

УДК 004.056:629.331

М. Демчишин; В. Тимошук; В. Шиманська; Д. Тимошук

(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КІБЕРЗАГРОЗИ СЕНСОРНИМ ПІДСИСТЕМАМ АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБІВ

UDC 004.056:629.331

M. Demchyshyn; V. Tymoshchuk; V. Shymanska; D. Tymoshchuk

CYBER THREATS TO SENSOR SUBSYSTEMS OF AUTONOMOUS VEHICLES

Автономні транспортні засоби (АТЗ) є технологічним проривом, який обіцяє змінити сучасну транспортну інфраструктуру, забезпечивши підвищення ефективності, зниження кількості дорожньо-транспортних пригод та покращення якості перевезень. Завдяки використанню численних сенсорів, таких як LiDAR [1], камери, радары та ультразвукові датчики, АТЗ здатні аналізувати навколишнє середовище, ідентифікувати об'єкти, передбачати дії інших учасників руху та приймати рішення в реальному часі (рисунк 1).



Рисунок 1. Сенсори автономного транспортного засобу

Проте впровадження цієї технології супроводжується серйозними викликами в галузі кібербезпеки, особливо в контексті захисту критично важливих сенсорних підсистем. Ключовою складовою функціонування автономного транспорту є точне сприйняття навколишнього середовища. Залежність від сенсорних систем створює вразливості, які можуть бути використані зловмисниками для компрометації безпеки транспортного засобу. Такі атаки можуть включати викривлення даних, відтворення попередніх показників або повне відключення сенсорів. Найбільшу загрозу становлять атаки, спрямовані на сенсори, адже вони можуть створити небезпечні ситуації, що безпосередньо впливають на керування та прийняття рішень. Наприклад, маніпуляція даними LiDAR може привести до хибної ідентифікації об'єктів або створення «сліпих зон», що унеможливує адекватне реагування транспортного засобу.

Зростаюча складність сучасних сенсорних систем вимагає розробки ефективних моделей захисту. Найбільш імовірними є атаки з частковою інформацією, коли зловмисник має обмежений доступ до системи та не може отримати повний огляд її роботи. У таких випадках атакуючий працює з мінімумом даних, наприклад, лише з вхідними показниками сенсора. Метою роботи був аналіз кіберзагроз сенсорним підсистемам АТЗ та розробка ефективних підходів до захисту.

Література

1. IBM. What is LiDAR? URL: <https://www.ibm.com/topics/lidar> (date of access: 07.12.2024).