Александр М. Коротин
АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ОТВЕТСТВЕННОЙ ИНФОРМАЦИИ,
ПЕРЕДАВАЕМОЙ СИСТЕМОЙ АЛС НА БАЗЕ РАДИОКАНАЛА

Александр М. Коротин
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, г. Москва, 115409, Россия, e-mail:
e-mail: alexkor91@gmail.com, ORCID iD 0000-0003-3773-342X

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ОТВЕТСТВЕННОЙ ИНФОРМАЦИИ,
ПЕРЕДАВАЕМОЙ СИСТЕМОЙ АЛС НА БАЗЕ РАДИОКАНАЛА

DOI: <http://dx.doi.org/10.26583/bit.2017.2.05>

Аннотация. Переход к использованию радиоканала для передачи ответственной информации в системах автоматической локомотивной сигнализации (АЛС) усложняет обеспечение безопасности перевозочного процесса, так как в этом случае создаются условия для получения несанкционированного доступа к каналу связи из-за пределов контролируемой зоны. В связи с этим представляется целесообразным решение задачи по определению угроз безопасности ответственной информации, передаваемой системой автоматической локомотивной сигнализации на базе радиоканала (АЛСР), реализация которых способна нарушить безопасность перевозочного процесса. Решение поставленной задачи возможно путем анализа угроз безопасности ответственной информации, определения степени их влияния на перевозочный процесс, разработки модели нарушителя. В статье показано, что нарушение безопасности перевозочного процесса возможно в случае нарушения целостности ответственной информации. Используя методические документы ФСТЭК России, разработана модель нарушителя безопасности ответственной информации. Сделан вывод, что угрозы со стороны внутреннего нарушителя для традиционных систем автоматической локомотивной сигнализации и систем АЛСР совпадают. Сформирован перечень угроз безопасности ответственной информации, направленных на нарушение безопасности перевозочного процесса со стороны внешнего нарушителя. Полученные в статье результаты могут использоваться при исследовании безопасности систем АЛСР, анализе существующих решений по защите ответственной информации, передаваемой АЛСР, или разработке новых способов защиты.

Ключевые слова: автоматическая локомотивная сигнализация на базе радиоканала, АЛСР, безопасность АЛСР, модель угроз и нарушителя АЛСР, безопасность ответственной информации, обеспечение целостности ответственной информации.

Для цитирования. КОРОТИН, Александр М. Анализ угроз безопасности ответственной информации, передаваемой системой АЛС на базе радиоканала. Безопасность информационных технологий, [S.l.], v. 24, n. 2, p. 42-49, June 2017. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/104>>. Дата доступа: 23 June 2017. doi:<http://dx.doi.org/10.26583/bit.2017.2.05>.

Alexander M. Korotin
National Research Nuclear University MEPhI,
Kashirskoe shosse, 31, Moscow, 115409, Russia,
e-mail: alexkor91@gmail.com, ORCID iD 0000-0003-3773-342X

Security threat analysis of critical information transmitted by the ALS system based on the radio channel

DOI: <http://dx.doi.org/10.26583/bit.2017.2.05>

Abstract. The transition to the use of a radio channel for the transfer of critical information in automatic locomotive signaling (ALS) systems complicates the security of the transportation process, because in this case conditions are created for obtaining unauthorized access to the communication channel from outside the controlled area. That's why it seems advisable to solve the problem of identifying security threats of critical information transmitted by the automatic locomotive signaling system based on the radio channel (ALSR), the implementation of which is

likely to disrupt the safety of the transportation process. The solution of this task is possible by analyzing security threats of critical information, determining the degree of their influence on the transportation process and developing violator model. The article shows that a security breach of the transportation process is possible in case of violation of the responsible information integrity. A model of violator of critical information security was developed using methodical documents of FSTEC of Russia. It was concluded that the threats from the internal violator for traditional automatic locomotive signaling systems and ALSR systems coincide. A list of security threats of sensitive information was developed, directed to violating the security of the transportation process by an external violator. The results obtained in the article can be used to study the safety of ALSR systems, to analyze existing solutions for protecting critical information transmitted by ALSR, or to develop new methods of protection.

