УДК 681.518

АВТОМОБІЛЬНА КІБЕРБЕЗПЕКА

Аршинніков Б.В., студ. гр. АА-51-24;
Наук. керівник – **Кравцов М. М.,** доц. каф. МБЖД
Харківський національний автомобільно-дорожній університет

Анотація. В статті розглянуті сучасний стан та перспективи розвитку механізмів складових безпеки: кібербезпеки, інформаційної безпеки, безпеки інформації, та інформаційних технологій. Стаття представляє інтерес як для фахівців, сфера діяльності яких безпосередньо пов'язана з розробкою механізмів складових безпеки та ІТ-технологій, способів забезпечення послуг безпеки та передачі даних в комунікаційних системах, так і для спеціалістів з безпеки інформації. Вона буде корисною викладачам, аспірантам і студентам, що спеціалізуються в області захисту інформації, кібербезпеки та інформаційної безпеки, інформаційних технологій, і всім, хто серйозно цікавиться проблемами взаємодії інформаційних технологій, безпеки та інформаційного суспільства.

Ключові слова: безпека, кібербезпека, інформаційна безпека, складова безпеки

Вступ

У ході всіх тих суттєвих змін, що зазнає автомобільна промисловість в її новітній історії, автомобілі, як відомо, стають дедалі більш інтелектуальними та ефективними. Це зумовлено насамперед впровадженням різноманітних ефектронних систем керування, інтелектуальних компонентів, вбудованих систем та інтерфейсів. Проте разом із очевидно великою користю процесів цифровізації, має місце небезпечний недолік. Кожен додатковий компонент в автомобілі, що керується електронікою, збільшує ризики потенційної кібератаки чи спроб несанкціонованого втручання. Кількість викрадень з допомогою високотехнологічних засобів зростає пропорційно із тим, як автомобілі стають «розумнішими». Задля протидії цій небезпеці створюються удосконалені технології захисту, надійні системи безпеки, розробляються нові правила автомобільної кібербезпеки.

Без перебільшення можна сказати, що віднедавна автомобільна кібербезпека стала справжнім викликом для компаній-виробників автомобільного транспорту. Як відомо, майже кожен комунікаційний інтерфейс, компонент, бортовий комп'ютер чи допоміжна система в автомобілі можуть зазнати хакерської атаки.

Кібербеспека на автомобільному транспорті

Наразі кібербезпека в автомобільній сфері забезпечується апаратними і програмними рішеннями. Проте до повноцінного захисту всіх електронних блоків управління (ЕБУ) – дуже непростий шлях. Кібербезпека в автомобілебудуванні є більш складною у порівнянні, наприклад, зі смартфонами чи

комп’ютерами. Це пов’язано з тим, що десятки ЕБУ в кожному авто з’єднані великою кількістю електронних шин та відповідають за різні функції та характеристики. Крім того, існує багато можливих точок доступу (всередині авто і віддалених), наприклад OBDII, USB і SD-порти, безключовий доступ, Bluetooth, Wi-Fi, датчики, додаток для смартфонів, підключення через хмарні системи, що також мають доступ до транспортного засобу.

Сучасний автомобіль може зазнати кібератаки по-різному. Одними з доступних місць потрапляння в систему автомобіля є функції підключення, а саме бездротові інтерфейси через Bluetooth і WLAN. Також вразливістю відзначаються додатки-супутники для керування важливими функціями. Вразливими автомобілями часто стають такі, що можуть отримувати оновлення «по повітрю», що все більше використовується на сучасних авто. Крім того, помічником для зловмисників може бути штучний інтелект, так як методи на його основі надають злочинцям перевагу у швидкості та ефективності. Протидією в даному випадку може бути запобіжне сканування вразливостей на основі ШІ. З’єднання типу Vehicle-to-everything також потребує значної уваги в майбутньому, оскільки воно передбачає постійний зв’язок між транспортними засобами та об’єктами навколо. Також небезпека може торкатись систем доступу без ключа, адже з’являється ризик викрадення шляхом перехоплення чи підробки сигналів.

Правила запобігання загроз на автомобільному транспорті

З метою запобігання загроз для автомобільної промисловості, у 2020-му році в ООН запровадили такі нові правила:

– UNECE R155, що передбачає вимоги до захисту транспортних засобів від кібератак та опис важливості нової Системи управління кібербезпекою (CSMS);

– UNECE R156, що визначає забезпечення безперервної безпеки протягом усього життєвого циклу транспортного засобу, а також зобов’язує використовувати систему управління оновленнями програмного забезпечення (SUMS).

Дані правила зобов’язують всі автотранспортні організації забезпечувати кібербезпеку своїх продуктів і систем у всьому ланцюжку постачання.

