Надежность, том 17, №2 2017
Оригинальная статья
DOI: 10.21683/1729-2646-2017-17-2-36-40
УДК 519.23/.24/.25

# Функциональная надежность программного обеспечения блока индикации комплекса БЛОК

**Ефим Н. Розенберг,** *ОАО «НИИАС», Москва, Россия*
**Наталья Г. Пенькова,** *ОАО «НИИАС», Москва, Россия*
**Александр С. Коровин,** *ОАО «НИИАС», Москва, Россия*

*Ефим Н. Розенберг*

*Наталья Г. Пенькова*

*Александр С. Коровин*

**Резюме. Цель.** *Статья посвящена решению задачи оценки функциональной надежности программного обеспечения (ПО) блока индикации, входящего в состав безопасного локомотивного объединенного комплекса БЛОК, связанной с ошибками программы при заданном времени работы системы 24 часа. Одной из центральных задач является расчет значений таких атрибутов функциональной надежности ПО, как безошибочность, правильность, защищенность, контролируемость, безотказность, устойчивость ПО к ошибкам и готовность, которые являются ключевыми показателями для оценки работоспособности устройств безопасности. При этом ставится задача оценки целесообразности проведения проверки программного обеспечения блока индикации перед каждой поездкой с помощью предрейсового тестирования.* **Методика.** *В исходных условиях задачи отсутствуют статистические данные о реализациях программы в процессе ее сопровождения. Также отсутствуют сведения о структурных характеристиках программы (количестве операторов, операндов, циклов и др.), что не позволяет использовать статические модели надежности типа модели Холстеда или модели IBM и им подобные. Поэтому в качестве аппарата определения исходных данных для решения задачи выбрана модель Шумана. Методика оценки функциональной надежности блока индикации основывается на результатах работы [1].* **Результаты.** *На первом этапе решения задачи были определены значения следующих исходных данных: первоначальное количество дефектов в программе, интенсивность ошибок программы и вероятность правильного однократного выполнения программы. С использованием найденных значений на следующем этапе получены значения таких параметров надежности, как вероятность отсутствия ошибки в результате выполнения программы в течение заданного времени, вероятность отсутствия отказов в работе блока индикации при выполнении программы в течение заданного времени и среднее время до ошибки программы. Рассчитав вероятность $P_{по}(t)$ отсутствия ошибки в результате выполнения программы в течение заданного времени, оценили такие атрибуты функциональной надежности ПО, как безошибочность, правильность, защищенность и контролируемость. Рассчитав вероятность отсутствия отказов в работе блока индикации $P_{Б}(t)$ при выполнении программы в течение заданного времени, дали оценку таким атрибутам, как безотказность и устойчивость ПО к ошибкам, а рассчитав среднее время до ошибки программы $T_{ср.по}$ и зная среднее время простоя, вызванного необходимостью устранения ошибки программы $\tau_{пп}$, определили атрибут готовности блока индикации в произвольный момент времени безошибочно выполнять определенный информационный процесс $к_{фг}$. Полученные значения коэффициента частичной функциональной готовности блока индикации показали, что проведение проверки блока индикации перед каждой поездкой и, в случае обнаружения ошибок, оперативное их устранение позволит существенно повысить пользовательские характеристики блока индикации локомотивного (БИЛ) в рамках своевременного информирования машиниста об актуальной поездной обстановке с целью своевременного принятия им решения по управлению движением поезда.*

**Ключевые слова:** *безопасный локомотивный объединенный комплекс БЛОК, блок индикации, функциональная надежность.*

**Формат цитирования:** *Розенберг Е.Н., Пенькова Н.Г., Коровин А.С. Функциональная надежность программного обеспечения блока индикации комплекса БЛОК // Надежность. 2017. Т. 17, № 2. С. 36-40. DOI: 10.21683/1729-2646-2017-17-2-36-40*

Безопасный локомотивный объединенный комплекс БЛОК является современным бортовым средством обеспечения безопасности движения поездов, широко внедряемым на сети Российских железных дорог. Комплекс БЛОК пришел на смену и заменяет собой, совмещая в себе их функции, такие бортовые устройства безопасности, как КЛУБ (комплексное локомотивное устройство безопасности), САУТ (система автоматического управления торможением) и ТСКБМ (телемеханическая система контроля бодрствования машиниста).

