4. Slyusar V. Artificial intelligence as the basis of future control networks. Coordination problems of military technical and devensive industrial policy in Ukraine. Weapons and military equipment development perspectives. VII International Scientific and Practical Conference. Abstracts of reports. 2019. Kyiv. C. 76 - 77.

КІБЕРБЕЗПЕКА НА АВТОМОБІЛЬНОМУ ТРАНСПОРТІ

Аббасов С.М., гр. А-51-24
Науковий керівник – Крайнюк О.В. доцент, к. т. н. каф. МБЖДі
Харківський національний автомобільно-дорожній університет

Сучасні автомобілі оснащені великою кількістю технічних рішень, що випередили транспортні засіб минулого століття на декілька десятиліть вперед. Всі нові розробки направлені на покращення систем безпеки та комфорт керування автомобільним транспортом. Їх перелік величезний, вони стосуються багатьох елементів та вузлів сучасних автомобілів.

Завдяки введенню новітніх систем безпеки у вигляді електронних систем керування, впроваджених в транспортні засоби, вони становляться більш інтелектуальними.

Прикладом сучасних транспортних технологій може постати Ізраїль, який до речі не має своїх заводів по виробництву автомобілів. Але вони розуміють всю важливість та перспективу за кібербезпекою на сучасних транспортних засобах загального користування. З більшою кількою складних рішень в нових автомобілях робить більш легким їх взлом та більш важким їх захист. У галузі комп'ютерного програмного забезпечення Ізраїль має великий вплив у світі.

Вважається, що проникнути у внутрішні системи автомобіля можна шляхом підключення через певні пристрої бортової діагностики, wi-fi з’єднання, bluetooth та інші елементи, завдяки яким хакери мають можливість взяти під контроль керування транспортним засобом в будь який момент на невизначений період часу.

Тому через певні загрози безпеки деякі компанії, що займаються у сфері кібебезпекою транспортних засобів мають розробки для захисту користувачів.

Argus Cyber Security одна з таких компаній, що займається в цій сфері та пропонує виробникам безпечне підключення для конфіденційності. Алгоритми Deep Packet Inspection (DPI) для виявлення аномалій, поширення атак та інших видів загроз, це той рівень кібербезпеки, який використовується в даній розробці.

Серед більш простих способів та методів заволодіння чужим автомобілем є також клонування електронного ключа. Найчастіше сучасні транспортні

засоби мають іммобілайзер. Захисна робота даної системи полягає в блокуванні руху до того як отримає певний сигнал від чіпа вбудованого в ключ.

Серед основних видів загроз для автомобільного транспорту:

1. **Віддалений доступ до систем автомобіля**: Хакери можуть отримати контроль над автомобілем через підключені до Інтернету системи, зокрема, через слабкі місця в бортових комп'ютерах або мобільних додатках, що пов'язані з автомобілем.

2. **Вплив на системи керування**: Сучасні автомобілі мають електронні системи контролю над двигуном, гальмами, коробкою передач, а також автономними системами водіння. Кібератаки можуть призвести до некоректної роботи цих систем, що становить серйозну небезпеку для водія і пасажирів.

3. **Крадіжка персональних даних**: Багато сучасних автомобілів зберігають дані користувачів, такі як маршрути пересування, контакти, дані телефонів та інші особисті відомості. Якщо ці дані потрапляють в руки зловмисників, вони можуть бути використані для шахрайства або інших злочинних дій.

4. **Зловживання бездротовими інтерфейсами**: Системи типу Bluetooth, Wi-Fi та NFC можуть використовуватися хакерами для проникнення в систему автомобіля або навіть для зупинки автомобіля на відстані.

Серед сучасних автомобілів є багато таких, які мають бесплітоне керування за рахунок різних систем впроваджених через електроніку. Тому такі авто мають ще більшу вразливість перед кіберзлочинцями, які наприклад можуть втрутитись в гальмівну систему, кермову чи управління двигуном, що має небезпеку для пішоходів та інших учасників дорожнього руху. Слід зазначити, що система управління кібербезпекою (CSMS) відноситься до систематичного, заснованого на оцінці ризиків підходу до встановлення організаційних процесів, обов'язків і керівництва в управлінні ризиками, пов'язаними з кіберзагрозами для транспортних засобів, і захистом транспортних засобів від кібератак». (*Джерело: Офіційний журнал Європейського Союзу за R 155).*

Слід також дотримуватись певних рекомендацій для безпеки , а саме купувати автомобіль потрібно лише у перевірених автодилерів. Проведення ремонту авто також потрібно здійснювати на перевірених СТО. Гореремонтники можуть маніпулювати комп'ютерними системами. Необхідно захищати важливу інформацію.

Якщо в машині встановлена якась система безпеки, то компанія-розробник надає цінну інформацію з управління або розблокування системи та всі необхідні паролі. Ці документи слід зберігати в надійному місці, не можна їх залишати в машині.

До переліку мір безпеки відноситься також покупка автозапчастин, треба бути обережним при їх покупці та різних пристроїв. Електроприлади, що продаються на ринку, рідко проходять ретельну перевірку або випробування. Якщо встановити такий пристрій, підвищиться вразливість автомобіля.

Також краще знайти кваліфікованого спеціаліста, який стежитиме за оновленням ПЗ або пояснить автовласнику, як це робити.

Треба встановлювати або оновлювати програмне забезпечення лише згідно з рекомендаціями автовиробника.

До списку рекомендацій можна віднести наступне, потрібно не допускати сторонніх осіб та невідомі пристрої до діагностичного порту автомобіля (OBD-II). Зазвичай він розташований з боку водія під панеллю приладів. Через цей порт можна отримати доступ до всіх систем автомобіля.

Для підвищення інформаційної безпеки транспортних систем необхідно проводити дослідження, які спрямовані на подальший розвиток методів та моделей розпізнаванні кіберзагроз інформаційно-комунікаційному середовищу транспорту (ІКСТ) та прийняття рішень при нечітко заданій вхідній інформації. Запропонований новий підхід прийняття рішень для забезпечення кібербезпеки інформаційних систем наземного транспорту.

Кібербезпека на автомобільному транспорті – це важлива сфера, що зосереджена на захисті транспортних засобів і транспортних систем від кібератак. Сучасні автомобілі оснащені багатьма електронними компонентами та підключеними системами, такими як GPS-навігація, Інтернет-з'єднання, бездротові системи (наприклад, Bluetooth), а також системи автоматичного керування, що робить їх вразливими до кіберзагроз.

Різні країни та організації створюють стандарти для підвищення рівня кібербезпеки в автомобільній індустрії. Наприклад, **ISO/SAE 21434** – це міжнародний стандарт, що визначає вимоги до кібербезпеки автомобільних систем протягом всього життєвого циклу транспортного засобу.

Висновок

Можна із впевненістю стверджувати, що з розвитком технологій автомобілі стають дедалі більш пов'язаними з мережею, і ризики кіберзагроз зростають. Тому для захисту від них важливо впроваджувати сучасні методи кібербезпеки, що охоплюють всі аспекти роботи транспортного засобу, від програмного забезпечення до апаратних компонентів.

Література

1. https://itrade.gov.il/ukraine/2022/11/09 автомобільна-кібербезпека-іновація

2. https://www.dqsglobal.com/uk-ua/navchajtesya/blog/avtomobil%27na-kiberbezpeka

3. https://media.neliti.com/media/publications/306568-improving-the-transport-cyber-security