Zhurn. «INFUSED BYTES».**8.** *Vinokurov, A. Y.* (2005). Yeshche raz pro GOST. Moscow: Monitor, 45.**9.** *Barichev, S.* (2008). Kriptografiya bez sekretov. Moscow: Moskva.**10.** *Varfolomeyev, A. A., Domnina, O. S., Pelenitsyn, M. B.* (2006). Upravleniye klyuchami v sistemakh kriptograficheskoy zashchity bankovskoy informatsii. Moscow.**11.** *Berezin, B. V., Doroshkevich, P. V.* (2002). Tsifrovaya podpis' na osnove traditsionnoy kriptografii. Moscow: MP "Irbis II".**12.** Zashchita informatsii ot nesanktsionirovannogo dostupa soglasno trebovaniyam FSTEK Rossii. Available at: http://www.pcweek.ru/security/article/detail.php?ID=169230 – zagl. z yekranu.**13.** Kod Bezopasnosti. Produkty. Available at: http://www.security code.ru/products/ – zagl. z yekranu.**14.** Kratko o vybore sertifitsirovannykh SZI ot NSD. Available at: http://www.altx-soft.ru/articles/show-1.htm – zagl. z yekranu.**15.** Avtomatizatsiya neftegazovykh predpriyatiy na baze SUBD LINTER. Available at: www / URL: https://linter.ru/ru/press-center/detail/27/1578/ – zagl. z yekranu.**16.** GIS 6 Secure Geodezicheskaya informatsionnaya sistema. Available at: http://www.shels.ru/download/gis6 secure_rus.pdf – zagl. z yekranu.**17.** Blochní shifri. Available at: http://citforum.ru/internet/infsecure/its2000_16.shtml – zagl. z yekranu.**18.** *Barichev, S. G., Goncharov, V. V., Serov, R. Ye.* (2002). Standart AES. Algoritm Rijdael. Moscow: Telekom, 30–35.

Поступила (received) 22.12.2015

Відомості про авторів / Сведения об авторах / About the Authors

Руженцев Віктор Ігоревич – кандидат технических наук, доцент, кафедра Безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, пр. Ленина, 14, г.. Харьков, Украина, 61166; тел.: 057-702-14-25; e-mail: diagnost@kture.kharkov.ua.

Руженцев Віктор Ігоревич – кандидат технічних наук, доцент, кафедра Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, пр. Леніна, 14, м. Харків, Україна, 61166; тел.: 057-702-14-25; e-mail: diagnost@kture.kharkov.ua.

Ruzhentsev Victor – PhD, Associate Professor, Department of Information Technology Security, Kharkov National University of Radioelectronics, Lenina Ave., 14, Kharkiv, Ukraine, 61166; tel.: 057-702-14-25; e-mail: diagnost@kture.kharkov.ua.

Порван Андрей Павлович – кандидат технических наук, старший научный сотрудник, кафедра биомедицинской инженерии, харьковский национальный университет радиоэлектроники, пр. Ленина, 14, г. Харьков, Украина, 61166; тел.: 066-294-06-70; e-mail: porvan_a_p@mail.ua.

Порван Андрій Павлович – кандидат технічних наук, старший науковий співробітник, кафедра біомедичної інженерії, Харківський національний університет радіоелектроніки, пр. Леніна, 14, м. Харків, Україна, 61166; тел.: 066-294-06-70; e-mail: porvan_a_p@mail.ua.

Porvan Andrei – PhD, Senior Research, Department of Biomedical Engineering, Kharkov National University of Radioelectronics, Lenina Ave., 14, Kharkiv, Ukraine, 61166; tel.: 066-294-06-70; e-mail: porvan_a_p@mail.ua.

Пащенко Мария Анатольевна – студентка, факультет Электронной техники, Харьковский национальный университет радиоэлектроники, пр. Ленина, 14, г. Харьков, Украина, 61166; тел.: 066-933-13-54; e-mail: maria-paschenko@mail.ru.

Пащенко Марія Анатоліївна – студентка, факультет Електронної техніки, Харківський національний університет радіоелектроніки, пр. Леніна, 14, м Харків, Україна, 61166; тел.: 066-933-13-54; e-mail: maria-paschenko@mail.ru.

Pashchenko Maria – student, Faculty of Electronic Engineering, Kharkiv National University of Radioelectronics, Lenina ave., 14, Kharkov, Ukraine, 61166; tel .: 066-933-13-54; e-mail: maria-paschenko@mail.ru.