БЛОК предназначен для обеспечения безопасности движения поездов на участках железных дорог с автономной и электрической тягой постоянного и переменного тока, оборудованных путевыми устройствами систем АЛСН (автоматическая локомотивная сигнализация непрерывного типа с числовым кодированием),

АЛС-ЕН (многозначная автоматическая локомотивная сигнализация непрерывного типа с фазоразностной модуляцией несущей частоты), САУТ, аппаратурой цифрового радиоканала, точечного канала, системы координатного интервального регулирования движения поездов, а также на участках, оборудованных устройствами полуавтоматической блокировки.

Важное место в обеспечении безопасности движения занимают вопросы человеко-машинного взаимодействия, которое осуществляется через устройства индикации и управления. Комплекс БЛОК имеет свой блок индикации. На блоке индикации отображается вся необходимая информация о поездной ситуации по маршруту следования и работе системы на борту локомотива, позволяющая машинисту достигать поставленные цели и успешно находить решение возникающих проблем.

Рассмотрим пример расчета показателей функциональной надежности программы блока индикации, входящего в состав безопасного локомотивного объединенного комплекса БЛОК.

## Результаты тестирования программного обеспечения блока индикации

Программа блока индикации предназначена для отображения машинисту поездной ситуации в реальном масштабе времени.

На этапе отладки проведено тестирование программы. Блок индикации подключен согласно структурной схеме, которая показана на рисунке 1.

В состав структурной схемы входит:

- источник питания;
- блок индикации БИЛ;
- персональный компьютер, с установленной на нем имитационной программой;
- Kvaser, преобразователь интерфесов USB в CAN (Controller Area Network).

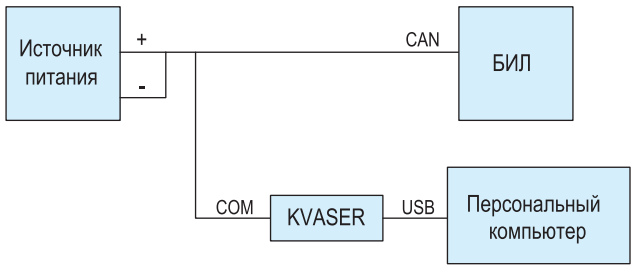


Рис. 1

Заявки на выполнение программы поступают с интенсивностью $\gamma = 1800$ 1/ч от имитационной программы, которая установлена на персональный компьютер.

Проведено 14 этапов тестирования:

1. Тестирование отображения сигналов светофора по данным АЛСН совместно с проверкой правильности отображения частоты по АЛСН.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации о поочередной смене сигналов светофора по АЛСН (значения сигналов светофора: белый, красный, красно-желтый, желтый, зеленый) и о поочередной смене частоты по АЛСН (значение частот: 25 Гц, 50 Гц, 75 Гц, 25 Гц). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

2. Тестирование отображения сигналов светофора по данным АЛС-ЕН совместно с проверкой правильности отображения движения прямо или с отклонением.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации о поочередной смене сигналов светофора по АЛС-ЕН (значения сигналов светофора: белый мигающий, красный, красно-желтый, 1БУ, 2БУ, 3БУ, 4БУ, 5БУ) и о поочередной смене движения прямо или с отклонением (значения: отсутствует, прямо, с отклонением). В результате тестирования данного этапа в работе программы было обнаружено две ошибки: при значениях светофоров по АЛС-ЕН красно-желтый и красный на блоке индикации неправильно отображается движение прямо или с отклонением.

3. Проверка правильности отображения фактической, целевой и допустимой скоростей.

