УДК 004.056.5

РАЗРАБОТКА МОДЕЛИ УГРОЗ КИБЕРБЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ БЛОКОВ УПРАВЛЕНИЯ В АВТОМОБИЛЕ

Тахаутдинова К.И. (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук, Маркина Т.А.
(Университет ИТМО)

Введение. Современные автомобили имеют большое количество компьютеров и мультимедийных систем, интенсивно обмениваются данными с облачными сервисами, а также другими автомобилями и дорожной инфраструктурой. Цифровизация транспорта добавляет к привычным опасностям ещё и риски, связанные с киберугрозами. Сегодня в автомобильной индустрии кибербезопасность должна обеспечивается как аппаратными, так и программными решениями. Организациям необходимо разработать стандарты и регламенты, которые регулировали бы кибербезопасность, что дополнительно поспособствует развертыванию киберзащитных решений во всех подключенных автомобилях. На данный момент только Международная организация по стандартизации ISO выпустила стандарт ISO/SAE 21434:2021 «Road vehicles – Cybersecurity engineering» [1] способствующий кибербезопасности автомобилей. ISO/SAE 21434:2021 является международным стандартом, однако при перспективном развитии российского автопрома необходимо также иметь собственные руководящие документы в области кибербезопасности автомобилей, которые бы описывали возможные угрозы и потенциальных нарушителей. Возникает необходимость в разработке модели угроз.

Основная часть. С помощью правильной модели угроз можно повысить уровень информационной кибербезопасности и сократить затраты на её обеспечение, сосредоточившись на самых вероятных угрозах. Методика построения модели угроз регламентирована следующим методическим документом: «Методика моделирования угроз безопасности информации (проект ФСТЭК России, 2020г.)» [2]. Процесс разработки модели угроз включает в себя:

- процесс определения угроз безопасности информации в информационной системе автомобиля;
- оценку возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя) электронных блоков управления автомобиля;
- определение актуальных угроз безопасности информации в информационной системе автомобиля.

Построение модели нарушителя подразумевает рассмотрение возможных внутренних и внешних нарушителей, категорию нарушителе, а также согласно банку данных угроз ФСТЭК [3] рассматривается возможный потенциал нарушителя.

При определении актуальных угроз для электронных блоков управления автомобилем из банка данных угроз ФСТЭК исключаются неактуальные угрозы. К актуальным угрозам присваивается вероятность реализации угрозы.

На основе выявленного списка актуальных угроз разрабатываются рекомендации по их устранению.

Выводы. Проведен анализ необходимости разработки руководящих документов в области кибербезопасности автомобилей и разработана модель угроз кибербезопасности электронных блоков управления в автомобилях, а также разработаны рекомендации по устранению угроз.

Список использованных источников:

1. ISO/SAE 21434: 2021 «Road vehicles – Cybersecurity engineering: [Электронный ресурс]. – август 2021 – URL: https://www.iso.org/standard/70918.html
2. Методический документ. «Методика моделирования угроз безопасности информации». Проект Федеральной службы по техническому и экспортному контролю России - 2020г. – 54с. – Текст : электронный [Электронный источник] – URL: https://fstec.ru/component/attachments/download/2727
3. Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России : [сайт]. – URL: https://bdu.fstec.ru.