УДК 629.33:004.056

А. В. МАКОВЕЦКИЙ

АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО АВТОМОБИЛЯ

Современные автомобили представляют собой сложные технические системы, оснащенные электронными устройствами для улучшения эксплуатационно-технических свойств. Устойчивая тенденция увеличения количества электронных устройств в современных автомобилях с проводным и беспроводным подключением неизбежно приводит к росту уязвимостей, а значит – снижению безопасности и эффективности эксплуатации. Проведенный анализ позволил выявить ряд угроз информационной безопасности автоматизированных систем современных автомобилей, которые приводят к необходимости разработки методов механической и электронной защиты транспортных средств.

Ключевые слова: информация, уязвимость, защита, угроза, безопасность, эксплуатация, автомобиль.

Введение. Современные автомобили представляют собой сложные технические системы, оснащенные электронными устройствами для улучшения эксплуатационно-технических свойств. В 1990 г. электронные устройства и программное обеспечение составляли около 16 % стоимости автомобиля, в 2001 г. – 25 %, а в 2005 г. – до 40 % [1]. По оценкам специалистов Центра автомобильных исследований штата Мичиган, по состоянию на 2014 г. электроника и программное обеспечение составляют уже до 40-50 % [2] стоимости современного автомобиля. Также по данным Инженерной Ассоциации IEEE известно, что программное обеспечение представляет 90 % [3] инноваций в автомобилях.

Устойчивая тенденция увеличения количества электронных устройств в современных автомобилях с проводным и беспроводным подключением неизбежно приводит к росту уязвимостей, а значит – снижению безопасности и эффективности эксплуатации.

Анализ литературных данных и постановка проблемы. На сегодняшний день новый автомобиль содержит от 50 до 100 и более электронных блоков управления [4]. В работе [5] указывается, что к 2025 г.

©А. В. Маковецкий. 2015

100 % автомобилей будут подключены к информационным системам, а в работе [6] – что к 2035 г. 75% автомобилей будут автономными.

Авторами ряда работ [4, 7] установлено, что злоумышленники могут получить удаленный доступ к электронным системам транспортных средств, управлять их компонентами или похищать личные данные автовладельцев. Помимо злоумышленников, атаки на автомобильные сети также могут проводиться в целях корпоративного шпионажа [8]. Современная аппаратура позволяет создавать различные степени повреждений – от радиочастотных помех вплоть до физического повреждения сетевых компонентов автомобиля.

Исследование состояния информационной безопасности показывает, что среди 173 исследованных автомобильных компаний по всему миру, число происшествий, выявленных в 2015 г. увеличилось на 32 % по сравнению с 2014 г. [7]. 98% всех протестированных программных приложений в автомобилях имеют серьезные дефекты, некоторые – от 10 до 15 [4]. В указанном исследовании приводятся и первые инциденты – взлом системы управления транспортом, приведший к аварии и пробкам на дорогах; кража автомобиля; блокирование GPS-отслеживания и угон инкассаторского автомобиля; взлом и перехват управления автомобилем Toyota Prius; произвольное ускорение автомобиля; подмена маршрута транспортных средств и т.д.

Вследствие атаки в 2014 г. злоумышленников на «Стрелки» [9], установленные на дорогах Подмосковья, ущерб для областного бюджета составил около 2 млн. рублей. Причиной сбоя, как выяснили в правительстве Подмосковья, стал компьютерный вирус, который вывел из строя 130 камер из 144 на семь дней.

В 2015 г. эксперты журнала Wired [10] провели показательный дистанционный взлом компьютерной системы Uconnect нового автомобиля Jeep Cherokee. Действуя с помощью ноутбука из другого города, программисты Ч. Миллер и К. Валасек сумели получить доступ к важным функциям автомобиля, включая самопроизвольный разгон, торможение, работу стеклоочистителей и т.д. В результате 1,4 млн. автомобилей с системой Uconnect соответствующей модификации были отправлены на сервис, а Национальное ведомство по вопросам дорожной безопасности NHTSA оштрафовало производителя на 105 млн. долларов [10] по целому ряду оснований: несвоевременный отзыв транспортных средств, недостаточный контроль безопасности, сокрытие информации от владельцев и властей и т.д.

По последним данным полиции Лондона [11], более трети всех угонов в столице Великобритании происходит с помощью перепрограммирования ключа зажигания, после чего преступникам требуется максимум 10 с на кражу. Угонщики используют вредоносные компьютерные программы, в том числе для получения контроля над спутниками. Это дает им возможность послать с орбиты сигнал – разблокировать двери, отключить сигнализацию и запустить двигатель нужного автомобиля. Данная проблема касается не только премиальных моделей, все современные автомобили подвержены рискам высокотехнологичных угонов [11].

Таким образом, анализ информационной безопасности современного автомобиля и поиск методов защиты информационных систем являются актуальными научными задачами и требуют изучения со стороны ученых и инженеров.

