УДК681.32.019.3

А.В. ФЕДУХИН[*], Н.В. СЕСПЕДЕС ГАРСИЯ[*]

ПАКЕТ ПРИКЛАДНЫХ ПРОГРАММ GARANTmod В ИНЖИНИРИНГЕ ГАРАНТОСПОСОБНЫХ СИСТЕМ

[*]Институт проблем математических машин и систем НАН Украины, Киев, Украина

Анотація. *Наводиться опис пакета прикладних програм GARANTmod, призначеного для розробників гарантоздатних комп'ютерних систем. Пакет вирішує різноманітні завдання щодо оцінки та забезпечення гарантоздатності систем критичного застосування.*
Ключові слова: *гарантоздатність, безвідмовність, готовність, живучість, цілісність, конфіденційність, обслуговуваність, функціональна безпека, рівень гарантоздатності.*

Аннотация. *Приводится описание пакета прикладных программ GARANTmod, предназначенного для разработчиков гарантоспособных компьютерных систем. Пакет решает разнообразные задачи по оценке и обеспечению гарантоспособности систем критического применения.*
Ключевые слова: *гарантоспособность, безотказность, готовность, живучесть, целостность, конфиденциальность, обслуживаемость, функциональная безопасность, уровень гарантоспособности.*

Abstract. *The description of the GARANTmod application package designed for developers of dependable computer systems is given. The package solves various problems of the evaluation of dependability and security of critical application systems.*
Keywords: *dependability, reliability, availability, survivability, integrity, confidentiality, serviceability, functional safety, level of dependability.*

1. Введение

Создание компьютерных систем, отвечающих требованиям гарантоспособности, является сложной и комплексной задачей, решение которой невозможно без привлечения компьютерной техники на всех этапах их инжиниринга. В настоящее время существует настоятельная потребность в создании наглядного инструментария, предназначенного для разработчиков гарантоспособных компьютерных систем (ГКС).

Целью статьи является описание основных характеристик и области применения пакета прикладных программ GARANTmod, решающего все основные задачи обеспечения гарантоспособности при проектировании ГКС.

2. Атрибутивная модель гарантоспособности систем

Впервые понятие «гарантоспособные системы» было введено А. Авиженисом в 70-х годах прошлого столетия. В те времена гарантоспособность всецело сводилась к свойствам (атрибутам) безотказности и отказоустойчивости системы. Позднее это понятие было расширено атрибутами безопасность, живучесть и понятием гарантоспособные вычисления. В результате чего модель гарантоспособности систем А. Авижениса [1], названная нами атрибутивной моделью, на сегодняшний день включает следующие составляющие: безотказность, готовность, живучесть, целостность (внешняя безопасность), конфиденциальность (внутренняя безопасность), обслуживаемость, функциональная безопасность. Таким

образом, гарантоспособные системы – это высоконадежные, отказоустойчивые, безопасные и живучие системы с гарантированно достоверными вычислениями.

Для реализации системного подхода к созданию гарантоспособных систем предполагается разработка специальной Программы обеспечения гарантоспособности (ПОГ), аналогичной Программе обеспечения надежности (ПОН) [2], но расширенной мероприятиями, обеспечивающими реализацию дополнительных атрибутов: живучесть, целостность, конфиденциальность и функциональная безопасность.

3. Пакет прикладных программ GARANTmod

Для разработки ПОГ и для реализации всех ее требований к вновь создаваемой ГКС служит пакет прикладных программ GARANTmod. Данный пакет представляет собой программный продукт, написанный в средах Visual Basic (интерфейс, экранные формы) и Quick Basic (расчетные модули). Интерфейс пакета выполнен в виде главного меню со следующими опциями:

– программа обеспечения гарантоспособности;
– теоретические основы обеспечения гарантоспособности;
– безотказность;
– готовность;
– живучесть;
– целостность;
– конфиденциальность;
– обслуживаемость;
– функциональная безопасность;
– уровень гарантоспособности;
– помощь.

Пример экранных форм пакета приведен на рис. 1.