Keywords: automatic locomotive signaling based on radio channel, ALSR, security of ALSR, threats model and violator model of ALSR, security of critical information, ensuring of critical information integrity.

For citation. KOROTIN, Alexander M. Security Threat Analysis of Critical Information Transmitted by the ALS System Based on the Radio Channel. IT Security (Russia), [S.l.], v. 24, n. 2, p. 42-49, june 2017. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/104>>. Date accessed: 23 june 2017. doi:<http://dx.doi.org/10.26583/bit.2017.2.05>.

Введение

Система автоматической локомотивной сигнализации (АЛС) представляет собой автоматизированную систему управления, применяемую на железнодорожном транспорте для обеспечения безопасности перевозочного процесса. Под безопасностью перевозочного процесса понимается такое его состояние, при котором отсутствует недопустимый риск возникновения транспортных происшествий и их последствий, причиняющих вред жизни или здоровью граждан, окружающей среде, имуществу физических или юридических лиц [1]. Одной из задач, решаемой системой АЛС в рамках обеспечения безопасности перевозочного процесса, является обмен ответственной информацией между станционными системами определения занятости пути и бортовыми устройствами безопасности [2-4]. Под ответственной информацией в статье понимается информация о допустимой скорости движения и дополнительных условиях следования железнодорожного подвижного состава (ограничения скорости, маршрут движения по железнодорожной станции), необходимая для обеспечения безопасности перевозочного процесса.

В состав системы АЛС входит станционное оборудование, расположенное на станциях или вдоль железнодорожных путей (станционная часть АЛС), и бортовое, расположенное на борту локомотива (бортовая часть АЛС) (см. рисунок 1). При этом в АЛС выделяют два логических уровня – уровень управления перевозочным процессом (прикладной уровень) и уровень передачи данных (канальный уровень). На прикладном уровне работают локомотивное устройство безопасности и шлюз взаимодействия с системой определения свободности пути [2]. Между ними происходит обмен ответственной информацией, которая используется для управления и обеспечения безопасности перевозочного процесса. На канальном уровне функционирует система связи, состоящая из напольного и бортового приемопередающего оборудования, отвечающая за доставку ответственной информации.

Рис. 1. Структурная схема системы АЛС
Fig. 1. Block diagram of the system ALS

Использование систем радиосвязи для передачи ответственной информации между станционной и бортовой частями АЛС обладает рядом преимуществ по сравнению с другими системами связи, например, позволяет увеличить объем передаваемых данных, уменьшить вероятность их искажения [5]. Однако, такой переход к использованию радиоканала усложняет обеспечение безопасности перевозочного процесса, так как в этом случае канал связи между станционной и бортовой частями АЛС выходит за пределы контролируемой зоны.

В связи с этим актуальной задачей является определение угроз безопасности перевозочного процесса, реализация которых возможна из-за пределов контролируемой зоны путем нарушения функции обмена ответственной информацией в системах АЛС на базе радиоканала (АЛСР). Для решения данной задачи представляется целесообразным провести анализ существующих угроз безопасности ответственной информации, передаваемой системой АЛСР. Под угрозой безопасности ответственной информации, передаваемой системой АЛСР, понимается совокупность условий и факторов, создающих потенциальную и реально существующую опасность нарушения конфиденциальности, целостности и/или доступности ответственной информации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для перевозочного процесса.

Анализ влияния аспектов безопасности на перевозочный процесс

Согласно работам [6-11] по исследованию кибербезопасности железнодорожного транспорта выделяют три основных класса угроз безопасности микропроцессорных систем железнодорожной автоматики и телемеханики по степени ущерба:

- нарушение безопасности перевозочного процесса (1-ый класс);
- снижение эффективности перевозочного процесса (2-ой класс);
- угрозы, не влияющие на перевозочный процесс, однако приводящие к операционным и/или финансовым потерям (3-ий класс).