Цель и задачи работы. Целью исследования является повышение информационной безопасности автомобиля путем анализа возможных угроз и перспективных методов защиты информационных систем. Для достижения данной цели необходимо решить следующие задачи:

– выполнить анализ возможных угроз информационной безопасности автоматизированных систем современных автомобилей;

– исследовать перспективные методы защиты информационных систем современных автомобилей.

Анализ возможных угроз информационной безопасности автоматизированных систем современных автомобилей. Согласно исследованию [12] потенциальным угрозам автомобили могут подвергаться через: проводной интерфейс – OBD-II, USB, диагностические, зарядные, сетевые разъемы, CD/DVD-плеер и бортовые сети автомобиля (CAN, FlexRay, Ethernet, MOST и т.д.); беспроводные сети малой дальности – радиочастотные (контроль давления в шинах, брелок и т.д.), Wi-Fi, Near Field, Bluetooth, выделенные сети; беспроводные сети большой дальности – GPS, GSM/CDMA.

Потенциальным методом доступа [12] может являться использование: внешних сетей – сетевой Call-центр, сетевой сервис центр, домашняя сеть, сеть сотовой связи); модифицированных компонентов; портативных устройств – персональный компьютер, брелок, трансивер, съемный медиа диск (CD, DVD и т.д.), смартфон, музыкальный проигрыватель (портативное музыкальное устройство), самодельное электронное устройство.

Указанное выше вмешательство в работу автомобиля в целом может привести к следующим последствиям [12]: необычное поведение автомобиля в нормальных условиях эксплуатации; нарушение обмена данных в сетях автомобиля; создание препятствий в управлении автомобилем в экстремальных условиях эксплуатации и при контраварийном вождении; отображение водителю ложной информации; отвлечение внимания водителя; кража идентификационных данных (пароли, данные адресных книг, ключи, права доступа и т.д.).

Матрица угроз информационной безопасности автомобиля [12] позволяет систематизировать данные о вероятности перехвата управлением автомобилей в результате вмешательства злоумышленников, в частности:

– силовым агрегатом (трансмиссией, двигателем, гибридными приводными системами, а также показаниями их датчиков);

– шасси и элементами систем безопасности (тормозной системой, рулевым управлением, экологическими датчиками, датчиками подушек безопасности, датчиками давления воздуха в шинах, датчиками шасси);

– электронными системами кузова (дверные модули, удаленные замки, управление светом, управление сидениями);

– системами обеспечения комфорта (вентиляции воздуха, климат-контроля, дистанционного запуска); информационно-развлекательными системами и т.д.).

Национальный институт стандартов и технологий США в документе NIST 800-30 [13] определяет уязвимость как «недостаток или слабость в процедурах безопасности, проектирования, реализации или внутреннего контроля системы, которые могут быть осуществлены (случайно или намеренно) и привести к нарушению безопасности или нарушению политики безопасности системы».

Эксперты [14] выделяют четыре класса уязвимостей в системе защиты автомобиля.

– прямой физический доступ;

– непрямой физический доступ (USB, PassThru, CD).

– беспроводной доступ на близкой дистанции (Bluetooth, Android-приложения, перехват MAC-адреса автомобильного сетевого устройства, брутфорс PIN);

– беспроводной доступ на дальней дистанции.

Автор исследования [10] приводит более 10 способов взлома автомобилей, которые относятся к одному из вышеперечисленных классов атак и проверены на практике.

Под кибербезопасностью авторы работы [14] предлагают понимать процесс жизненного цикла, который включает в себя следующие элементы: оценивание, проектирование, внедрение, эффективное тестирование и программу сертификации.

В результате исследования [12] разработана классификация тяжести последствий при недостаточной информационной безопасности автомобиля:

– высокая: серьезные травмы вплоть до летального исхода; потеря контроля над автомобилем;

– средняя: вероятность травм; опытный водитель может сохранить контроль над транспортным средством;

– низкая: отсутствие травм и потеря контроля над транспортным средством; мотив нападения – кража, создание неприятностей, самореклама.

Автор работы [10] утверждает, что автомобиль Tesla Model S потенциально уязвим к хакерским атакам. Проблема кроется в безопасности аутентификации интерфейса прикладного программирования API Tesla через удаленный доступ. При взломе сетевой базы данных злоумышленники получают свободный доступ ко всем автомобилям, зарегистрированным на сайте на срок до трех месяцев, а именно: возможность активировать механизм люка, определить местоположение автомобиля, подать звуковой сигнал, открыть багажник и выполнить ряд других операций. Данная уязвимость не приведет к возникновению дорожно-транспортного происшествия, однако может быть использована для слежки за автовладельцем.