В течение 8 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значениями фактической, целевой и допустимой скоростей. Задаваемые значения фактической скорости: 0, 20, 40, 60, 80, 100, 120, 140, 160, 180, 200, 220, 240, 260, 120, 0. Задаваемые значения целевой скорости: 0, 20, 40, 60, 80, 100, 120, 140, 160, 180, 200, 220, 240, 260, 200. Задаваемые значения допустимой скорости: 0, 20, 40, 60, 80, 100, 120, 140, 160, 180, 200, 220, 240, 260, 0). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

4. Проверка правильности отображения координаты, номера пути, направления движения вперед или назад.

В течение 9 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значениями координат (0 км 0 пк 1 м, 4 км 5 пк 99 м, 9999 км 9 пк 99 м, 0 км 0 пк 0 м), со значениями номера пути (0, 8, 15, 1), со значениями направления движения (вперед, назад). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

5. Проверка правильности отображения названия цели, вида цели и расстояния до цели и названия станции.

В течение 8 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации с названиями цели (Икша, Нахабино, Нет цели), с видами цели (светофор, станция, опасное место, мост, переезд, платформа, тоннель, стрелка, рельсовая цепь, ППУ ТКС-САУТ (приемопередающее устройство точечного канала связи САУТ), тупик, хвост поезда, место остановки, работают люди, усл-разр. сигнал, станция), с расстояниями до цели (1 м, 1000 м, 8191 м, 0 м) и с названиями станции (Москва, Тушино, Болевое, Нет

станции). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

6. Проверка правильности отображения давления в тормозном цилиндре, тормозной магистрали и в уравнительном резервуаре.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значениями давления в тормозном цилиндре (0,1 МПа, 0,5 МПа, 1,0 МПа, 0 МПа), со значениями давления в тормозной магистрали (0,1 МПа, 0,5 МПа, 1,0 МПа, 0 МПа) и со значениями давления в уравнительном резервуаре (0,1 МПа, 0,5 МПа, 1,0 МПа, 0 МПа). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

7. Формирование блоком индикации сообщений в CAN-интерфейс о состоянии работоспособности программы.

В течение 10 часов с помощью имитационной программы происходила проверка формирования блоком индикации сообщений в CAN-интерфейс, каждые 500 мс, о состоянии работоспособности программы. В результате тестирования данного этапа были обнаружены две ошибки, и блок индикации дважды производил программно перезапуск программного обеспечения и начинал снова формировать каждые 500 мс сообщения в CAN-интерфейс о состоянии работоспособности.

8. Проверка правильности отображения режима работы автоведения, значения заданной скорости от автоведения и времени по графику от автоведения.

В течение 9 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значениями режима работы автоведения (автоведение выключено, автоведение в информационном режиме, автоведение в автоматическом режиме), со значениями заданной скорости от автоведения (0, 20, 40, 60, 80, 100, 120, 140, 160, 180, 200, 220, 240, 260, 120, 0), со значениями времени по графику от автоведения (0 часов 10 минут 15 секунд; 3 часа 12 минут 19 секунд; 5 часов 19 минут 22 секунды; 11 часов 23 минуты 27 секунд; 15 часов 27 минут 34 секунды; 19 часов 34 минуты 38 секунд; 22 часа 44 минуты 47 секунд; 23 часа 57 минут 59 секунд). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

9. Проверка правильности отображения предварительной сигнализации, предварительной сигнализации ТСКБМ, запроса подтверждения работоспособности машиниста и устойчивой связи по радиоканалу.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значением предварительной сигнализации (включена, выключена), со значением предварительной сигнализации ТСКБМ (включена, выключена), со значением запроса подтверждения работоспособности машиниста (есть запрос, нет запроса) и со значением устойчивой связи по радиоканалу (наличие связи, отсутствие связи). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

