ВИКОРИСТАННЯ ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАСОБІВ АВДЕНТИФІКАЦІЇ АВТОМОБІЛЯ

Фесенко Д. О., Горбенко І. Д.
Харківський національний університет радіоелектроніки, Харків, Україна

Можливості обходу систем захисту все більше цікавлять зловмисників, зокрема можливості модифікації та підміни даних в них, на що вони витрачають багато ресурсів для відкриття нових можливостей для компрометації роботи систем, тому до систем безпеки пред'являються все більш жорсткі вимоги щодо забезпечення ефективності та безпечності їх функціонування. Розглянені сучасні системи захисту від незаконного заволодіння автотранспортом, більш відомі всім як «сигналізація» намагаються стримувати атаки зловмисників, але в свою чергу можуть привносити додаткові бекдори для зловмисників зовсім ненавмисно, наприклад додаючи цікаву функцію в систему автомобіля, а згодом ця функція може мати двояке значення через проблеми з системою авдентифікації[2]. Тож, виходячи з цього, системи безпеки автомобіля повинні мати найвищий рівень безпеки авдентифікації, для реалізації якого пропонується використання децентралізованої мережі блокчейн[1] з вузлами для кожного автомобіля, що авдентифікують користувача групово, це дозволить відійти від стандартної клієнт-серверної архітектури, що є не достатньо захищеною. Основними шляхами вирішення зазначеної проблеми є побудування комплексної системи безпеки, що в свою чергу включає покращений та надійний захід авдентифікації на основі децентралізованої мережі блокчейн та двох комплексних схем оновлення системи передачі критичних даних автомобіля – мережі CAN[2].

Метою доповіді є розгляд особливостей використання технології блокчейн в системі авдентифікації автомобіля дозволить розширити можливості безпеки авдентифікації для доступу до автомобіля, роблячи цей процес в той самий час простішим для користувача, бо всі дії можна виконувати за допомогою смартфону, що працює на широко відомій платформі, але ж і в одночас підвищується рівень безпеки та довіри, в одночас не вимагає додаткових грошових вкладень, є легким до налаштування та використання та є гарно захищеним як від поствантових атак так і від інших видів атак, що зараз є дуже загрозливими для безпеки сучасної автоіндустрії.

Список літератури

1. NISTIR 8202. Blockchain Technology Overview / NIST // NISTIR. – Gaithersburg, US Department of Commerce, 2017. – C.1-26..

2. Brown. Vehicle Security Systems: Build Your Own Alarm and Protection Systems,: Newnes, 160, 1996. – C. 7 – 155.