Рис. 1. Экранные формы титульной и главной страниц пакета GARANTmod

При переходе на главную страницу пакета раскрывается содержание меню первого уровня. Так, например, опция Программа обеспечения гарантоспособности содержит следующие разделы:

– план-график работ по ПОГ;
– распределение обязанностей и ответственности;
– перечень мероприятий на каждом этапе жизненного цикла ГКС [15];

– отчет о выполнении ПОГ.

Опция Теоретические основы обеспечения гарантоспособности предназначена для ознакомления пользователя с методами и алгоритмами, заложенными в программные модули пакета GARANTmod. Эта опция содержит следующие разделы:

– теория проектирования гарантоспособных систем [1, 56, 61, 62];
– теоретические основы надежности систем [3];
– теоретические основы живучести систем [4];
– методы обеспечения целостности систем;
– методы обеспечения конфиденциальности систем.

Например, раздел Теоретические основы надежности систем освещает следующие вопросы:

– теоретические модели надежности [3];
– методы анализа надежности [17, 18, 22, 47, 48, 50];
– методы расчета надежности [14, 16, 18];
– методы прогнозирования надежности [15,18,32,33,43];
– методы моделирования надежности [5, 8, 9–11, 23, 45, 46, 49, 53, 56, 58, 60];
– методы испытаний на надежность [12, 13, 20, 21, 30, 35–38, 61];
– методы оценки эффективности [31, 47].

В качестве основной теоретической модели надежности элементов, составных частей и системы в целом принято *DN* -распределение наработки до отказа (на отказ) [3], специально разработанное для описания надежности изделий электронной техники, электронных устройств и систем, построенных на их основе.

Рассмотрим более подробно опции главного меню, касающиеся атрибутов гарантоспособности систем.

Опция Безотказность содержит следующие разделы (рис. 2):

– расчет надежности изделий электронной техники [3, 16, 26];
– оценка показателей надежности элементов по справочным данным [3, 16];
– табулирование теоретических функций надежности [44];
– уточненный расчет надежности устройств [3, 7];
– анализ отказоустойчивости структуры системы [18, 19, 47, 48, 51, 52–57];
– ориентировочный априорный расчет надежности устройств [3, 6, 18, 19, 59];
– статистическое моделирование надежности систем [5, 8, 9–11];
– имитационное моделирование надежности систем [56, 58, 60];
– оценка показателей надежности по результатам испытаний [3, 23–27, 29, 34–42].
– оценка остаточной наработки систем [3].

Опция Готовность содержит следующие разделы:

– априорный расчет показателей готовности систем [3, 6, 62];
– оценка готовности систем методом имитационного моделирования [5, 8–11];
– методы повышения готовности систем;
– основные показатели готовности системы (рис. 2).

В качестве основных показателей готовности систем приняты следующие показатели: коэффициент готовности; коэффициент оперативной готовности и коэффициент технического использования.

Опция Живучесть содержит следующие разделы:

– априорный расчет показателей живучести систем [4];
– методы повышения живучести систем [4].

В качестве основных показателей живучести систем приняты следующие: коэффициент живучести, коэффициент деградации и параметр выживаемости системы.