10. Проверка правильности отображения ускорения, наличия нейтральной вставки/токораздела и расстояния до нейтральной вставки/токораздела.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значениями ускорения (-1,0, -0,92, -0,80, -0,73, -0,69, -0,53, -0,44, -0,30, -0,22, -0,10, -0,02, 0,04, 0,15, 0,23, 0,37, 0,49, 0,56, 0,66, 0,79, 0,83, 0,94, 1,0), со значениями наличия нейтральной вставки/токораздела (нет нейтральной вставки или токораздела, есть нейтральная вставка, есть токораздел), со значениями расстояния до нейтральной вставки/токораздела (0 м, 140 м, 631 м, 1202 м, 3044 м, 9999 м, 42142 м, 65535 м). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

11. Проверка правильности ввода команд в информационной строке блока индикации.

В течение 8 часов с помощью клавиатуры блока индикации вводились команды в информационной строке (К0, К5, К6, К7, К71, К70, К91, К92, К261, К517, К522, К773, К799, К809, К800, К1029, К2565). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

12. Проверка правильности отображения в информационной строке блока индикации диагностических сообщений.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со следующими диагностическими сообщениями (срыв кон, срыв эпк тскбм, срыв эпк саут, боксование, номер электронной карты, отображение наличия в конфигурации модулей, которые входят в состав комплекса БЛОК, отображение версии, подверсии и контрольной суммы модулей, которые входят в состав комплекса БЛОК). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

13. Проверка правильности отображения текущего времени.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значениями текущего времени (0 часов 10 минут 15 секунд; 3 часа 12 минут 19 секунд; 5 часов 19 минут 22 секунды; 11 часов 23 минуты 27 секунд; 15 часов 27 минут 34 секунды; 19 часов 34 минуты 38 секунд; 22 часа 44 минуты 47 секунд; 23 часа 57 минут 59 секунд). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

14. Проверка правильности отображения состояния кассеты регистрации и режима работы.

В течение 7 часов с помощью имитационной программы задавались CAN-сообщения для блока индикации со значением состояния кассеты регистрации (в наличии, отсутствует) и со значениями режима работы (поездной, маневровый, режим двойной тяги). В результате тестирования данного этапа ошибки в работе программы не обнаружены.

Результаты этапов тестирования приведены в сводной таблице 1.

**Таблица 1.**

| Номер этапа тестирования | Длительность этапа тестирования *t*, ч | Количество выявленных ошибок программы *m* |
|---|---|---|
| 1 | 7 | 0 |
| 2 | 7 | 2 |
| 3 | 8 | 0 |
| 4 | 9 | 0 |
| 5 | 8 | 0 |
| 6 | 7 | 0 |
| 7 | 10 | 2 |
| 8 | 9 | 0 |
| 9 | 7 | 0 |
| 10 | 7 | 0 |
| 11 | 8 | 0 |
| 12 | 7 | 0 |
| 13 | 7 | 0 |
| 14 | 7 | 0 |

## Исходные условия для расчета показателей надежности программного обеспечения блока индикации

Кроме результатов тестирования, приведенных в предыдущем разделе статьи, в расчете показателей надежности программного обеспечения БИЛ использованы следующие исходные данные. Вероятность того, что ошибка ПО приведет к отказу функционирования блока $g_{фт} = 0{,}047$ [1]. Интенсивность отказов аппаратной составляющей блока индикации составляет $\lambda_{ап} = 3{,}01 \cdot 10^{-6}$ 1/ч [4]. Предполагается наличие подпрограммы самотестирования, характеризующейся вероятностью обнаружения отказов на уровне $\alpha = 0{,}5$ [3]. А также, наличие механизмов реагирования на обнаружения отказа, характеризующихся вероятностью успешного парирования обнаруженного функционального отказа $\beta = 0{,}99$.

$$\beta = 1 - \lambda_{ап} * t,$$

где $\lambda_{ап}$ – интенсивность отказов аппаратной составляющей блока индикации;

$t$ – заданное время работы системы.

Среднее время простоя блока индикации, вызванного необходимостью устранения ошибки программы, равно $\tau_{пп} = 24$ ч.