Используя данную классификацию, был выполнен анализ угроз, связанных с нарушением разных аспектов безопасности ответственной информации, передаваемой по

радиоканалу. Выявлено, что угрозы, связанные с нарушением целостности ответственной информации, способны привести к получению участниками движения неверных данных, что, в свою очередь, может стать причиной создания ложных свободных блок-участков на пути следования локомотива или изменения разрешенной скорости движения на участке. Возникновение подобных событий нарушает безопасность перевозочного процесса, следовательно, угрозы, связанные с нарушением целостности ответственной информации, относятся к первому классу угроз по уровню ущерба.

Угрозы, связанные с нарушением доступности передаваемой информации или используемого канала связи, относятся ко второму классу угроз. Создание помех в канале связи или подавление радиостанций приведет к невозможности получения ответственной информации, таким образом, подвижной состав продолжит движение по полученным ранее данным до тех пор, пока локомотивное устройство безопасности не остановит его согласно кривой торможения, заранее высчитанной локомотивным устройством безопасности. Таким образом, безопасность перевозочного процесса не будет нарушена, однако его эффективность будет снижена.

Угрозы нарушения конфиденциальности передаваемой ответственной информации могут быть отнесены к третьему классу, так как перехват и раскрытие передаваемых данных в системе АЛСР не влияют напрямую на перевозочный процесс и скорее могут быть использованы для анализа протокола передачи, определения загруженности блок-участка или частоты движения поездов в рамках подготовки проведения компьютерных атак на железнодорожную инфраструктуру.

Таким образом, был сделан вывод, что нарушение безопасности перевозочного процесса возможно только в случае реализации угроз, связанных с нарушением целостности ответственной информации.

Модель нарушителя

При анализе возможных источников угроз технические отказы аппаратуры, а также случайные (непреднамеренные) ошибки людей (персонала) не рассматривались, так как задача защиты перевозочного процесса от подобных угроз относится к области функциональной безопасности и должна выполняться самой системой АЛСР [2]. В связи с этим в качестве источников угроз в работе рассматривались только антропогенные источники – внешний нарушитель, не имеющий доступ к оборудованию системы АЛСР, и внутренний нарушитель.

При этом в качестве внутреннего нарушителя в соответствии с нормативными документами ФСТЭК России [12] рассматривались лица первой категории, имеющие доступ к оборудованию АЛСР, но не являющиеся пользователями системы (обслуживающий персонал, например, электромеханик СЦБ или ремонтная бригада [13]), второй категории, являющиеся пользователями системы (локомотивная бригада [14]), седьмой категории, являющиеся разработчиками ПО прикладного уровня и обеспечивающие его техническое сопровождение, а также восьмой категории – занимающиеся поставкой, сопровождением и ремонтом технических средств, применяемых в АЛСР. Лица 3-6 категорий в работе не рассматривались, так как процесс функционирования системы АЛСР является автономным (отсутствует управляющее воздействие со стороны персонала), и сама система не имеет привилегированных или удаленных пользователей. Кроме того, в ходе анализа было сделано предположение, что нарушители могут вступать в сговор с целью обмена имеющейся у них информацией о системе, а также консолидации возможностей по нарушению безопасности ответственной информации.

На основе выбранных источников угроз была разработана модель нарушителя безопасности ответственной информации.

Внешний нарушитель может осуществлять:

- подмену базовой и/или абонентской радиостанции;
- отправку поддельной ответственной информации в радиоканал;
- повторную отправку ранее перехваченной в радиоканале ответственной информации.

Внешний нарушитель может располагать следующей информацией о системе:

- доступные в открытых источниках сведения о системе АЛСР и ее компонентах;
- фрагменты информации, передаваемой по радиоканалу.

Внутренний нарушитель первой категории может осуществлять:

- реализацию автономных программно-аппаратных закладок в систему АЛСР на уровне ее компонентов (без внесения изменений в используемые технические средства).

Внутренний нарушитель первой категории может располагать следующей информацией:

- любая информация, доступная внешнему нарушителю;
- информация об используемых интерфейсах и способах подключения компонентов АЛСР между собой и с внешними системами;
- фрагменты информации, передаваемой между компонентами АЛСР, а также между системой АЛСР и внешними системами (системой определения свободы пути и месторасположения поезда, системой управления локомотивом и др.).

Внутренний нарушитель второй категории может осуществлять:

- все действия, доступные внутреннему нарушителю первой категории;
- внедрение вредоносных компьютерных программ в компоненты АЛСР, к которым имеется легитимный доступ.