В работе [15] приведены цифровые порты ввода/вывода модели типичного автомобиля 2012-го года выпуска, которые могут иметь уязвимости с точки зрения информационной безопасности (рис. 1).

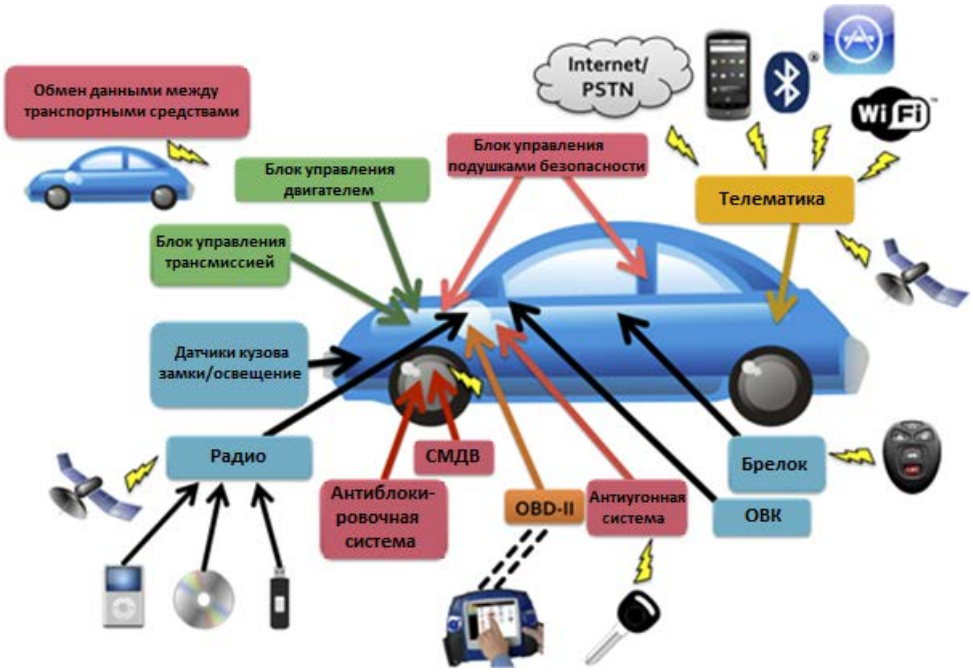

Рис. 1 – Цифровые каналы ввода-вывода данных современного автомобиля: ОВК – обогрев, вентиляция, кондиционирование воздуха; СМДВ – система мониторинга давления воздуха в шинах

Согласно данным немецкой огранизации ADAC [16], более 2 млн. автомобилей BMW с системой коммуникации ConnectedDrive не защищены от взлома с помощью смартфона, который можно осуществить в течение минуты. Проблема связана с использованием одного и того же кода доступа для различных автомобилей и незащищенного протокола.

В работе [17] систематизированы результаты проверки устойчивости автомобилей к кибератакам. В качестве объектов исследования выбраны 20 популярных моделей автомобилей 2006 – 2015 гг. выпуска.

С помощью метода экспертного оценивания присвоим баллы «лучше всех» – 5, «неплохо» – 4, «плохо» – 3, «хуже некуда» – 2 по результатам проверки

устойчивости автомобилей к кибератакам. В качестве параметров устойчивости используем: наличие слабозащищенных каналов связи; оценка электроники; опасность внешней блокировки жизненно важных систем. Результаты выполненного экспертного оценивания приведем на рис. 2.

Анализ рис. 2 показывает, что с точки зрения информационной безопасности по среднему баллу можно выделить три группы автомобилей: первая группа имеет средний балл экспертной оценки выше 4-х; вторая группа 3…4; ниже 3-х. К первой группе с высшей безопасностью относятся 20 % исследуемых автомобилей, ко второй и третьей – по 40 % исследуемых транспортных средств.

