Клец Дмитрий Михайлович, д.т.н., доц., Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», d.m.klets@gmail.com
Маковецкий Андрей Владимирович, к.т.н., Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», makoveckiyandrey@gmail.com

ИДЕНТИФИКАЦИЯ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОТРАНСПОРТНЫХ СРЕДСТВ

Характеристики бортовой электроники и каналов связи большинства современных автомобилей не соответствуют минимальным требованиям к их информационной безопасности (ИБ). Уязвимости автоматизированных систем автотранспортных средств снижают их ИБ, а следовательно – эффективность эксплуатации и безопасность дорожного движения. Создание эффективной системы менеджмента ИБ предполагает идентификацию организационных потребностей относительно требований ИБ автомобиля с помощью системного подхода. Приведем перечень рисков в различных областях безопасности автомобиля, с учётом активов, которые подвержены этим уязвимостям:

– Силовой агрегат: самопроизвольные запуск и выключение двигателя; внесение изменений в работу электронного блока управления; внесение изменений в режимы работы коленчатого вала; отключение цилиндров двигателя; внесение изменений в работу стартера; увеличение числа оборотов холостого хода; искажение показаний спидометра.

– Шасси и элементы систем безопасности: активация отдельных контуров тормозной системы; предотвращение торможения; считывание угла поворота рулевого колеса; изменение алгоритмов работы антиблокировочной системы; изменение алгоритмов работы подушек безопасности; блокирование передачи данных о местоположении; блокирование передачи сигнала о краже автомобиля; изменение маршрута движения; искажение показаний датчиков бортовой диагностики выброса вредных веществ.

– Электронные системы кузова: блокирование/разблокирование дверей; отключение Shift-Lock соленоида; отключение сигнализации; активация сигнала и изменение его частоты; активация стеклоомывателя; отключение приборов наружного освещения; вмешательство в работу приборов освещения салона.

– Системы обеспечения комфорта: перехват местоположения автомобиля; подмена POI в навигационной системе; кража данных информационно-развлекательной системы; нарушение работы стеклоочистителей; увеличение громкости аудиосистемы; изменение дисплея аудиосистемы; вмешательство в работу адаптивного круиз-контроля; блокировка обновления фирменного программного обеспечения; хищение данных персональной идентификации.

Полученные результаты могут быть использованы на этапах производства и эксплуатации автотранспортных средств с целью повышения как информационной безопасности, так и безопасности дорожного движения в целом.