Оригинальная статья
DOI: 10.21683/1729-2646-2019-19-2-28-32

Модель оценки эффективности диагностических средств в бортовых устройствах

Ефим Н. Розенберг, *АО «НИИАС», Российская Федерация, Москва*
Александр С. Коровин, *АО «НИИАС», Российская Федерация, Москва*
Наталья Г. Пенькова, *АО «НИИАС», Российская Федерация, Москва*

Ефим Н. Розенберг

Александр С. Коровин

Наталья Г. Пенькова

Резюме. Цель *данной статьи – показать, что разработка, внедрение новых средств диагностики и улучшение существующих средств диагностики в бортовых устройствах позволяет добиться улучшения эксплуатационных характеристик и снижения вероятности перехода интеллектуальных систем железнодорожного транспорта в запрещенное состояние.* **Методика.** *Для интеллектуальных систем железнодорожного транспорта наибольший интерес представляет построение аналитической модели оценки вероятности в связи с ее возможностью наглядной демонстрации учитываемых в модели факторов. Запрещенные события, которые приводят к нарушению работоспособности интеллектуальных систем железнодорожного транспорта, являются случайными, и их можно представить в виде случайного процесса. Случайный процесс развития системы, переход системы из разрешенного состояния в запрещенное состояние, изменение состояний системы во времени может быть описан полумарковским процессом. При оценке вероятности попадания системы в запрещенное состояние возникает вопрос выбора метода расчета. В статье показана возможность представления и решения полумарковской модели с помощью связанной графовой модели [3, 5], которая обладает высоким уровнем наглядности и является хорошо формализованным методом определения вероятности перехода системы в запрещенное состояние. Множество состояний системы и связи между ними представлены в виде ориентированного графа состояний, для которого определены топологические понятия [3]. Для определения влияния введения новых средств диагностики и улучшения существующих средств диагностики в бортовых устройствах на вероятность перехода интеллектуальных систем железнодорожного транспорта в запрещенное состояние используется теорема определения вероятности перехода системы из начального неопасного состояния в опасное состояние и приведена формула расчета этой вероятности.* **Результаты.** *Реализованный в представленной статье графовый метод демонстрирует, что применение дополнительных средств диагностики позволяет уменьшить вероятность попадания системы в запрещенное состояние, то есть, в состояние, когда отказ не будет обнаружен штатными или дополнительными средствами диагностики, более чем в 2 раза.*

Ключевые слова: *бортовые устройства безопасности, блок индикации, функциональная надежность, графовая модель.*

Формат цитирования: *Розенберг Е.Н., Коровин А.С., Пенькова Н.Г., Модель оценки эффективности диагностических средств в бортовых устройствах// Надежность. 2019. №2. С. 28-32. DOI: 10.21683/1729-2646-2019-19-2-28-32*

Введение

Для планирования мероприятий по обработке запрещенных событий на железнодорожном транспорте широко применяется моделирование. Для интеллектуальных систем большие возможности предоставляет математическое моделирование. Методы математического моделирования подразделяют на две группы: аналитические и имитационные. В виду определенных недостатков метода имитационного моделирования [1], для интеллектуальных систем железнодорожного транспорта наибольший интерес представляет построение аналитической модели оценки вероятности в связи с возможностью наглядной демонстрации учитываемых в модели факторов. Запрещенные события, приводящие к нарушению работоспособности интеллектуальных систем железнодорожного транспорта, являются случайными, их можно представить в виде случайного процесса. Случайный процесс развития системы, переход системы из разрешенного состояния в запрещенное состояние, изменение состояний системы во времени может быть описан полумарковским процессом. Построение и решение полумарковских моделей в общем виде сводится к формированию системы однородных дифференциальных уравнений. Такой путь всегда чреват математическими трудностями. Поэтому в статье показана возможность представления и решения полумарковской модели с помощью связанной графовой модели [3, 5]. Такая модель обладает высоким уровнем наглядности, позволяет формализовать искомые состояния системы, а также пути перехода из разрешенного в запрещенное состояние, не требует применения сложного математического аппарата для формирования мероприятий по обработке запрещенных событий.

