УДК 629.33:004.056

Д. М. Клец,
А. В. Маковецкий

Менеджмент риска информационной безопасности автотранспортных средств

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

На основе системного подхода выполнено ранжирование основных угроз информационной безопасности автотранспортных средств. С использованием комплекса критериев безопасности автомобилей определена вероятность и возможные последствия рисков при перехвате управления автомобилем или предоставления недостоверной информации в результате вмешательства злоумышленников. Результаты исследования процесса менеджмента риска информационной безопасности могут быть использованы как при производстве, так и при эксплуатации автотранспортных средств с целью повышения безопасности дорожного движения и сохранности информации.

***Ключевые слова**:* информация, уязвимость, защита, угроза, безопасность, менеджмент, риск, автомобиль.

Введение

Характеристики бортовой электроники и каналов связи большинства современных автомобилей не соответствуют минимальным требованиям к их информационной безопасности (ИБ) [1]. Уязвимости автоматизированных систем автотранспортных средств снижают их ИБ, а следовательно – эффективность эксплуатации и безопасность дорожного движения. Указанные проблемы приводят к актуальности менеджмента риска ИБ, а также к необходимости разработки методов механической и электронной защиты систем транспортных средств.

Менеджмент риска ИБ состоит из следующих этапов – установления контекста, оценки риска, обработки риска, принятия риска, коммуникаций риска, а также мониторинга и переоценки риска [2]. Данные этапы должны быть реализованы как в процессе производства, так и при эксплуатации автотранспортных средств.

Анализ литературных данных и постановка проблемы

Дорожно-транспортные происшествия (ДТП) каждый год уносят до 1,3 млн. людей, а убытки достигают миллиардов долларов [3]. Существующие методы повышения эффективности эксплуатации автотранспортных средств базируются на исследовании отдельных характеристик системы «водитель-автомобиль-дорожная среда» (ВАДС), без учета их синергетики [4]. Однако высокоэффективное использование автомобилей требует системного исследования их свойств, которые существенным образом влияют на безопасность дорожного движения.

Различают активную, послеаварийную, информационную, экологическую и пассивную безопасность автомобилей (рис. 1). Европейская программа The European New Car Assessment Programme (Euro NCAP) [5] предлагает общую оценку безопасности новых автомобилей на основе оценки четырёх важнейших составляющих (рис. 2). Указанные составляющие определяются с помощью комплекса критериев, приведенных далее.