Требуется рассчитать показатели надежности блока, связанные с ошибками программы при заданном времени работы системы $t = 24$ часа в предположении отсутствия сбойных ошибок, а также в предположении, что при исправлении обнаруженных ошибок новые дефекты не вносятся в программу.

## Расчет показателей надежности программного обеспечения блока индикации

В исходных условиях задачи отсутствуют статистические данные о реализациях программы в процессе ее сопровождения. Также отсутствуют сведения о структурных характеристиках программы (количестве операторов, операндов, циклов и др.), что не позволяет использовать статические модели надежности типа модели Холстеда или модели IBM и им подобные. Поэтому выберем путь решения задачи, базирующийся на модели Шумана. А именно: найдем первоначальное количество дефектов в программе, затем интенсивность ошибок и значения искомых вероятностей, характеризующие показатели надежности ПО.

Первоначальное количество дефектов в программе $N$ вычисляют из следующего уравнения:

$$\sum_{j=1}^{k} m_j \cdot \frac{\sum_{j=1}^{k} t_j}{\sum_{j=1}^{k} \frac{m_j}{N - n_{j-1}}} = \sum_{j=1}^{k} (N - n_{j-1}) t_j,$$

где $k = 14$ (количество этапов тестирования);

$m_j$ – количество выявленных ошибок программы на $j$-ом этапе тестирования;

$n_j = m_1 + m_2 + \ldots + m_j$ – суммарное количество выявленных ошибок программы на 1–$j$-ом этапах тестирования;

$t_j$ – длительность $j$-го этапа тестирования.

Значения $m_j$, $n_j$ и $t_j$ заданы в таблице 1. В соответствии с данными значениями методом подбора получено $N = 7$.

Интенсивность ошибок программы $\lambda_{по}$ вычисляется по формуле Шумана

$$\lambda_{по} = \frac{\sum_{j=1}^{k} \frac{m_j}{N - n_{j-1}}}{\sum_{j=1}^{k} t_j} \left(N - n_k\right)$$

При значениях переменных, рассчитанных на предыдущем шаге $\lambda_{по}$ составляет 0,014 1/ч.

Вероятность правильного однократного выполнения программы $P_{по\ одн}$ после ее отладки вычисляется по формуле

$$P_{по\ одн} = \frac{1 - \frac{\lambda_{по}}{\gamma}}{P_п} = \frac{1 - \frac{0{,}014}{1800}}{1} = 1 - 7{,}77 \cdot 10^{-6} = 0{,}99999,$$

где $P_п$ – вероятность отсутствия сбойных ошибок, которая в предположении отсутствия сбойных ошибок (см. пункт Исходные данные) равна 1.

Теперь определим показатели надежности блока, связанные с ошибками программы при заданном времени работы системы 24 ч.

Вероятность $P_{по}(t)$ отсутствия ошибки в результате выполнения программы в течение заданного времени $t = 24$ ч.

$$P_{по}(t) = \exp(-\lambda_{по} t) = \exp(-24 \cdot 0,014) \approx 0.7.$$

Среднее время до ошибки программы $T_{ср.по}$

$$T_{ср.по} = \frac{1}{\lambda_{по}} = \frac{1}{0,014} = 71,43 \text{ ч.}$$

Вероятность отсутствия отказов в работе блока индикации $P_Б$(t) при выполнении программы в течение заданного времени $t$ = 24 ч.

$$P_Б(t) = \exp(-\lambda_{ап} t)[1-(1-\alpha\beta)g_{фт}(1-\exp(-\lambda_{по} t))] =$$
$$= \exp(-24 \cdot 3,01 \cdot 10^{-6}) \cdot [1-(1-0,5 \cdot 0,99) \cdot 0,047 \cdot$$
$$\cdot (1-\exp(-24 \cdot 0,014))] = 0,99.$$