Внутренний нарушитель первой и второй категории может располагать следующей информацией:

- любая информация, доступная внутреннему нарушителю первой категории;
- эксплуатационная документация на систему АЛСР;
- фрагменты информации, обрабатываемые компонентами системы АЛСР, к которым имеется легитимный доступ.

Внутренний нарушитель седьмой категории может осуществлять:

- все действия, доступные внутреннему нарушителю второй категории;
- модификацию ПО прикладного уровня системы АЛСР.

Внутренний нарушитель седьмой категории может располагать следующей информацией:

- любая информация, доступная внутреннему нарушителю второй категории;
- техническая документация на систему АЛСР;
- эксплуатационная документация на технические средства, используемые в АЛСР;
- алгоритм работы ПО прикладного уровня;
- любые фрагменты информации, обрабатываемой ПО прикладного уровня.

Внутренний нарушитель восьмой категории может осуществлять:

- реализацию конструктивно-встроенных программно-аппаратных закладок в технические средства, используемые на канальном и прикладном уровнях системы АЛСР.

Внутренний нарушитель восьмой категории может располагать следующей информацией:

- весь комплект документации на используемые в АЛСР технические средства;
- любые фрагменты информации, обрабатываемой в АЛСР.

В результате анализа разработанной модели нарушителя было установлено, что возможности внутренних нарушителей не зависят от наличия и использования радиоканала в системе АЛС. Следовательно, можно сделать вывод, что возможности внутренних нарушителей одинаковы для традиционных систем АЛС и систем АЛС на базе радиоканала. В связи с этим защита от угроз со стороны внутреннего нарушителя в АЛСР может быть реализована аналогично системам АЛС. Для нейтрализации данных угроз могут быть использованы способы, применяемые для обеспечения транспортной безопасности железнодорожных объектов [15], а также организационные и физические меры защиты.

Оставшиеся угрозы, влияющие на безопасность перевозочного процесса и связанные с применением в системе АЛС радиоканала, представлены в таблице 1.

Таблица 1 – Угрозы нарушения безопасности перевозочного процесса, связанные с использованием в АЛС радиоканала

№	Название	Параметр	Значение/Описание
1	Подмена базовой и/или абонентской радиостанции	Источник	Внешний нарушитель
		Уязвимость	Отсутствие процедуры взаимной аутентификации абонентов и базовой станции
		Способ реализации	Подавление сигнала базовой/абонентской радиостанции и поднятие на частоте ее радиообмена собственной радиостанции, передающей поддельную информацию
		Объект воздействия	Ответственная информация в радиоканале
		Деструктивное воздействие	Нарушение целостности ответственной информации
2	Отправка поддельной ответственной информации в радиоканал	Источник	Внешний нарушитель
		Уязвимость	Отсутствие контроля целостности передаваемой ответственной информации
		Способ реализации	Создание пакета данных с поддельной ответственной информацией и отправка его базовой/абонентской радиостанции
		Объект воздействия	Ответственная информация в радиоканале
		Деструктивное воздействие	Нарушение целостности ответственной информации
3	Повторная отправка ранее перехваченной в радиоканале	Источник	Внешний нарушитель
		Уязвимость	Отсутствие временной метки или порядкового номера пакета при передаче ответственной

Александр М. Коротин
АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ОТВЕТСТВЕННОЙ ИНФОРМАЦИИ,
ПЕРЕДАВАЕМОЙ СИСТЕМОЙ АЛС НА БАЗЕ РАДИОКАНАЛА

	ответственной информации.		информации
		Способ реализации	Перехват легитимного сообщения, передаваемого по радиоканалу, и его повторная отправка участнику движения через некоторый период времени
		Объект воздействия	Ответственная информация в радиоканале
		Деструктивное воздействие	Нарушение целостности ответственной информации

Заключение

Таким образом, в результате анализа существующих угроз безопасности ответственной информации, передаваемой системой АЛСР, был определен перечень угроз, реализация которых из-за пределов контролируемой зоны может привести к нарушению безопасности перевозочного процесса. К ним относятся угрозы, связанные с нарушением целостности ответственной информации, передаваемой системой АЛСР, реализуемые со стороны внешнего нарушителя:

- подмена базовой и/или абонентской радиостанции;
- отправка поддельной ответственной информации в радиоканал;
- повторная отправка ранее перехваченной в радиоканале ответственной информации.