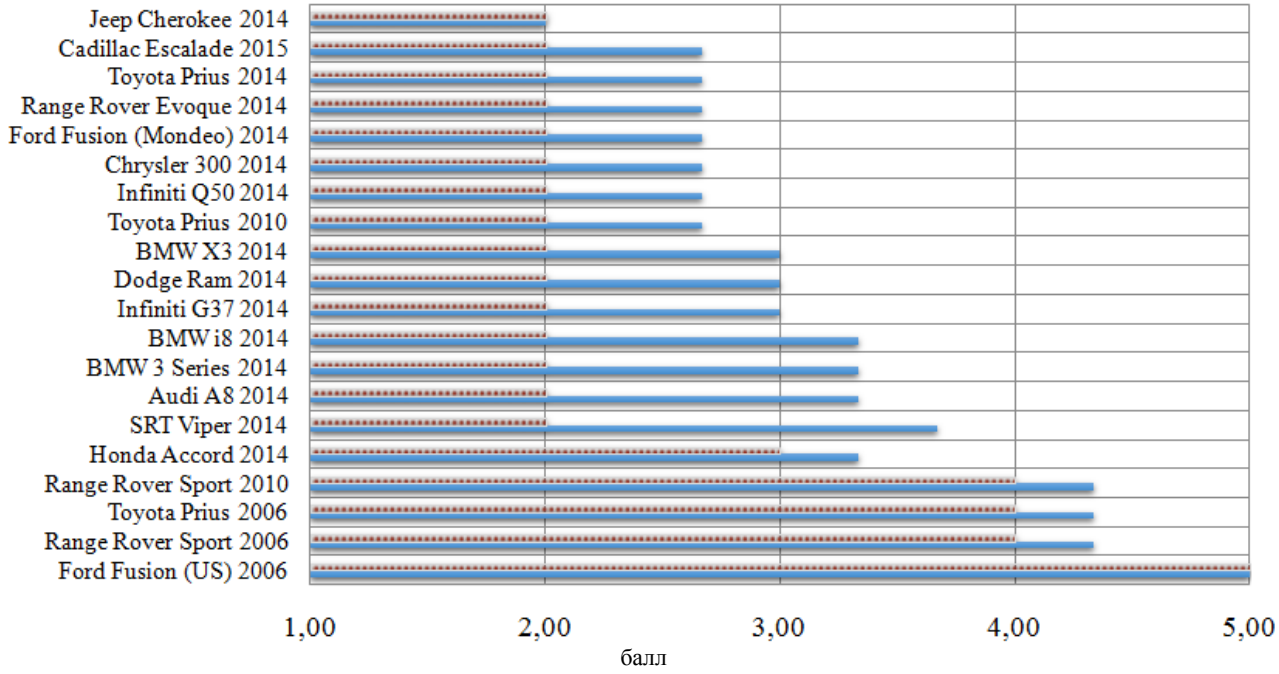

Рис. 2 – Результаты проверки устойчивости автомобилей к кибератакам: ─ средний балл; ••••• минимальный балл

По минимальному баллу к первой группе с высшей безопасностью относятся 20 % исследуемых автомобилей, ко второй группе – 5 %, а к третьей группе с низшей безопасностью – 75 % исследуемых транспортных средств.

Очевидно, что максимальную оценку информационной безопасности имеют автомобили более старых годов выпуска, вследствие меньшего количества бортовых электронных систем и возможных уязвимостей.

Средние баллы экспертного оценивания информационной безопасности автомобилей описываются законом нормального распределения (рис. 3).

Закон нормального распределения, приведенный на рис. 3, может быть описан с помощью следующей зависимости

$$D = f(\mu, \sigma | M) = \frac{1}{0{,}756 \cdot \sqrt{2\pi}} \cdot e^{\frac{-(M-3{,}234)^2}{2 \cdot 0{,}756^2}},$$

где D – плотность распределения; μ – математическое ожидание; σ – среднеквадратическое отклонение; M – экспертная оценка (балл).

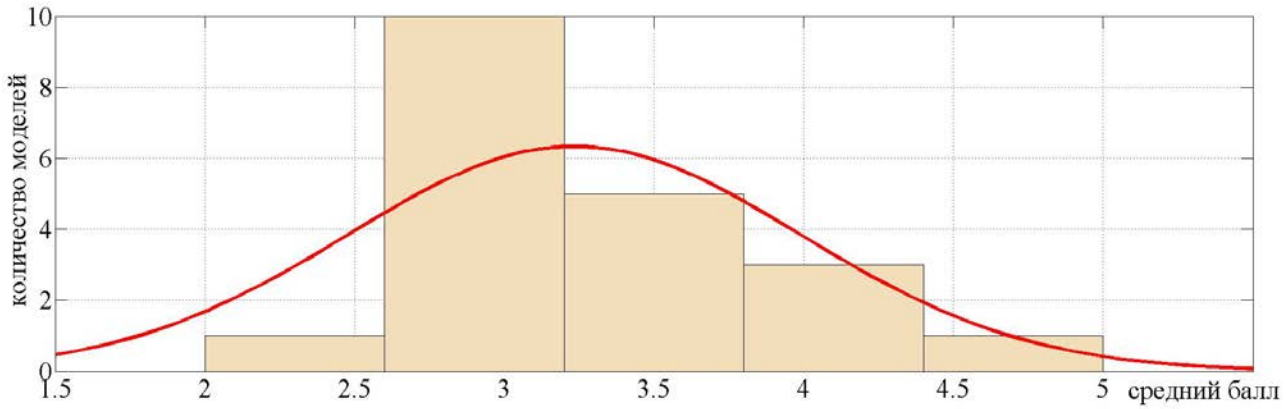

Рис. 3 – Закон нормального распределения оценок информационной безопасности автомобилей

Стандартная ошибка среднего (Std. Err.) для математического ожидания составляет 0,169, а для среднеквадратического отклонения 0,124.