Постановка задачи

В настоящее время на железнодорожном транспорте одними из интеллектуальных систем на борту локомотива являются: устройство безопасности КЛУБ-У (унифицированное комплексное локомотивное устройство безопасности), комплекс БЛОК (безопасный локомотивный объединенный комплекс) и комплекс БЛОК-М (безопасный локомотивный объединенный комплекс масштабируемый). Устройство безопасности КЛУБ-У, комплекс БЛОК и комплекс БЛОК-М имеют свои блоки индикации, которые оснащены человеко-машинным интерфейсом. Блок индикации является программно-аппаратным устройством. Данное устройство предназначено для отображения информации, необходимой машинисту, помощнику машиниста, оператору, в случае беспилотного движения локомотива, сервисному персоналу при ведении локомотива и при проведении предрейсовой диагностики.

Отображаемая информация о допустимой скорости, целевой скорости, фактической скорости, профиле пути, расстоянии, о впередилежащей точке остановки, графике движения, впередиидущем поезде, показании запрещающего светофора, позволяет достигать цели по безопасному ведению локомотива – как соблюдение скоростного режима при штатной работе, так и прогнозирование безопасного режима ведения локомотива.

В процессе работы устройства возможно нарушение его работоспособности вследствие случайного отказа его аппаратной части, проявления систематической ошибки в его программе, ошибки машиниста, взаимодействующего с устройством, ошибки во входных данных. Любое нарушение работоспособности устройства расценивается как его отказ. Это приводит к отображению неактуальной информации и принятию машинистом неверных решений по соблюдению безопасного режима ведения локомотива.

В связи с этим уделяется большое внимание разработке и применению диагностических технических средств, позволяющих минимизировать вероятность попадания блока индикации в запрещенное состояние, которое приведет к нарушению работоспособности устройства отображения информации. Под запрещенным состоянием в данном случае понимается скрытый (не обнаруживаемый диагностическими средствами) отказ.

Блок индикации имеет внутренние средства диагностики, которые с приемлемой для обеспечения безопасности полнотой диагностического покрытия проверяют состояние работоспособности устройства индикации.

С помощью внутренних средств диагностики удается выявить ряд нарушений в работе блока индикации. Для расширения перечня выявляемых ошибок предлагается дополнительно перед каждой поездкой, машинистом или сервисным персоналом проводить предрейсовую диагностику блока индикации. Это, в том числе, позволяет предотвратить выход на линию локомотива с неисправным устройством безопасности.

Цель данной статьи – показать эффективность применения диагностических средств в человеко-машинном взаимодействии, применительно к бортовым устройствам. А также продемонстрировать, что разработка, внедрение новых средств диагностики и улучшение существующих средств диагностики позволяет добиться улучшения эксплуатационных характеристик блока индикации и снижения вероятности перехода блока индикации в запрещенное состояние.

Описание моделей

Представим алгоритм работы блока индикации с внутренними средствами диагностики и предрейсовой диагностикой в виде блок-схемы (рисунок 1).

Построим граф состояний алгоритма работы блока индикации, представленного на рисунке 1.

События возникновения нарушений при работе блока индикации носят случайный характер. Представим исследуемые состояния алгоритмов работы блока индикации с помощью ориентированного графа состояний $G(S, H)$, где S – конечное множество состояний системы; H – конечное множество дуг между вершинами i, j (состояниями s_i, s_j). Состояния работы блока индикации можно описать следующим образом: если блок индикации находится в состояние s_i, то с вероятностью p_{ij} он сможет перейти в состояние s_j.

На рисунке 2а представлен граф состояний, в котором для обнаружения отказа в работе блока индикации используются только внутренние средства диагностики. А на рисунке 2б представлен граф состояний, в котором для обнаружения отказа в работе устройства помимо внутренних средств диагностики блока индикации, добавляется еще предрейсовая диагностика блока индикации с участием машиниста или сервисного персонала. Для достижения цели нашей статьи исследуем граф на рисунке 2б. Граф имеет следующие состояния:

Состояние «$S1$» – отображение программой блока индикации текущей поездной обстановки;

Состояние «$S2$» – проверка наличия отказа внутренними средствами диагностики (программная проверка наличие ошибок в CAN, проверка на зависание контроллера программно переключением watchdog timer, программная проверка наличия блока индикации в конфигурации);

Состояние «$S3$» – устранение блоком индикации отказа, обнаруженного внутренними средствами диагностики (программный перезапуск CAN – интерфейса, аппаратный перезапуск контроллера с помощью watchdog timer, программный перезапуск программного обеспечения блока индикации);

Состояние «$S4$» – проверка наличия отказа с помощью предрейсовой диагностики блока индикации (правильность обработки команд, правильность отображения поездной обстановки, правильность установленной версии программного обеспечения, правильность значений параметров постоянных характеристик);