Приведенные в статье результаты работы могут использоваться при исследовании безопасности систем АЛСР, анализе существующих решений по защите ответственной информации, передаваемой АЛСР, или разработке новых способов защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. О железнодорожном транспорте в Российской Федерации [Текст]: Федеральный закон от 10.01.2003 №17-ФЗ (ред. от 03.07.2016). Собрание законодательства Российской Федерации. – 2003. – № 2, (13 января). – статья 169.
2. Андерс Э. Системы автоматики и телемеханики на железных дорогах мира [Текст]: учебное пособие для вузов ж.-д транспорта Андерс Э., Берндт Т.; пер. с англ.; ред. Г. Тега, С. Власенко. – М.: Интекст, 2010. – 496 с. – ISBN 978-3-7771-0394-5.
3. ГОСТ Р 53431-2009. Автоматика и телемеханика железнодорожная. Термины и определения (с Изменением № 1) [Текст]. – Введ. 2011-01-01. – М.: Стандартинформ, 2010. – 23 с.
4. ОСТ 32.17-92. Безопасность железнодорожной автоматики и телемеханики. Основные понятия. Термины и определения [Текст]. – МПС России. – Введ. 1993-01-01. – СПб.: Типография ПИИТ, 1992. – 33 с.
5. Тильк И.Г. АЛС с использованием радиоканала [Текст] Тильк И.Г. Автоматика Связь Информатика. – 2010. – №7 – С. 7-9.
6. Шубинский И.Б. Немного о кибербезопасности [Текст] Шубинский И.Б., Макаров Б.А. Автоматика Связь Информатика. – 2014. – №8. С. 15-18.
7. Шубинский И.Б. О киберзащищенности информационных систем управления движением поездов [Текст] Шубинский И.Б., Макаров Б.А. Автоматика Связь Информатика. – 2014. – №11. – С. 6-12.
8. Макаров Б.А. Актуальность кибербезопасности на железнодорожном транспорте [Текст] Макаров Б.А. Техника железных дорог. – 2015. – №3 (31). – С. 19-24.
9. Гордейчик С.В. Кибербезопасность микропроцессорных систем ЖАТ [Текст] Гордейчик С.В. Автоматика Связь Информатика. – 2015. – №4. – С. 4-6.
10. Гордейчик С.В. Модель киберугроз МПЦ [Текст] Гордейчик С.В., Грицай Г.С., Баранов Д.С. Автоматика Связь Информатика. – 2015. – №7. – С. 18-20.
11. Konyavskiy V. The design of integrity monitoring and reliability verification system for critical information, transmitted in automatic train signaling system, based on DMR-RUS radio channel [Текст] Konyavskiy V., Epishkina A., Korotin A. Procedia Computer Science. – 2016. – Volume 88C. – P. 318-323.
12. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: утверждена ФСТЭК России 15.02.2008. – Режим доступа: [http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-](http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye)

dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения: 03.04.2017).

13. О системе технического обслуживания и ремонта локомотивов ОАО «РЖД» [Электронный ресурс]: Распоряжение ОАО «РЖД» от 17.01.2005 г. № 3р. – Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=546128#0> (дата обращения: 03.04.2017).

14. Об утверждении правил технической эксплуатации железных дорог Российской Федерации [Электронный ресурс]: Приказ Министерства транспорта РФ от 21.12.2010 № 286. – Режим доступа: http://doc.rzd.ru/doc/public/ru?id=4051&layer_id=5104&STRUCTURE_ID=704 (дата обращения: 03.04.2017).

15. О транспортной безопасности [Текст]: Федеральный закон от 09.02.2007 №16-ФЗ Собрание законодательства Российской Федерации. – 2007. – № 7, (12 февраля). – статья 837.