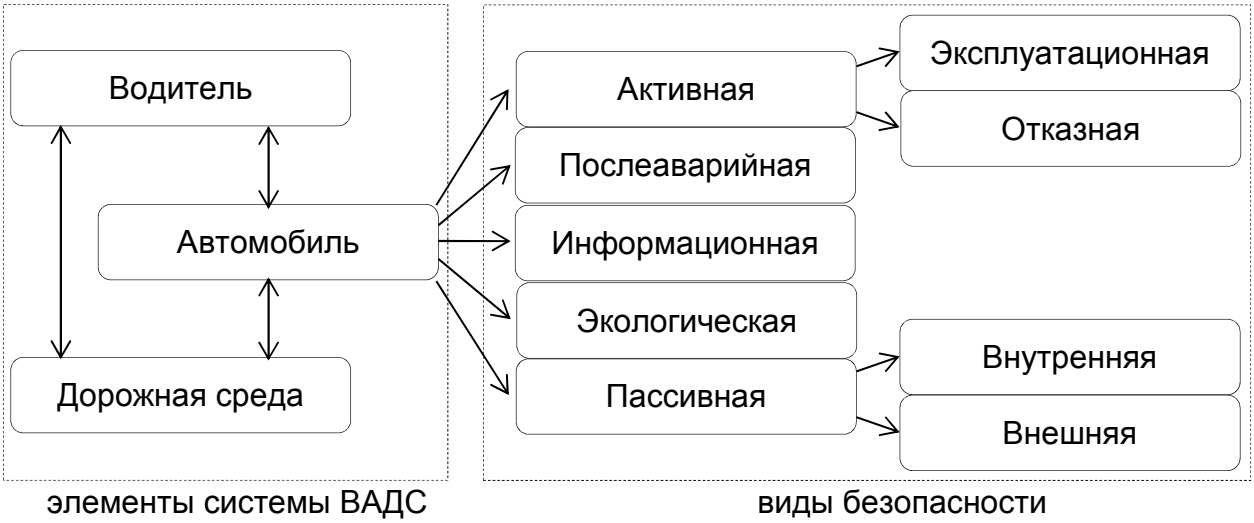

Рис. 1. Виды безопасности автотранспортных средств

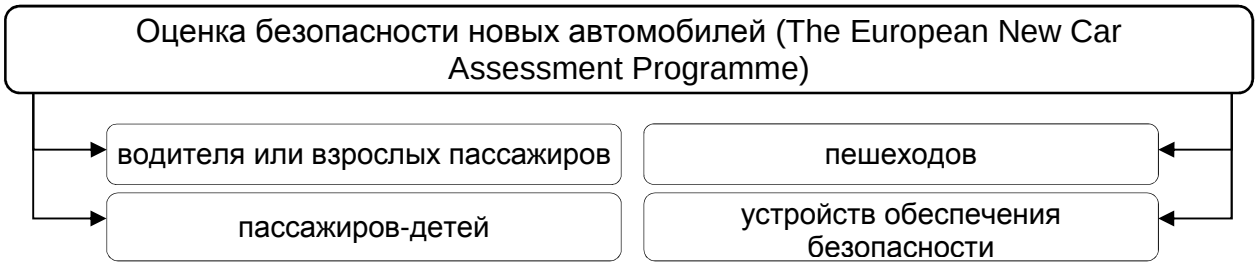

Рис. 2. Составляющие оценки безопасности новых автомобилей согласно программе Euro NCAP

При формировании критериев оценки безопасности водителя или взрослых пассажиров согласно программе Euro NCAP рассматриваются [5]:

- уровень безопасности при столкновении со смещением с деформируемым препятствием;
- уровень безопасности при столкновениях без смещения;
- уровень безопасности при боковых столкновениях;
- уровень безопасности при столкновении со столбом;
- уровень защиты от хлыстовых травм;
- эффективность системы автономного экстренного торможения в городских условиях.

Для оценки безопасности пассажиров-детей определяются [5]:

- эффективность детских удерживающих устройств;
- оснащенность автомобиля;
- параметры детской удерживающей системы.

Для оценки безопасности пешеходов рассматриваются [5]:

- уровень безопасности при ударах головой;
- уровень безопасности при ударах по верхней части ног;
- уровень безопасности при ударах по нижней части ног;
- эффективность системы автономного экстренного торможения для защиты пешеходов.

Для проверки эффективности работы оцениваются такие устройства обеспечения безопасности, как [5]:

- электронная система курсовой устойчивости;
- сигнализаторы непристегнутых ремней безопасности;
- система обеспечения рекомендованного скоростного режима;
- система автономного экстренного торможения в междугородных поездках;
- система удержания автомобиля на полосе движения.

При оценке безопасности также выполняется анализ участков обзора, закрытых от водителя; мониторинг работы системы предупреждения о превышении скоростного режима, системы помощи в восстановлении концентрации водителя, системы автоматического экстренного вызова, системы улучшения обзора и т.п.

Согласно требованиям международного стандарта ISO/IEC 27005:2011 [2], менеджмент риска ИБ должен быть непрерывным процессом. Данный процесс должен способствовать:

– идентификации рисков ИБ автотранспортных средств;

– оценке рисков, исходя из последствий их реализации для безопасности дорожного движения и вероятности их возникновения;

– установлению приоритетов в рамках обработки рисков ИБ;

– проведению регулярного мониторинга и пересмотра процесса менеджмента риска;

– сбору информации для совершенствования менеджмента риска;

– подготовке водителей и персонала технического обслуживания по вопросам рисков ИБ и необходимых действий, предпринимаемых для их уменьшения.

Проведенный автором работы [1] анализ позволил выявить ряд угроз информационной безопасности автоматизированных систем современных автомобилей, которые снижают эффективность эксплуатации и безопасность дорожного движения. Определено, что 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 [1]. Выявленные уязвимости информационных систем современных автомобилей приводят к необходимости разработки методов механической и электронной защиты транспортных средств. Таким образом, вопрос снижения риска информационной безопасности автотранспортных средств требует дополнительных исследований.

Цель и задачи работы

Целью исследования является повышение эффективности эксплуатации автотранспортных средств путем менеджмента риска их информационной безопасности. Для достижения данной цели необходимо решить следующие задачи:

– идентифицировать риски информационной безопасности;

– выполнить ранжирование угроз посредством мер риска;

– оценить ценности для степени вероятности и возможных последствий рисков.