Проведенный анализ позволил выявить ряд угроз информационной безопасности автоматизированных систем современных автомобилей. Выявленные уязвимости информационных систем современных автомобилей приводят к необходимости разработки более совершенных методов механической и электронной защиты транспортных средств.

Перспективные методы защиты информационных систем современных автомобилей. За последние несколько лет хакеры представили недорогие инструменты для несанкционированного доступа к транспортным средствам. Так, набор для взлома электронных систем автомобиля BMW предлагается за 30 дол. США, а устройство, размером с iPhone, способное полностью вывести автомобиль из строя доступно за 20 дол. США [17]. Угрозы взлома электронных систем автотранспортных средств и доступность соответствующих инструментов привела к появлению электронных и механических устройств для защиты от злоумышленников.

Инжиниринговый центр НИЯУ МИФИ [17] разработал и запатентовал устройство для защиты автомобилей от хакерских атак «Автовизор». Устройство устанавливается аналогично сигнализации, сканирует всю электронику транспортного средства на предмет вирусов, посторонних команд и обнаруживает любое стороннее оборудование, которое может провоцировать сбои в управлении. Все изменения отображаются в приложении на мобильном устройстве владельца и блокируются автоматически. Стоимость установки защитного устройства начинается от 400 дол. США и выше в зависимости от набора функций.

Эксперты Ч. Миллер и К. Валасек, о которых было сказано ранее, представили собственный прототип устройства, способного обеспечить информационную безопасность автомобиля [10]. Себестоимость указанного устройства не превышает 150 дол. США. Оно состоит из микроконтроллера NXP и панели управления, подключается к порту OBD-II любого современного автомобиля. После включения в течение минуты обычного вождения, устройство фиксирует характерные данные автомобиля. Переключение его в режим обнаружения позволит детектировать аномалии, отличающиеся от типичного «поведения» транспортного средства.

Ключевые вопросы информационной безопасности призван решить проект Европейского Союза E-Safety Vehicle Intrusion Protected Applications (EVITA) [18]. Целью проекта EVITA является проектирование, проверка и создание прототипа архитектуры бортовых автомобильных сетей, компоненты которых защищены от взлома при передаче данных внутри транспортного средства.

Архитектура Secure Vehicle Communication (SEVECOM) предполагает защиту внутренних коммуникаций, хранение ключей шифрования и сертификатов, защищенное исполнение элементов электронных систем транспортных средств [19].

К концу 2016 г. ожидается начало работы нового международного органа, объединяющего автопроизводителей – Центра передачи и анализа информации (ISAC). Указанная организация создается совместно с Альянсом автопроизводителей и Ассоциацией глобальных автопроизводителей (двумя крупнейшими отраслевыми объединениями в мире). Ее целью являются сбор данных о кибератаках на автомобили и разработка способов противодействия им. Поскольку работа ISAC связана с серьезными вопросами безопасности и бизнеса, ее деятельность будет в значительной мере засекречена. Предполагается, что автомобильные компании будут на анонимной основе предоставлять экспертам ISAC информацию об обнаруженных в их автомобилях уязвимостях, а, те в свою очередь, должны оценить степень угрозы и помочь в выработке общих решений, стандартизации мер безопасности и т. д.

В Конгресс США внесен законопроект «Акт о безопасности и приватности автомобиля», который призван защитить автовладельцев от опасностей со стороны хакеров. Документ предусматривает многоступенчатую систему защиты от постороннего подключения к современным автомобилям. Государственные органы США, в т.ч. Национальная администрация безопасности дорожного движения (NHTSA) занимаются разработкой федеральных стандартов защиты от киберпреступников, обязательные для выполнения всеми автопроизводителями, а также созданием систему специальных тестов и рейтингов кибербезопасности. Это связано с тем, что согласно данным NHTSA в США на сегодняшний день представлены лишь два автопроизводителя, в автомобилях которых установлена защита от киберпреступности.

Проведенный анализ показывает недостаточную реализацию защитных систем современных автомобилей. Для решения указанных проблем необходим синтез устройств и конкретных практических рекомендаций для повышения безопасности и эффективности эксплуатации автотранспортных средств.

Выводы. Проведенный анализ позволил выявить ряд угроз информационной безопасности автоматизированных систем современных автомобилей, что снижает эффективность эксплуатации и безопасность дорожного движения. Проводной или беспроводной доступ к информационным сетям современного автомобиля позволяет получить контроль над его силовым агрегатом, шасси, элементами систем безопасности и систем обеспечения комфорта.

По критериям оценки бортовой электроники, наличия слабозащищенных каналов связи, опасности внешней блокировки жизненно важных систем 75 % исследуемых современных автомобилей не соответствуют минимальным требованиям к информационной безопасности. Выявленные уязвимости информационных систем современных автомобилей приводят к необходимости разработки методов механической и электронной защиты транспортных средств.

Определен закон нормального распределения средних баллов экспертного оценивания информационной безопасности автомобилей. Математическое ожидание составляет 3,234, среднеквадратическое отклонение – 0,756. Стандартная ошибка среднего для

математического ожидания составляет 0,169, а для среднеквадратического отклонения 0,124.

Список литературы: 1. *Electronics: Driving Automotive Innovation* [Text]: Auto Electronics, Facts and Forecasts, 2005. – 15 p. **2.** Hill, K. Just How High-Tech is the Automotive Industry [Text] / K. Hill // Center for Automotive Research, 2014. – 73 p. **3.** *Frischkorn, H.* Automotive software – the silent revolution [Text] / *H. Frischkorn* // Automotive SW Workshop, 2004. – 302 p. **4.** *Лукацкий, А.* Информационная безопасность современного автомобиля [Электронный ресурс] / *А. Лукацкий* // Cisco Systems. – 2015. – Режим доступа: http://www.slideshare.net/lukatsky/connected-car-security. **5.** *Kearney, A.* The Mobile Economy [Text] / *A. Kearney* // GSMA, 2013. – 101 c. **6.** Smart City Suppliers [Text]: Navigant Research Leaderboard Report, 2014. – 52 p. **7.** *Захарченко, А. Д.* Угрозы информационной безопасности автоматизированных систем современных автомобилей [Текст] / *А. Д. Захарченко, А. К. Шилов* // Экономика и социум. – 2015. – No 3 (16). – С. 157–160. **8.** Risk Management Framework Applied to Modern Vehicles [Text]: National Institute of Standards And Technology Cyber Security, 2014. – 27 p. **9.** *Редькина, Е.* В Подмосковье подсчитали ущерб от неработающих камер видеофиксации [Электронный ресурс] / *Е. Редькина* // За рулём. – 2014. – Режим доступа: http://www.zr.ru/content/news/607363-v-podmoskove-podschitali-ushherb-ot-nerabotayushhix-kamer-vieofiksacii/.
10. *Данилина, В.* Fiat-Chrysler знал о возможности взлома еще полтора года назад [Электронный ресурс] / *В. Данилина* // За рулём. – 2015. – Режим доступа: http://www.zr.ru/content/news/803779-fiat-chrysler-znal-o-vozmozhnosti-vzloma-eshhe-poltora-goda-nazad/.
11. *Родионов, П.* В Лондоне треть угонов авто приходится на хакеров [Электронный ресурс] / *П. Родионов* // За рулём. – 2014. – Режим доступа: http://www.zr.ru/content/news/703636-tret-ugonov-avtomobilej-v-londone-prixoditsya-na-xakerov/. **12.** Characterization of Potential Security Threats in Modern Automobiles [Text]: NHTSA, 2014. – 46 p. **13.** Risk Management Guide for Information Technology Systems Practices [Text]: NIST, 2002. – 56 p. **14.** A Summary of Cybersecurity Best Practices [Text]: NHTSA, 2014. – 40 p. **15.** *Checkoway, S.* Comprehensive Experimental Analyses of Automotive Attack Surfaces [Text] / *S. Checkoway* // IEEE Symposium on Security and Privacy. – 2010. – 16 p. **16.** Hacker konnten BMW-Türen jahrelang per Handy öffnen [Электронный ресурс] / ADAC. – 2015. – Режим доступа: http://www.zeit.de/mobilitaet/2015-01/bmw-hacker-sicherheit.
17. *Колодочкин, М.* Взлом без лома: легко ли вскрыть машину со смартфона [Электронный ресурс] / *М. Колодочкин* // За рулём. – 2015. – Режим доступа: http://www.zr.ru/content/articles/783458-vzlom-bez-loma-legko-li-vskryt-mashinu-so-smartfona/. **18.** E-Safety Vehicle Intrusion Protected Applications [Text]: EVITA, 2011. – 2 p. **19.** *Leinmuller, T.* Secure Vehicle Communication [Text] / *T. Leinmuller* // SEVECOM, 2015. – 5 p.

Bibliography (transliterated): 1. *Electronics: Driving Automotive Innovation* (2005). Auto Electronics, Facts and Forecasts, 15. **2.** *Kill, H.* (2014). Just How High-Tech is the Automotive Industry. Center for Automotive Research, 73. **3.** *Frischkorn, H.* (2004). Automotive software – the silent revolution. Automotive SW Workshop, 302. **4.** *Lukatskiy, A.* (2015). Information security of a modern car. Cisco Systems. Available at: http://www.slideshare.net/lukatsky/connected-car-security. **5.** *Kearney, A.* (2013). The Mobile Economy. GSMA, 101. **6.** *Smart City Suppliers* (2014). Navigant Research Leaderboard Report, 52. **7.** *Zaharchenko, A.* (2015). Threats of the information security of modern cars automated systems. Economy and Society, 3, 157–160. **8.** *Risk Management Framework Applied to Modern Vehicles* (2014). National Institute of Standards And Technology Cybersecurity, 27. **9.** *Redkina, H.* (2014). It has estimated the damage from the working video-fixing cameras in Moscow. At the wheel. Available at: http://www.zr.ru/content/news/607363-v-podmoskove-podschitali-ushherb-ot-nerabotayushhix-kamer-vieofiksacii/. **10.** *Danilina, V.* (2015). Fiat-Chrysler knew about the possibility of hacking a half years ago. At the wheel. Available at: http://www.zr.ru/content/news/803779-fiat-chrysler-znal-o-vozmozhnosti-vzloma-eshhe-poltora-goda-nazad/.
11. *Rodionov, P.* (2014). In London, a third of car hijackings accounted for hackers. At the wheel. Available at: http://www.zr.ru/content/news/703636-tret-ugonov-avtomobilej-v-londone-prixoditsya-na-xakerov/. **12.** *Characterization of Potential Security Threats in Modern Automobiles* (2014). NHTSA, 46. **13.** *Risk Management Guide for Information Technology Systems* (2002). NIST, 56. **14.** *A Summary of Cybersecurity Best Practices* (2014). NHTSA, 40. **15.** *Checkoway, S.* (2010). Comprehensive Experimental Analyses of Automotive Attack Surfaces. IEEE Symposium on Security and Privacy, 16. **16.** *Hacker konnten BMW-Türen jahrelang per Handy öffnen* (2015). ADAC. Available at: http://www.zeit.de/mobilitaet/2015-01/bmw-hacker-sicherheit. **17.** *Kolodochkin, M.* (2015). Hacking without scrap: how easy is it to open the car with your smartphone. At the wheel. Available at: http://www.zr.ru/content/articles/783458-vzlom-bez-loma-legko-li-vskryt-mashinu-so-smartfona/. 1**8.** E-Safety Vehicle Intrusion Protected Applications (2011). EVITA, 2. **19.** *Leinmuller, T.* (2015). Secure Vehicle Communication. SEVECOM, 5.

Поступила (received) 06.06.2015

Відомості про авторів / Сведения об авторах / About the Authors

Маковецкий Андрей Владимирович – кандидат технических наук, доцент, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ»; Кафедра автомобилей и транспортной инфраструктуры, ул. Чкалова, 17, г. Харьков, Украина, 61070;

Маковецький Андрій Володимирович – кандидат технічних наук, доцент, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»; Кафедра автомобілів та транспортної інфраструктури, вул. Чкалова, 17, м. Харків, Україна, 61070, тел.: 050-624-09-33; e-mail: makoveckii.andre@mail.ru.

Makovetskyi Andrii – Ph.D., associate professor, National Aerospace University named after N. Zhukovsky «KhAI»; Automobiles and Transport Infrastructure Department, Chkalova st., 17, Kharkov, Ukraine, 61070

УДК 504.03 / 628.3.03

В. В. МИХАЙЛЕНКО

ПІДВИЩЕННЯ ЕКОЛОГІЧНОЇ БЕЗПЕКИ ВОДНИХ ОБ'ЄКТІВ В ЗОНІ ВПЛИВУ ЗВАЛИЩ ТВЕРДИХ ПОБУТОВИХ ВІДХОДІВ

Робота присвячена дослідженню технологічних заходів щодо підвищення рівня екологічної безпеки водних в зоні негативного впливу звалища твердих побутових відходів м. Маріуполя. Розроблені комплексні заходи щодо перешкоджання потрапляння забрудненого фільтрату в підземні води та ріку Кальміус. Визначено оптимальні умови процесу анаеробного зброджування за яких ефективність очищення максимальна. Доведено ефективність застосування методу осадження для видалення заліза з фільтрату звалища ТПВ та шаруватих подвійних гідроксидів для сорбції фенолів. Визначено оптимальний склад нейтралізуючої суміші.

Ключові слова: екологічна безпека, звалище твердих побутових відходів, фільтрат, анаеробне зброджування, шаруваті подвійні гідроксиди.

© В. В. Михайленко. 2015