Среднее время до частичного функционального отказа блока индикации $T_{ср.б}$

$$T_{ср.\,б} = \frac{1бg_{фт}(1+\,б\,е}{\lambda_{ап}} + \frac{g_{фт}(1+\,б}{\lambda_{по}+\lambda_{ап}} = \frac{1+б\,е\,время\,до,99)}{3,01б10^{-6}} +$$
$$+ \frac{101б\,е\,время\,до\,час}{0,014+3,01p10^{-6}} = 3,08410^5 \text{ ч.}$$

Коэффициент частичной функциональной готовности блока индикации

$$K_{фг} = \frac{T_{ср.по}}{T_{ср.по}+\tau_{пп}} = \frac{71,43}{71,43+24} = 0,749.$$

В результате стендовых испытаний программного обеспечения блока индикации на этапе отладки удалось выявить ряд ошибок программы. Однако не исключено, что при работе данного программного обеспечения на локомотиве в реальных условиях эксплуатации могут быть выявлены и другие ошибки. Поэтому целесообразно проводить проверку программного обеспечения блока индикации перед каждой поездкой и, в случае обнаружения ошибок в результате предрейсового тестирования, оперативно осуществлять устранения обнаруженных ошибок программного обеспечения. Систематическое проведение такой процедуры позволит существенно повысить показатель готовности БЛОК. Например, сокращение времени устранения ошибки программы с 24 часов до 1 часа за счет своевременного устранения обнаруженных отказов ($\tau_{пп}$ = 1 ч), позволяет получить значение коэффициента частичной функциональной готовности блока индикации равное

$$K_{фг} = \frac{T_{ср.по}}{T_{ср.по}+\tau_{пп}} = \frac{71,43}{71,43+1} = 0,986.$$

Таким образом, при времени устранения ошибки программы, равном $\tau_{пп}$ = 24 часа, коэффициент частичной функциональной готовности блока индикации равен $K_{фг}$ = 0,749, а сокращение времени устранения ошибки до $\tau_{пп}$ = 1 часа, позволяет получить значение коэффициента частичной функциональной готовности блока индикации равное $K_{фг}$ = 0,986, что практически на 25% улучшает эксплуатационные характеристики ПО БИЛ.

## Заключение

В рамках данной статьи был рассмотрен пример расчета показателей функциональной надежности программы блока индикации, входящего в состав безопасного локомотивного объединенного комплекса БЛОК. На примере данного частного случая показано, что используемая методика работает и может применяться на практике.

Полученные значения коэффициента частичной функциональной готовности блока индикации показывают, что проведение проверки блока индикации перед каждой поездкой и, в случае обнаружения ошибок, оперативное их устранение позволит существенно повысить пользовательские характеристики БИЛ в рамках своевременного информирования машиниста об актуальной поездной обстановке с целью своевременного принятия им решения по управлению движением поезда.

## 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. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. ООО «Журнал Надежность» 2012 г. – 296 с.;

2. Шухина Е.Е., Астрахан В.И. Безопасный локомотивный объединенный комплекс БЛОК. Москва 2013г. – 103 с.;

3. ГОСТ Р МЭК 61508-7-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»;

4. Пояснительная записка с расчетом надежности для блока индикации.

## Сведения об авторах

**Ефим Н. Розенберг** – профессор, доктор технических наук, первый заместитель Генерального директора ОАО «НИИАС». Россия, 109029, Москва, ул. Нижегородская, д. 27, стр. 1, тел. 8 (499) 262-62-17, e-mail: info@vniias.ru

**Наталья Г. Пенькова** – заместитель начальника центра безопасности и алгоритмической поддержки ОАО «НИИАС». Россия, 109029, Москва, ул. Нижегородская, д. 27, стр. 1, тел. 8 (499) 260-77-52, e-mail: N.Penkova@vniias.ru

**Александр С. Коровин** – главный специалист сектора разработки микропроцессорных устройств ОАО «НИИАС». Россия, 109029, Москва, ул. Нижегородская, д. 27, стр. 1, тел. 8 (499) 262-82-53, e-mail: A.Korovin@vniias.ru

**Поступила 06.12.2016**