Идентификация риска информационной безопасности

Применим процесс менеджмента риска ИБ к современному автомобилю. Обзор указанного процесса изложен в нормативном документе ISO/IEC 27005:2011 [2], а схема – на рис. 3.

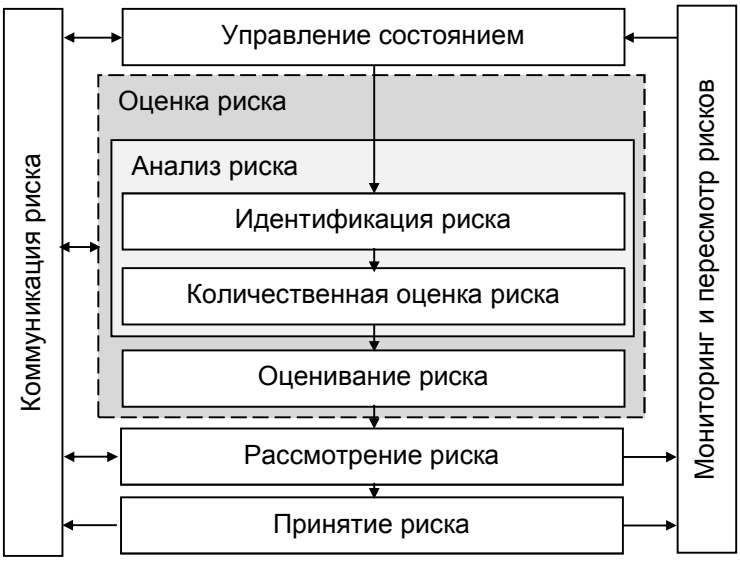

Рис. 3. Процесс управления риском ИБ

Создание эффективной системы менеджмента ИБ предполагает идентификацию организационных потребностей относительно требований ИБ автомобиля с помощью системного подхода. Идентификация риска ИБ включает в себя определение активов, определение угроз и источников угроз, определение существующих мер и средств контроля и управления, а также выявление уязвимостей ИБ и последствий.

Под риском ИБ будем понимать потенциальную угрозу эксплуатации уязвимости с причинением вреда элементам системы ВАДС. Согласно рекомендациям [2], одновременная реализация всех мер и средств контроля и управления не всегда возможна, поэтому с помощью процесса обработки риска рассмотрим только наиболее критичные риски.

Под «активами» будем понимать элементы автомобиля, которые оказывают существенное влияние на безопасность дорожного движения, сохранность персональной информации и, поэтому, нуждающиеся в защите. Для каждого актива рассмотрим соответствующие уязвимости и их соответствующие угрозы.

В работе [1] систематизированы 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.).

В связи с вышесказанным примем, что система «автомобиль» имеет четыре актива: A_1 – силовой агрегат; A_2 – шасси и элементы систем безопасности; A_3 – электронные системы кузова; A_4 – системы обеспечения комфорта;

Угрозы ИБ автомобиля могут иметь естественную или антропогенную природу, а также могут быть случайными и преднамеренными. Угроза может возникнуть от любого элемента системы ВАДС. Эксперты [6] 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.

Поэтому предположим, что существуют четыре угрозы, применимые к системе: $У_1$ – прямой физический доступ; $У_2$ – непрямой физический доступ; $У_3$ – беспроводной доступ на близкой дистанции; $У_4$ – беспроводной доступ на дальней дистанции.

В табл. 1 приведен перечень рисков в различных областях безопасности автомобиля, с учётом активов, которые подвержены этим уязвимостям. Перечень рисков используется в процесса оценки угрозы ИБ.

Таблица 1

Перечень рисков в различных областях безопасности автомобиля

Наименования активов	Основные риски, соответствующие активу
Силовой агрегат (Актив A_1): трансмиссия; двигатель; гибридные приводные системы; показания их датчиков	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 (Актив A_2): тормозная система; рулевое управление; экологические датчики; датчики подушек безопасности; датчики давления воздуха в шинах; датчики шасси	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 (Актив A_3): дверные модули;	блокирование/разблокирование дверей; отключение Shift-Lock соленоида; отключение сигнализации; активация сигнала и изменение его частоты;

Наименования активов	Основные риски, соответствующие активу
удаленные замки; управление приборами освещения; управление сидениями	активация стеклоомывателя; отключение наружных приборов освещения; вмешательство в работу приборов освещения салона.
Системы обеспечения комфорта (Актив A_4): вентиляция воздуха; климат-контроль; дистанционный запуск; информационно-развлекательные системы	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.