Состояние «$S5$» – устранение с помощью машиниста или сервисного персонала отказа, обнаруженного предрейсовой диагностикой (оперативное устранение

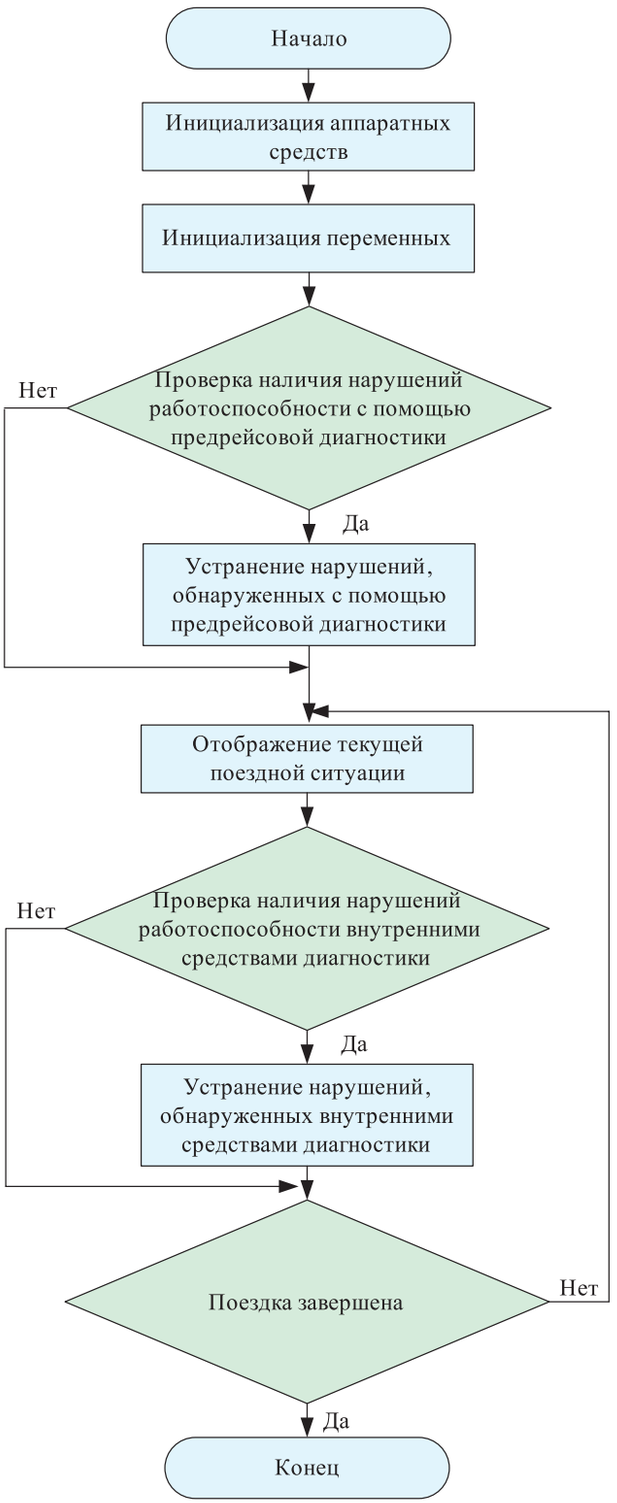

Рисунок 1 – Блок-схема алгоритма работы блока индикации с внутренними средствами диагностики и предрейсовой диагностикой.

обнаруженных ошибок, обновление программного обеспечения блока индикации, ввод правильных значений параметров постоянных характеристик);

Состояние «*S*6» – нахождение блока индикации в режиме со скрытым отказом.

S – полное множество состояний, $S = \{S1, S2, S3, S4, S5, S6\}$;

$S_р$ – подмножество состояний не относящихся к запрещенным, $S_р = \{S1, S2, S3, S4, S5\}$;

$\overline{S}_p$ – подмножество запрещенных состояний, $\overline{S}_p = \{S6\}$.

При исправных внутренних средствах диагностики и средствах предрейсовой диагностики блока индикации обнаруживается факт отказа в работе блока индикации, после чего осуществляется перевод устройства в состояние устранения отказа.

Предполагается, что при обнаружении отказа устройство восстанавливается. В случае необнаружения отказа внутренними средствами диагностики и средствами предрейсовой диагностики блока индикации вследствие их отказа или недостаточной их эффективности, осуществляется перевод устройства в состояние скрытого отказа устройства (запрещенное состояние).