REFERENCES:

1. O zheleznodorozhnom transporte v Rossiyskoy Federatsii [Text]: Federalniy zakon ot 10.01.2003 №17-FZ (red. ot 03.07.2016) Sobraniye zakonodatelstva Rossiyskoy Federatsii. – 2003. – № 2, (13 yanvarya). – statya 169. (in Russian).
2. Anders E. Systems of automatics and telemechanics on the Railways of the world [Text]: textbook for universities. -d transportation Anders, E., Berndt, T.; lane. from English.; by G. Teega, S. Vlasenko. – M.: Intext, 2010. – 496 p. – ISBN 978-3-7771-0394-5. (in Russian).
3. GOST R 53431-2009. Avtomatika i telemekhanika zheleznodorozhnaya. Terminy i opredeleniya (s Izmeneniyem № 1) [Text]. – Vved. 2011-01-01. – M.: Standartinform, 2010. – 23 p. (in Russian).
4. OST 32.17-92. Bezopasnost' zheleznodorozhnoy avtomatiki i telemekhaniki. Osnovnyye ponyatiya. Terminy i opredeleniya [Text]. – MPS Rossii. – Vved. 1993-01-01. – SPb.: Tipografiya PIIT, 1992. – 33 p. (in Russian).
5. Tilk I. G. ALS using the radio [Text] Tilk I. G. Automation Communication Informatics. – 2010. – No. 7 – P. 7-9. (in Russian).
6. Shubinskiy I. B. a Little bit about cyber security [Text] Shubinskiy I. B., Makarov, B. A. Automation, Communication Informatics. – 2014. – No. 8. S. 15-18. (in Russian).
7. Shubinskiy I. B. On cybercasino information systems for train traffic control [Text] Shubinskiy I. B., Makarov, B. A. Automation, Communication Informatics. – 2014. – No. 11. – P. 6-12. (in Russian).
8. Makarov B. A. the Relevance of cyber security on railway transport [Text] Makarov B. A. the Moscow times. – 2015. – №3 (31). – P. 19-24. (in Russian).
9. S. V. Gordeychik Cybersecurity microprocessor based railway automatics and telemechanics systems [Text] S. V. Gordeychik Automation Communication Informatics. – 2015. – No. 4. – P. 4-6. (in Russian).
10. Gordeychik, S. V. Model of cyber threats MOC [Text] Gordeychik, S. V., Gritsai, G. S., Baranov D. S. Automation Communication Informatics. – 2015. – No. 7. – P. 18-20. (in Russian).
11. Konyavskiy V. The design of integrity monitoring and reliability verification system for critical information, transmitted in automatic train signaling system, based on DMR-RUS radio channel [Text] Konyavskiy V., Epishkina A., Korotin A. Procedia Computer Science. – 2016. – Volume 88C. – p. 318-323.
12. The basic model of threats to the security of personal data during their processing in personal data information systems (extract) [Electronic resource]: approved by the FSTEC of Russia 15.02.2008. – Access: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god> (data obrashcheniya: 03.04.2017). (in Russian).
13. O sisteme tekhnicheskogo obsluzhivaniya i remonta lokomotivov ОАО «РЖД» [Elektronnyy resurs]: Rasporyazheniye ОАО «РЖД» ot 17.01.2005 g. № 3р. – Access: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=546128#0> (data obrashcheniya: 03.04.2017). (in Russian).
14. Ob utverzhdenii pravil tekhnicheskoy ekspluatatsii zheleznykh dorog Rossiyskoy Federatsii [Elektronnyy resurs]: Prikaz Ministerstva transporta RF ot 21.12.2010 № 286. – Access: http://doc.rzd.ru/doc/public/ru?id=4051&layer_id=5104&STRUCTURE_ID=704 (data obrashcheniya: 03.04.2017). (in Russian).
15. O transportnoy bezopasnosti [Text]: Federal'nyy zakon ot 09.02.2007 №16-FZ Sobraniye zakonodatel'stva Rossiyskoy Federatsii. – 2007. – № 7, (12 fevralya). – statya 837. (in Russian).

Поступила в редакцию – 20 февраля июля 2017 г. Окончательный вариант – 21 мая 2017 г.

Received – February 20, 2017. The final version – May 21, 2017.