспортних засобів використовуючи обчислювальну основу штучного інтелекту на базі нейронних процесорів, функція Edge AI від xCarbon може співвідносити дані про транспортний засіб та події безпеки між кількома електронними блоками керування двигуном, акумуляторної батареї, вдосконалених систем допомоги водієві тощо через центральний шлюз. В результаті використання системи xCarbon транспортні засоби можуть навчатися, розпізнавати загрози та захищатися, зменшуючи залежність від хмарних технологій, знижуючи витрати та забезпечуючи безпеку даних [4].

Висновки

Електромобілі необхідно розглядати як кіберфізичні системи, тому що вони включають як фізичні системи, так і інтегровані обчислювальні блоки керування. Така інтеграція створює численні «поверхні кібератаки», які можуть бути використані кіберзлочинцями. Кібербезпека електромобілів повинна захищати від атак як сам транспортний засіб, так і зовнішні системи, до яких він підключається.

Література

1. Tirulo A., Chauhan S., Shafie-khah M. LLM-Powered Threat Intelligence: Proactive Detection of Zero-Day Attacks in Electric Vehicle Cyber-Physical Systems. Sustainable Energy, Grids and Networks. 2025. P. 101877. URL: https://doi.org/10.1016/j.segan.2025.101877 (date of access: 06.10.2025).
2. Cybersecurity in vehicle-to-grid (V2G) systems: A systematic review / M. A. Razzaque et al. Applied Energy. 2025. Vol. 398. P. 126364. URL: https://doi.org/10.1016/j.apenergy.2025.126364 (date of access: 06.10.2025).
3. A Comprehensive Review of Vehicle-to-Grid (V2G) Technology as an Ancillary Services Provider / S. Alamgir et al. Results in Engineering. 2025. P. 106813. URL: https://doi.org/10.1016/j.rineng.2025.106813 (date of access: 06.10.2025).
4. xCarbon. VicOne. URL: https://vicone.com/products/xcarbon (date of access: 06.10.2025).

УДК 656.1.078:004.056

СУБ'ЄКТИ ПРОВЕДЕННЯ ОБОВ'ЯЗКОВОГО ТЕХНІЧНОГО КОНТРОЛЮ ТРАНСПОРТНИХ ЗАСОБІВ: СУТНІСТЬ ТА ОСОБЛИВОСТІ ДОТРИМАННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Віштак Інна Вікторівна, канд. техн. наук, доцент кафедра БЖДПБ,
Вінницький національний технічний університет,
e-mail: innavish322@gmail.com, ORCID: 0000-0001-5646-4996
Майданевич Леонід Олександрович, адвокат, канд. філос. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет,
e-mail: lmaidanevych@gmail.com, ORCID: 0000-0002-7364-8874

Актуальність теми роботи пов'язана з тим, що забезпечення технічного захисту інформації в інформаційно-комунікаційних системах суб'єктів проведення обов'язкового технічного контролю транспортних засобів є ключовою умовою дотримання вимог законодавства України у сфері безпеки дорожнього руху та цифрової безпеки. Недотримання встановлених стандартів призводить до ризику несанкціонованого доступу, втрати або викривлення даних про результати технічного контролю, що негативно впливає на функціонування Єдиного державного реєстру транспортних засобів та підриває довіру до державної системи контролю. У контексті цифрової трансформації та зростання кіберзагроз дана проблема набуває особливої актуальності.

Метою дослідження є визначення основних вимог та розробка практичних рекомендацій щодо приведення робочих місць суб'єктів обов'язкового технічного контролю у відповідність до норм законодавства України у сфері технічного захисту інформації.