Состояния *S*1 и *S*2 являются разрешенными и находятся во множестве «штатный режим работы блока индикации в период эксплуатации по прямому назначению». Выбор значений вероятностей переходов $p11$ и $p12$ выполнен исходя из соотношения объема частей программы, реализующих функцию отображения текущей поездной обстановки и функцию проверки наличия отказов внутренними средствами диагностики. Рейс длится 10 часов (то есть каждые 10 часов требуется переход в состояние предрейсовой диагностики).

Выбор значения $p21$ определен фактической надежностью блока индикации в ходе его эксплуатации. По статистике отказ блока индикации – маловероятное событие (зафиксировано 70 отказов за 2018 год на всей сети железных дорог по данным эксплуатации, всего ориентировочно 11740 изделий). То, что в ходе эксплуатации отказ не зафиксирован, не означает, что блок все это время находился в работоспособном состоянии, он мог некоторую долю времени находиться в запрещенном состоянии скрытого отказа. Распределение значений вероятностей переходов $p23$ и $p26$ осуществлено исходя из эффективности реализованной в блоке внутренней диагностики. Обнаруживающая способность отказов внутренними средствами диагностики, реализованными в блоке индикации, в соответствии с ГОСТ Р 61508-7-2012, находится на уровне 0,5.

В таблице 1 представлены значения вероятностей переходов за один шаг из *i*-го состояния в состояние *j* (p_{ij}).

Таблица 1. Матрица переходных вероятностей

		Состояние						
		1	2	3	4	5	6	∑
Состояние	1	0,72	0,18	0	0,1	0	0	1
	2	0,85	0	0,075	0	0	0,075	1
	3	1	0	0	0	0	0	1
	4	0,7	0	0	0	0,15	0,15	1
	5	1	0	0	0	0	0	1
	6	0	0	0	0	0	1	1

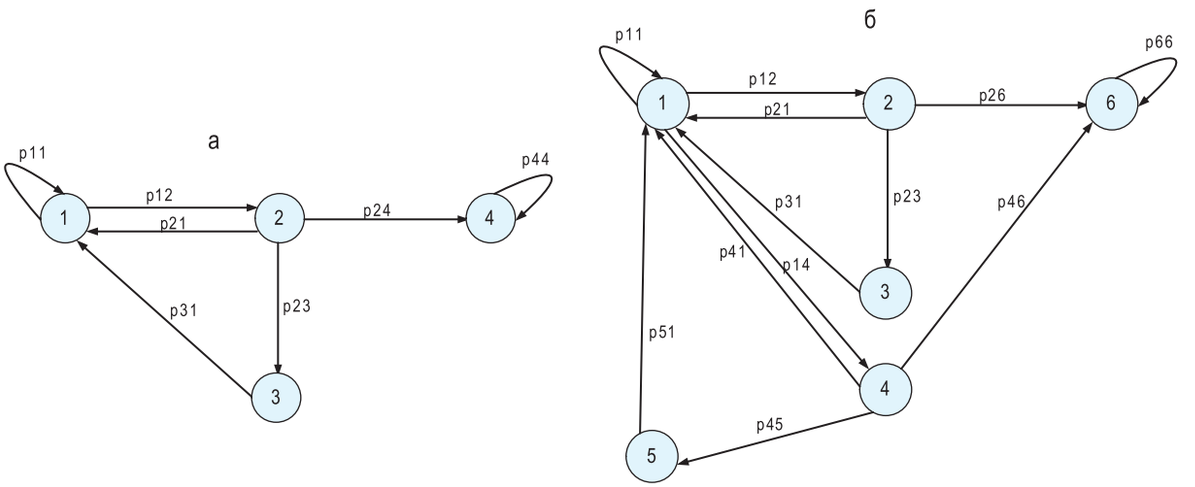

Рисунок 2 – Граф состояний: а) с внутренними средствами диагностики; б) с внутренними средствами диагностики и добавлением предрейсовой диагностики блока индикации с участием машиниста или сервисного персонала.

Задача состоит в определении влияния введения предрейсовой диагностики на вероятность перехода блока индикации в запрещенное состояние во время эксплуатации по назначению, когда используется только внутренняя диагностика.