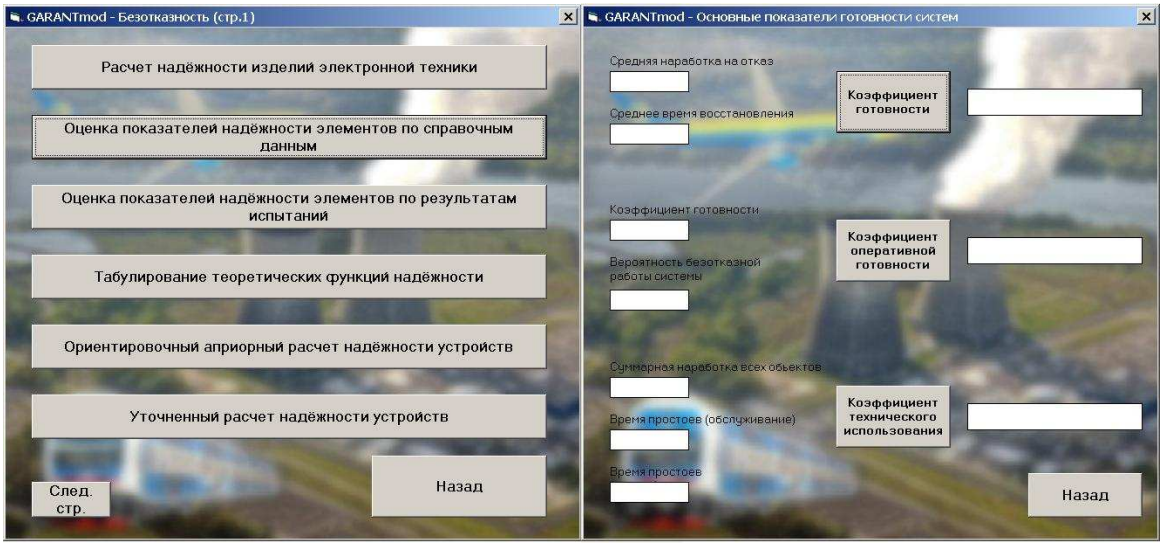

Рис. 2. Экранные формы опций Безотказность и Основные показатели готовности системы

Опция Конфиденциальность содержит следующие разделы:

– оценка показателей конфиденциальности систем;

– методы обеспечения конфиденциальности систем.

В качестве основных показателей конфиденциальности систем приняты следующие: вероятность угроз, уровень доступности и уровень секретности.

Опция Целостность содержит следующие разделы:

– оценка показателей целостности систем;

– методы обеспечения целостности систем.

В качестве основных показателей целостности систем приняты следующие: уровень целостности вычислительных ресурсов, уровень целостности программных ресурсов и уровень целостности информации.

Опция Функциональная безопасность содержит следующие разделы:

– оценка показателей функциональной безопасности систем;

– методы обеспечения функциональной безопасности систем.

В качестве основных показателей функциональной безопасности систем приняты следующие: вероятность безопасной работы, вероятность опасного отказа, средняя наработка до опасного отказа, параметр потока опасных отказов, средняя наработка на опасный отказ и коэффициент безопасности.

Опция Обслуживаемость содержит следующие разделы:

– оценка показателей обслуживаемости систем;

– методы обеспечения обслуживаемости систем.

В качестве основных показателей обслуживаемости систем приняты следующие: продолжительность технического обслуживания, трудоемкость технического обслуживания, стоимость технического обслуживания, среднее время восстановления и коэффициент технического использования**.**

Опция Помощь содержит следующие разделы:

– расширенная справочная система пакета;

– инструкция пользователя;

– инструкция программиста.

Опция Уровень гарантоспособности является финальным аккордом в процессе инжиниринга ГКС. Вводимое нами понятие, как уровень гарантоспособности системы, интересует нас, прежде всего, на этапе ее проектирования, когда сравниваются между собой различные варианты исполнения системы. Однако достигнутый уровень гарантоспособно-

сти можно оценивать и экспериментальным путем на этапе подконтрольной эксплуатации системы.

4. Выводы

Описанный пакет прикладных программ GARANTmod представляет собой эффективное программное средство, предназначенное для решения самых разнообразных задач, связанных с инжинирингом гарантоспособных компьютерных систем. Решение задач надежности и отказоустойчивости базируется на использовании более эффективного, по сравнению с экспоненциальным, двухпараметрического распределения отказов – *DN*-распределения, приводящего к более точным прогнозным оценкам количественных показателей надежности элементов, составных частей и систем в целом. В качестве интегральной характеристики систем используется параметр – уровень гарантоспособности системы, позволяющий объективно сравнивать между собой конкурирующие варианты исполнения системы и выбирать наиболее предпочтительный, с точки зрения гарантоспособности, вариант.

СПИСОК ЛИТЕРАТУРЫ

1. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie, B. Randell [et al.] // IEEE Trans. on Dependable and Secure Computing. – 2004. – Vol. 1, N 1. – P. 11 – 33.
2. ДСТУ 2863-94. Надійність техніки. Програма забезпечення надійності. Загальні вимоги. – Київ: Видавництво Держстандарту України, 1995. – 38 с.
3. Стрельников В.П. Оценка и прогнозирование надежности электронных элементов и систем / В.П. Стрельников, А.В. Федухин. – К.: Логос, 2002. – 486 с.
4. Сербін В.Г. Визначення і формалізація основних показників гарантоздатності живучих комп'ютерних систем керування на основі ймовірнісно-фізичного підходу для їх проектної оцінки і прогнозування / В.Г. Сербін, А.І. Сухомлин // Математичні машини і системи. – 2012. – № 4. – С. 182 – 189.
5. Сеспедес Гарсия Н.В. Статистическое моделирование надежности системы с последовательной структурой элементов / Н.В. Сеспедес Гарсия // Математические машины и системы. – 1999. – № 2. – С. 123 – 127.
6. Сеспедес Гарсия Н.В. Расчет показателей надежности персональных компьютеров / Н.В. Сеспедес Гарсия // Математические машины и системы. – 1998. – № 2. – С. 83 – 85.
7. Федухин А.В. Уточненный расчет надежности электронных устройств на основе DN-распределения / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2000. – № 2, 3. – С. 170 – 175.
8. Федухин А.В. К вопросу о статистическом моделировании надежности / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2006. – № 1. – С. 156 – 163.
9. Федухин А.В. Моделирование надежности восстанавливаемой системы с «холодным» резервом / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2007. – № 1. – С. 144 – 150.
10. Федухин А.В. Моделирование надежности восстанавливаемой системы с «холодным» резервом и ненадежным восстанавливающим органом / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2007. – № 2. – С. 125 – 131.
11. Федухин А.В. Моделирование надежности невосстанавливаемой системы со структурой типа «k из n» с реконфигурацией / А.В. Федухин, Н.В. Сеспедес Гарсия // Радіоелектронні і комп'ютерні системи. – 2009. – № 7 (41). – С. 82 – 84.
12. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. – Київ: Видавництво Держстандарту України, 1994. – 92 с.
13. ДСТУ 2861-94. Надійність техніки. Аналіз надійності. Основні положення. – Київ: Видавництво Держстандарту України, 1994. – 33 с.

14. ДСТУ 2862-94. Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги. – Київ: Видавництво Держстандарту України, 1995. – 40 с.
15. ДСТУ 2863-94. Надійність техніки. Програма забезпечення надійності. Загальні вимоги. – Київ: Видавництво Держстандарту України, 1995. – 38 с.
16. ДСТУ 2992-95. Вироби електронної техніки. Методи розрахунку надійності. – Київ: Видавництво Держстандарту України, 1995. – 42 с.
17. ДСТУ 3004-95. Надійність техніки. Методи оцінки показників надійності за експериментальними даними. – Київ: Видавництво Держстандарту України, 1995. – 123 с.
18. ДСТУ 3433-96. Надійність техніки. Моделі відмов. Основні положення. – Київ: Видавництво Держстандарту України, 1996. – 42 с.
19. ГОСТ 27.005-97. Надежность в технике. Модели отказов. Основные положення. – Київ: Видавництво Держстандарту України, 1997. – 45 с.
20. ДСТУ 3942-99. Надійність техніки. Плани контрольних випробувань для перевірки відповідності середнього наробітку до відмови (на відмову). – Ч. 2: Дифузійний розподіл. – Київ: Видавництво Держстандарту України, 1999. – 35 с.
21. ГОСТ 27.506-2000. Надежность в технике. Планы испытаний для контроля средней наработки до отказа (на отказ). – Ч. 2: Диффузионное распределение. – Київ: Видавництво Держстандарту України, 2000. – 32 с.
22. РД 50-690-89. Надежность в технике. Методические указания. Методы оценки показателей надежности по экспериментальным данным. – М.: Издательство стандартов, 1990. – 132 с.
23. Федухин А.В. Моделирование ресурса ИЭТ в различных температурных режимах эксплуатации: Сб. научн. тр. ИК имени В.М. Глушкова АН УССР «Моделирование и разработка интегральных структур» / А.В. Федухин. – Киев: Изд-во ИК, 1985. – С. 47 – 51.
24. Методические рекомендации по экспериментальной оценке показателей надежности ЭВМ / В.П. Стрельников, А.В. Федухин, Л.И. Бутенко [и др.]. – Киев: ИК имени В.М. Глушкова АН УССР, 1987. – 61 с.
25. Федухин А.В. Априорная оценка коэффициента форсирования скорости деградации: Сб. научн. тр. ИК имени В.М. Глушкова АН УССР «Проектирование элементов и узлов ЭВМ» / Федухин А.В. – Киев: Изд-во ИК, 1988. – С. 21 – 26.
26. Федухин А.В. Расчетно-экспериментальный метод оценки надежности ИЭТ по результатам форсированных испытаний / А.В. Федухин // Надежность и контроль качества. – 1989. – № 9. – С. 8 – 11.
27. Федухин А.В. Ускоренная оценка надежности изделий электронной техники / А.В. Федухин, Е.В. Бутенко // Математические машины и системы. – 1997. – № 2. – С. 84 – 93.
28. Стрельников В.П. Вероятностно-физический подход к расчету показателей надежности механических узлов средств вычислительной техники / В.П. Стрельников, А.В. Федухин, М.Ф. Яковлев // Математические машины и системы. – 1997. – № 2. – С. 101 – 113.
29. Федухин А.В. Ускоренная оценка надежности типовых функциональных блоков средств вычислительной техники / А.В. Федухин // Математические машины и системы. – 1998. – № 1. – С. 108 – 112.
30. Федухин А.В. Оценка влияния логической функции восстанавливающего органа на надежность резервированного дискретного устройств / А.В. Федухин // Математические машины и системы. – 1998. – № 2. – С. 74 – 79.
31. Федухин А.В. Оценка эффективности мультиустойчивых систем с учетом надежности их компонент / А.В. Федухин // Математические машины и системы. – 1999. – № 1. – С. 118 – 122.
32. Федухин А.В. Прогнозирование параметрической надежности полупроводниковых приборов с использованием диффузионного распределения наработки до отказа / А.В. Федухин // Математические машины и системы. – 1999. – № 2. – С. 117 – 122.
33. Стрельников В.П. Прогнозирование надежности слаботочного плоского разъемного соединения / В.П. Стрельников, А.В. Федухин, М.Ф. Яковлев // Математические машины и системы. – 1999. – № 3. – С. 69 – 79.
34. Федухин А.В. Ускоренная оценка надежности многослойных печатных плат / А.В. Федухин, М.Ф. Яковлев // Математичні машини і системи. – 2000. – № 1. – С. 101 – 110.
35. Федухин А.В. Методы ускоренной оценки надежности СВТ. Классификация, основные понятия и определения / А.В. Федухин // Математичні машини і системи. – 2001. – № 1, 2. – С. 194 – 204.

36. Федухин А.В. Контрольные испытания СВТ на надежность в форсированных режимах / А.В. Федухин // Математичні машини і системи. – 2002. – № 1. – С. 134 – 140.
37. Федухин А.В. Автомодельность форсированных испытаний на надежность / А.В. Федухин // Математичні машини і системи. – 2002. – № 2. – С. 184 – 192.
38. Федухин А.В. Ускоренные определительные испытания в форсированных режимах / А.В. Федухин // Математичні машини і системи. – 2002. – № 3. – С. 148 – 154.
39. Федухин А.В. К вопросу ускоренной оценки надежности технических средств информатики по результатам форсированных испытаний / А.В. Федухин // Управляющие системы и машины. – 2003. – № 1. – С. 18 – 24.
40. Федухин А.В. Ускоренная оценка надежности технических средств автоматизации производственных процессов / А.В. Федухин // Автоматизація виробничих процесів. – 2003. – № 2 (17). – С. 121 – 125.
41. Федухин А.В. Оценка коэффициента вариации по результатам испытаний в форсированном режиме / А.В. Федухин // Математичні машини і системи. – 2004. – № 2. – С. 196 – 199.
42. Федухин А.В. Прогнозирование надежности электронных устройств после длительного хранения / А.В. Федухин // Математичні машини і системи. – 2004. – № 4. – С. 164 – 170.
43. Федухин А.В. К вопросу о табулировании функций распределения отказов / А.В. Федухин // Математичні машини і системи. – 2006. – № 2. – С. 147 – 152.
44. Федухин А.В. Моделирование надежности восстанавливаемой резервированной системы с учетом тренда параметров надежности составных частей / А.В. Федухин // Математичні машини і системи. – 2007. – № 3, 4. – С. 239 – 244.
45. Федухин А.В. Моделирование надежности невосстанавливаемой нерезервированной системы с последовательной структурой элементов / А.В. Федухин // Математичні машини і системи. – 2008. – № 1. – С. 171 – 177.
46. Федухин А.В. Анализ эффективности смешанного резервирования невосстанавливаемых систем / А.В. Федухин // Математичні машини і системи. – 2008. – № 2. – С. 137 – 146.
47. Федухин А.В. Оценка эффективности избыточных систем по критерию средней продолжительности простоя / А.В. Федухин // Математичні машини і системи. – 2008. – № 3. – С. 153 – 156.
48. Федухин А.В. Моделирование надежности восстанавливаемой резервированной системы со структурой «k из n» / А.В. Федухин // Математичні машини і системи. – 2008. – № 4. – С. 189 – 193.
49. Федухин А.В. К вопросу об аппаратной реализации избыточных структур. Поэлементное резервирование / А.В. Федухин // Математичні машини і системи. – 2009. – № 4. – С. 193 – 199.
50. Федухин А.В. ПЛИС – системы как способ повышения отказоустойчивости информационно-управляющих комплексов / А.В. Федухин, Ар.А. Муха, А.А. Муха // Математичні машини і системи. – 2010. – № 1. – С. 198 – 204.
51. Федухин А.В. К вопросу об аппаратной реализации избыточных структур. Резервирование цифровых функциональных блоков / А.В. Федухин, Ар.А. Муха // Математичні машини і системи. – 2010. – № 2. – С. 138 – 143.
52. Федухин А.В. Моделирование систем железнодорожной автоматики и телемеханики / А.В. Федухин, А.М. Кашпуренко // Сб. наук. праць ДЕТУТ. – (Серія «Транспортні системи і технології»). – К.: РВЦ ДЕТУТ, 2010. – Вип. 16. – С. 186 – 189.
53. Федухин А.В. К вопросу об аппаратной реализации избыточных структур: резервированная двухканальная система с реконфигурацией / А.В. Федухин, Ар.А. Муха // Математичні машини і системи. – 2010. – № 4. – С. 156 – 159.
54. Федухин А.В. Классификация структур микропроцессорных информационно-управляющих систем / А.В. Федухин, В.А. Гладков, А.В. Гладков // Сб. науков. праць ДЕТУТ. – (Серія «Транспортні системи і технології»). – К.: РВЦ ДЕТУТ, 2010. – Вип. 17. – С. 231 – 237.
55. Федухин А.В. Имитационное моделирование отказоустойчивой резервированной двухканальной системы в интегрированной инструментальной среде Matlab Simulink / А.В. Федухин, Ар.А. Муха // Математичні машини і системи. – 2011. – № 2. – С. 178 – 181.
56. Федухин А.В. Новый подход к автоматизации переездов на железнодорожном транспорте / А.В. Федухин, А.В. Гладков, Ар.А. Муха // Математичні машини і системи. – 2011. – № 3. – С. 135 – 141.
57. Федухин А.В. Моделирование надежности систем средствами пакета программ RELIABmod / А.В. Федухин, В.П. Пасько // Математичні машини і системи. – 2011. – № 4. – С. 176 – 182.

58. Федухин А.В. К вопросу о количественных характеристиках безотказности избыточных компьютерных систем / А.В. Федухин, В.П. Пасько // Математичні машини і системи. – 2012. – № 1. – С. 145 – 156.
59. Федухин А.В. Моделирование надежности систем / А.В. Федухин, В.П. Пасько // Методы менеджмента качества. – 2012. – № 3. – С. 50 – 55.
60. Федухин А.В. Графо-аналитический метод оценки параметров DN-распределения в условиях малой статистики отказов / А.В. Федухин, Н.В. Сеспедес Гарсия // Математичні машини і системи. – 2012. – № 2. – С. 161 – 167.
61. Системы радиоуправления стрелками и сигналами на промышленном железнодорожном транспорте / А.В. Федухин, В.В. Федоровский, А.И. Сухомлин [и др.] // Математичні машини і системи. – 2012. – № 4. – С. 75 – 83.
62. Федухин А.В. Радиомикропроцессорная система автоматической переездной сигнализации на железнодорожном транспорте / А.В. Федухин // Математичні машини і системи. – 2013. – № 1. – С. 157 – 162.

Стаття надійшла до редакції 08.07.2013