УДК 004.056

РАЗРАБОТКА КОМПЛЕКСА МЕР ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМУ БЕЗОПАСНОСТИ ТРАНСПОРТНОГО СРЕДСТВА

Рашидов М.-И.М.-Б. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Попов И.Ю. (ИТМО)
Научный консультант – инженер ФБИТ Савков С.В. (ИТМО)

Введение. Разработка комплекса мер защиты от несанкционированного доступа в систему безопасности транспортного средства представляет собой процесс создания и внедрения системы, направленной на обеспечение информационной, физической и функциональной безопасности. В связи с активным развитием технологии VANET (Vehicular ad hoc network) [1] возникает риск прослушивания и перехвата конфиденциальной информации, такой как местоположение транспортного средства и его прошлые, настоящие и вероятные будущие маршруты, состояние автомобиля и информация о его владельце. Также существует возможность атак, ориентированных на нарушение целостности данных, к которым можно отнести атаки типа DoS (отказ в обслуживании), что может негативно сказаться на безопасности дорожного движения. Изучение данной сферы наиболее актуально в связи с ежегодным увеличением количества автомобилей, подключенных к сети, которые можно использовать для связи с другими транспортными средствами (V2V) или инфраструктурой (V2I) для самых различных целей, таких как: приложения безопасности, которые помогают уменьшить количество несчастных случаев и незамедлительно сообщают информацию о возникшем дорожно-транспортном происшествии в службы спасения без участия человека, приложения помощи водителю, которые облегчают сложность в управлении транспортным средством, рекламные приложения, которые сообщают водителю о близлежащих магазинах и развлекательных заведениях. Конечной целью данной работы является создание комплекса мер, включающего в себя как существующие методы обеспечения защиты в системе безопасности транспортного средства, так и предложенные в ходе написания исследования.

Основная часть. В рамках исследования рассмотрены наиболее популярные точки уязвимости автомобиля, подключенного к сети. Эти уязвимости могут быть реализованы как с помощью атак типа Black/Grey/Worm-hole, которые распространены в одноранговых сетях, к которым относится VANET, так и атаки Сивиллы, когда транспортное средство будет подключено к сети, которое контролируется злоумышленником. Однако система VANET не является единственным источником реализации угроз в системе автомобиля. Для обеспечения безопасности также следует учитывать атаки на шины типа CAN (Controller Area Network) [2], физическую безопасность водителя и пассажиров. На основе вышеперечисленных уязвимостей разработан набор универсальных решений и правил для минимизации риска безопасности разных типов автомобиля для водителя и для производителей транспортных средств. В работе представлена классификация угроз по разным уровням, включая распределение их по степени тяжести последствий для водителя, пассажиров и окружающей инфраструктуры, а также риски возникновения этих угроз. Рассмотрены новейшие технологии, применяемые в безопасности автомобиля, такие как биометрическая аутентификация водителя, система мониторинга мертвых зон и система оповещения водителя о его физическом состоянии, и влияние этих технологий на обеспечение конфиденциальности, целостности и доступности цифровой инфраструктуры транспортного средства. На основе собранной информации проанализированы наиболее вероятные угрозы и предложены меры для их предотвращения.

Выводы. На основе анализа выделены и рассмотрены наиболее вероятные уязвимости, несущие ущерб водителю, пассажирам и окружающей инфраструктуре, а также разработан комплекс мер защиты в системе безопасности транспортного средства, включающий в себя

обеспечение конфиденциальности, целостности и доступности информации и физической безопасности водителя.

Список использованных источников:

1. Lee M., Atkison T. VANET applications: Past, present, and future // Vehicular Communications. – 2020. – p. 44.
2. Avatefipoure O., Saad Al-Sumaiti A., El-Sherbeeny A., Awwad E., El-Meligy M., Mohammed M., Malik H. An Intelligent Secured Framework for Cyberattack Detection in Electric Vehicles' CAN Bus Using Machine Learning // IEEE Access . – 2019. – p. 13.