Для решения этой задачи воспользуемся теоремой, которая гласит, что вероятность перехода системы из конкретного *i*-го начального неопасного состояния в любое опасное состояние *f* определяется выражением [5]

$$b_{if} = \frac{\sum_{f \in \overline{S}p} \sum_{k} l_k^{if} \Delta G_k^f}{\Delta G_{\overline{S}p}},$$

где l_k^{if} – *k*-ый путь, ведущий из неопасного состояния графа *i* в опасное состояние *f*;

ΔG_k^f – вес разложения графа без *f*-й вершины и вершин графа, расположенных на *k*-ом пути;

$\Delta G_{\overline{S}p}$ – вес разложения графа без вершин множества опасных состояний.

Приведем следующие топологические понятия, используемые для математического моделирования [3]:

- *путь* – это цепь последовательно соединенных однонаправленных дуг с началом в состоянии *i* и окончанием в состоянии *j*, вес пути

$$l_k^{ij} = \prod_{i,r,j \in S} p_{ir} p_{rj},$$

где p_{ir} – вероятность перехода за один шаг из состояния *i* в состояние *r*;

p_{rj} – вероятность перехода за один шаг из состояния *r* в состояние *j*;

- *замкнутый контур* – это цепь последовательно соединенных однонаправленных дуг, в которой выход конечной вершины в цепи соединен с начальной вершиной в цепи. Вес *j*-го контура определяется выражением:

$$C_j = \prod_{i,j \in S} p_{ij} p_{ji};$$

- *петля* – частный случай замкнутого контура, в ней входящие и исходящие дуги сливаются в одну дугу, вес петли $C_j = p_{ij}$;

- *разложение графа* – это часть графа, не содержащая выделенных вершин и связанных с ней дуг; вес разложения ΔG^i рассчитывается с учетом исключения из графа вершины *i* и связанных с ней дуг; вес разложения $\Delta G_{\overline{S}p}$ рассчитывается с учетом дополнительного исключения из графа вершин множества $\overline{S}_p$ и связанных с ними дуг; вес разложения ΔG_k^f рассчитывается с учетом исключения из графа вершины *f*, а также вершин, расположенных на *k*-ом пути из начальной вершины в вершину *f* и связанных с ними дуг;

- *вес разложения* находится по формуле Мезона:

$$\Delta G = 1 - \sum_{j} C_j + \sum_{rj} C_r \cdot C_j - \sum_{irj} C_i \cdot C_r \cdot C_j + \ldots$$

Для того чтобы оценить эффективность введения предрейсовой диагностики, рассчитаем условную вероятность перехода из исходного состояния «1» в запрещенное состояние «6», при условии, что штатные средства диагностики (внутренняя диагностика) отключены (пути *S*1→*S*2→*S*6 и *S*1→*S*2→*S*3).

В соответствии с теоремой оценки вероятности перехода из начального разрешенного состояния в запрещенное состояние, условная вероятность перехода из *S*1 в *S*6 определяется выражением:

$$b_{16/\overline{S}_{126}} = \frac{\sum_{f \in \overline{S}p} \sum_{k} l_k^{16} \Delta G_k^6}{\Delta G_{\overline{S}p}}.$$

Как видно из графа на рисунке 2б, количество *k* путей перехода из *S*1 в *S*6 при условии, что для обнаружения отказа в работе блока индикации используется только предрейсовая диагностика блока индикации с участием машиниста или сервисного персонала, равно 1.

Определение весов путей: $l_1^{16} = S1 \rightarrow S4 \rightarrow S6 = p14 \cdot p46$.

Определение весов контуров:

*C*1: *S*1→*S*1, вес контура – *p*11;

*C*2: *S*1→*S*2→*S*1, вес контура – *p*12·*p*21;

$C3$: $S1 \rightarrow S2 \rightarrow S3 \rightarrow S1$, вес контура – $p12 \cdot p23 \cdot p31$;
$C4$: $S1 \rightarrow S4 \rightarrow S1$, вес контура – $p14 \cdot p41$;
$C5$: $S1 \rightarrow S4 \rightarrow S5 \rightarrow S1$, вес контура – $p14 \cdot p45 \cdot p51$;
$C6$: $S6 \rightarrow S6$, вес контура – $p66$.

Для рассматриваемого случая вес разложения графа без вершин множества запрещенных состояний равен: $\Delta G_{\bar{S}p} = 1 - (C1+C2+C3+C4+C5)$.

А вес разложения с учетом исключения из графа вершины «6», а также вершин, расположенных на k-ом пути из вершины «1» в вершину «6» и связанных с ними дуг равен: $\Delta G_1^6 = 1$.