Ранжирование угроз посредством мер риска

Детальный процесс оценки риска ИБ включает тщательное определение и установление ценности активов, оценку угроз этим активам и оценку уязвимостей [2]. Определение последствий (ценности активов) выполним с учетом критериев их влияния. Степень вероятности возникновения угрозы определим, принимая во внимание частоту возникновения угроз и простоту использования уязвимостей. Шкалу для ценности активов и степени вероятности возникновения угрозы выберем от «1» до «4», причём «1» соответствует наименьшим последствиям и самой низкой степени вероятности возникновения.

Установим значения (меру) рисков M_i, учитывая значения вероятности возникновения угрозы и последствий, с помощью следующей зависимости

$$M_i = S_i \times P_i,$$

где i – идентификатор угрозы;

S – последствия (ценность актива);

P – степень вероятности возникновения угрозы.

Угрозы ИБ ранжируем в порядке соответствующей меры риска и сводим в табл. 2.

Таблица 2

Ранжирование угроз ИБ посредством мер риска

Идентификатор угрозы	S	P	M	Ранг угрозы
Угроза активу A_1 (силовой агрегат)	3	2	6	3
Угроза активу A_2 (шасси и элементы систем безопасности)	4	1	4	2
Угроза активу A_3 (электронные системы кузова)	2	4	8	4
Угроза активу A_4 (системы обеспечения комфорта)	1	3	3	1

Результаты ранжирования угроз используются для оценки рисков, а затем для определения способа обработки риска.

Оценка ценности для степени вероятности и возможных последствий рисков

Организация NHTSA предлагает следующую классификацию тяжести последствий при недостаточной ИБ автомобиля [7]:

– 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 потери контроля над транспортным средством; мотив нападения – кража, создание неприятностей, самореклама.

Согласно приведенной классификации введем степень тяжести последствий: *Z* - высокая; *Y* - средняя; *X* – низкая. Определим вероятность осуществления сценария инцидентов с ИБ и сведём полученные результаты в табл. 3.

Таблица 3

Вероятность осуществления сценария инцидентов

Тяжесть последствий	*X* (отсутствие травм)			*Y* (вероятность травм)			*Z* (серьезные травмы)		
Уровни уязвимости	*H*	*C*	*B*	*H*	*C*	*B*	*H*	*C*	*B*
Значение степени вероятности	0	1	2	1	2	3	2	3	4

Уровни уязвимости для каждого актива определим с помощью табл. 2, используя следующий масштаб риска: *H* – низкий (*P* = 1…2); *C* – средний (*P* = 3); *B* – высокий (*P* = 4). Тяжесть последствий для каждой угрозы определяем с помощью метода экспертного оценивания.

Далее с помощью табл. 3 определим значения степени вероятности, например – если для актива A_1 и угрозы $У_1$ уровень уязвимости *H*, а тяжесть последствий *Z*, то значение степени вероятности равно 2 и т.д. Баллы для соответствующего актива и угрозы определим с помощью табл. 4.

Таблица 4

Ценности актива и значения степени вероятности

Значение степени вероятности	Ценность актива				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Результаты сведены в табл. 5.

Таблица 5

Значения степени вероятности возникновения угроз

Актив	Угроза	Уровень уязвимости	Тяжесть последствий	Значение степени вероятности	Балл
A_1	$У_1$	H	Z	2	5
	$У_2$		Z	2	5
	$У_3$		Z	2	5
	$У_4$		Y	1	4
A_2	$У_1$	H	Y	1	5
	$У_2$		Y	1	5
	$У_3$		X	0	4
	$У_4$		X	0	4
A_3	$У_1$	B	Z	4	6
	$У_2$		Y	3	5
	$У_3$		Y	3	5
	$У_4$		X	2	4
A_4	$У_1$	C	X	1	2
	$У_2$		X	1	2
	$У_3$		X	1	2
	$У_4$		X	1	2

Итоговые баллы для каждого актива определяем путём суммирования баллов всех его угроз. Полученные результаты приведены на рис. 4 и позволяют выполнить ранжирование угроз ИБ.