Система управління кібербезпекою (CSMS) є систематичним і заснованим на оцінці ризиків підходом, що передбачає встановлення організаційних процесів, обов’язків і керівництва в управлінні ризиками, що пов’язані з кіберзагрозами, і захистом автотранспортних засобів від кібератак.

Систему CSMS впроваджують з метою систематизації кібербезпеки в організації та узгодження її зі встановленими національними або міжнародними стандартами. Одні з головних аспектів її успішного впровадження це:

– від організації вимагається сучасна система управління ризиками та надійні шляхи розпізнавання, оцінки та пом’якшення ризиків кіберзагроз;

– керування ризиками має включати увесь життєвий цикл транспортного засобу;

– наявність повноцінного моніторингу нових вразливих місць і відомих атак, що забезпечить швидку реакцію на атаки завдяки цілеспрямованим оновленням.

Варто додати, що CSMS пропонує компаніям певні переваги, серед яких є одна з основних: вона передбачає те, що забезпечується можливість виміряти кібербезпеку організації. а саме у рамках незалежної оцінки уповноваженого постачальника послуг аудиту.

Висновки

Таким чином, сучасні автомобілі складно навіть уявити без мережевих електронних систем і програмного забезпечення, а це означає, що захист і безпека цих складових є дуже вагомим питанням у всій галузі автомобілебудування, а забезпечення цього захисту залежить від якісної роботи в цьому напрямку всіх учасників, що беруть участь у виготовленні електроніки автомобіля.

Перелік використаної літератури

1. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та понятях / В. А. Ліпкан, О. С. Ліпкан. – 2-ге вид., доп. і перероб. – К.: Текст, 2008. – 400 с.

2. Ліпкан В. А. Національна безпека України : навчальний посібник / В. А. Ліпкан. – 2-ге вид. – К. : КНТ, 2009. – 576 с.

3. Тімкін І. Ф. Структурно-функціональна характеристика системи забезпечення національної безпеки України [Електронний ресурс] / І. Ф. Тімкін, Н. Є. Новікова. – Режим доступу : er.nau.edu.ua

4. Поняття та зміст системи забезпечення кібербезпеки [Електронний ресурс]. – Режим доступу : http://goal-int.org

5. Діордіца І. В. Поняття та зміст національної системи кібербезпеки [Електронний ресурс] / І. В. Діордіца. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/

6. Мельник С. В. Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ / С. В. Мельник, В. І. Кащук. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

7. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312–320.

8. Шеломенцев В. П. Формування законодавчих основ забезпечення кібербезпеки України / В. П. Шеломенцев // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

9. Бурячок В. Л. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки / В. Л. Бурячок, С. О. Гнатюк, О. Г. Корченко // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

МОДЕЛЮВАННЯ ПОВЕДІНКИ АВТОНОМНОГО ТРАНСПОРТНОГО ЗАСОБУ В СКЛАДНИХ ДОРОЖНІХ УМОВАХ: РОЗРОБКА ТА АНАЛІЗ ІМІТАЦІЙНИХ МОДЕЛЕЙ ДЛЯ СКЛАДНИХ СЦЕНАРІЇВ

Герасимов А.В., А51-24
Наук. керівник – **Кравцов М. М.,** доц. каф. МБЖД
Харківський національний автомобільно-дорожній університет

Анотація. Публікація досліджує потребу в точних імітаційних моделях для безпілотних автомобілів, виклики, з якими вони стикаються в складних дорожніх умовах, і технологічні досягнення, спрямовані на подолання цих викликів. Під час дослідження проведено аналіз реакції АТЗ на несприятливі погодні умови та надзвичайні ситуації за допомогою передового моделювання, за допомогою якого можна отримати уявлення про їхню готовність до реального застосування та кроки, необхідні для забезпечення їхньої безпечної та ефективної роботи.

Ключові слова: автономний транспортний засіб, моделювання поведінки, імітаційні моделі, реалістичні симуляції, надзвичайні ситуації, алгоритми прийняття рішень.

Розвиток автономних транспортних засобів (АТЗ) є революційним досягненням у сучасному транспорті, що обіцяє революціонізувати мобільність, зменшити кількість дорожньо-транспортних пригод та підвищити паливну ефективність. Однак, для того, щоб повністю інтегруватися в повсякденне життя, безпілотні автомобілі повинні бути здатні справлятися з широким спектром дорожніх умов, включаючи складні, непередбачувані ситуації. Такі ситуації можуть виникати через несприятливі погодні умови, такі як сильний дощ, сніг або туман, а також надзвичайні ситуації, такі як раптова поломка транспортного засобу, аварії або дорожнє сміття. Моделювання поведінки автономних транспортних засобів у цих складних сценаріях має вирішальне значення для їх розробки та широкого впровадження.