Подставляя данные из таблицы 1 получаем, что условная вероятность перехода из состояния $S1$ в состояние $S6$:

$$b_{16/\bar{S}_{126}} = \frac{\sum_{f \in \bar{S}p} \sum_k l_k^{16} \Delta G_k^6}{\Delta G_{\bar{S}p}} =$$

$$= \frac{p14 * p46 * \Delta G_1^6}{1 - C1 - C2 - C3 - C4 - C5} = 0,53.$$

Поскольку исследуемые модели описывают полную группу событий, то вероятность попадания в единственное запрещенное состояние в обоих случаях равна 1. Таким образом, исходя из вычисленного значения условной вероятности $b_{16/\bar{S}_{126}}$, получаем, что введение предрейсовой диагностики блока индикации с участием машиниста или сервисного персонала позволяет уменьшить вероятность попадания блока индикации в запрещенное состояние во время рейса больше, чем в 2 раза (с 1 до 0,47).

Заключение

В данной статье показана эффективность добавления предрейсовой диагностики блока индикации с участием машиниста или сервисного персонала к внутренним средствам диагностики обнаружения отказа в работе блока индикации. Так, вероятность попадания в запрещенное состояние, то есть, в состояние, когда отказ не будет обнаружен штатными или дополнительными средствами диагностики, уменьшится более чем в 2 раза.

Благодарность

Авторы выражают благодарность профессору, доктору технических наук Шубинскому Игорю Борисовичу за оказанную помощь, ценные советы и замечания при написании настоящей статьи.

Библиографический список

1. **Ивницкий В.А.** Моделирование информационных систем железнодорожного транспорта. Учебное пособие [Текст] / В.А. Ивницкий. – М.: МИИТ, 2011. – 143 с.

2. **Шубинский И.Б.** Функциональная надежность информационных систем. Методы анализа [Текст] / И.Б. Шубинский. – М.: ООО «Журнал «Надежность», 2012. – 296 с.

3. **Шубинский И.Б.** Надежные отказоустойчивые информационные системы. Методы синтеза [Текст] / И.Б. Шубинский. – М.: Журнал Надежность, 2016. – 544 с.

4. **Шубинский И.Б.** О понятии функциональной надежности [Текст] / И.Б. Шубинский, Х. Шебе // Надежность. – 2012. – № 4. – С. 74-84.

5. **Шубинский И.Б.** Методы обеспечения функциональной надежности программ [Текст] / И.Б. Шубинский // Надежность. – 2014. – №4. – С. 87-101.

6. **Шубинский И.Б.** Графовый метод оценки производственной безопасности на объектах железнодорожного транспорта [Текст] / И.Б. Шубинский, А.М. Замышляев, О.Б. Проневич // Надежность. – 2017. – Т.17. – № 1. – С. 40-45.

7. **Проневич О.Б.** Алгоритм расчета и прогнозиорвания показателей функциональной безопасности систем электроснабжения железнодорожного транспорта [Текст] / О.Б. Проневич, В.Э. Швед // Надежность. – 2018. – № 18(3). – С. 46-55.

8. **Розенберг Е.Н.** Функциональная надежность программного обеспечения блока индикации комплекса БЛОК [Текст] / Е.Н. Розенберг, Н.Г. Пенькова, А.С. Коровин // Надежность. – 2017. – № 17(2). – С. 36-40.

9. **Шухина Е.Е.** Безопасный локомотивный объединенный комплекс БЛОК [Текст] / Е.Е. Шухина, В.И. Астрахан. – М.: 2013. – 103 с.

10. **Зорин В.И.** Унифицированное комплексное локомотивное устройство безопасности (КЛУБ-У) [Текст] / В.И. Зорин, В.И. Астрахан. – М.: ГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2008. – 177 с.

11. **ГОСТ Р МЭК 61508-7-2012.** Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства [Текст]. – Введ. 2012-10-29. – М.: Стандартинформ, 2014. – V, 94 с.

Сведения об авторах

Ефим Н. Розенберг – профессор, доктор технических наук, первый заместитель Генерального директора АО «НИИАС». Российская Федерация, Москва, e-mail: info@vniias.ru

Александр С. Коровин – главный специалист сектора разработки микропроцессорных устройств АО «НИИАС». Российская Федерация, Москва, e-mail: A.Korovin@vniias.ru

Наталья Г. Пенькова – заместитель начальника центра безопасности и алгоритмической поддержки АО «НИИАС». Российская Федерация, Москва, e-mail: N.Penkova@vniias.ru

Поступила 08.04.2019