Рис. 4. Результаты ранжирования угроз ИБ автотранспортных средств

Анализ рис. 4 показывает, что электронные системы кузова современного автомобиля имеют наибольшую вероятность повреждения злоумышленниками (20 баллов), что может привести к хищению транспортного средства.

Силовой агрегат автомобиля (19 баллов) также уязвим с точки зрения ИБ, что позволяет выполнять самопроизвольный запуск и выключение двигателя или вносить изменения в работу электронного блока управления (ЭБУ). Последнее может привести к отказу в обслуживании транспортного средства.

Шасси и элементы систем безопасности (18 баллов) значительно влияют на безопасность движения, поэтому нарушение их функционирования приводит к высокой вероятности травм, и лишь опытный водитель может при этом сохранить контроль над транспортным средством.

Наименьшую вероятность повреждения имеют системы обеспечения комфорта (8 баллов). Однако вмешательство в их работу всё же может принести ощутимый вред водителю и пассажирам (перехват местоположения автомобиля, кража данных, переутомление водителя и т.д.).

Выводы

1. На основе системного подхода выполнено ранжирование основных угроз информационной безопасности автотранспортных средств. Электронные системы кузова современного автомобиля имеют наибольшую вероятность повреждения злоумышленниками, что может привести к хищению транспортного средства.
2. С использованием комплекса критериев безопасности автомобилей определена вероятность и возможные последствия рисков при перехвате управления автомобилем.
3. 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.

Список литературы

1. Маковецкий А. В. Анализ информационной безопасности современного автомобиля [Текст] / А. В. Маковецкий // Вісник Національного технічного університету «ХПІ»: зб. наук. праць. Серія: Механіко-технологічні системи та комплекси. – Х.: НТУ «ХПІ». – 2015 р. – № 52 (1161). – С. 137-142.
2. Information technology. Security techniques. Information security risk management (ISO/IEC 27005:2011). – [Published on 2011-06-01]. – International Organization for Standardization, 2011. – 68 p.
3. Глобальные технические правила ООН № 8 «Электронные системы контроля устойчивости» – [26 июня 2008 г.] – (ECE TRANS 180 GE.08–24699) – Офиц. изд. – Женева : ООН, 2008. – 116 с.
4. Клец Д. М. Концепція забезпечення стабільності показників стійкості та керованості автомобілів : автореф. дис. на здобуття наук. ступеня докт. техн. наук : спец. 05.22.20 «Експлуатація та ремонт засобів транспорту» / Д. М. Клец. – Х., 2015. – 40 с.
5. The European New Car Assessment Programme [Electronic resource] / Brussel. – 2015. – Access mode: http://www.euroncap.com.
6. A Summary of Cybersecurity Best Practices [Текст] / NHTSA, 2014. – 40 с.
7. Characterization of Potential Security Threats in Modern Automobiles [Текст] / NHTSA, 2014. – 46 с.

Поступила в редакцию 16.05.2016

Менеджмент ризику інформаційної безпеки автотранспортних засобів

На основі системного підходу виконано ранжування основних загроз інформаційній безпеці автотранспортних засобів. З використанням комплексу критеріїв безпеки автомобілів визначена ймовірність і можливі наслідки ризиків при перехопленні управління автомобілем в результаті втручання зловмисників. Результати дослідження процесу ризик-менеджменту інформаційної безпеки можуть бути використані як при виробництві, так і при експлуатації автотранспортних засобів з метою підвищення безпеки дорожнього руху та збереження інформації.

***Ключові слова**:* інформація, вразливість, захист, загроза, безпека, менеджмент, ризик, автомобіль.

Motor vehicles information security risk management

On the basis of a systematic approach it’s performed rankings of main threats to the vehicle information security. With using of the automobile security complex criteria it’s determined the likelihood and possible consequences of the risks during interception of driving as a result of malicious interference. Results of the process of information security risk management study can be used both in production and in the operation of motor vehicles in order to improve road safety and the information safety.

***Key words**:* information, vulnerability, protection, threat, security, management, risk, automobile.

Сведения об авторах:

Клец Дмитрий Михайлович – докт. техн. наук, доцент, кафедра автомобилей и транспортной инфраструктуры, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина.

Маковецкий Андрей Владимирович – канд. техн. наук, кафедра автомобилей и транспортной инфраструктуры, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина.