

GUIDELINES FOR PUBLICATION IN THE JOURNAL «DEPENDABILITY»

■ STRUCTURAL RELIABILITY THE THEORY AND PRACTICE

- Methods of calculation, technologies and methods of modeling, packages of applied programs, practical calculations of reliability of complex systems.
- The mathematical theory of maintenance service, practical results of complex system operations, life cycle of systems, optimization of reliability and costs at all stages of life cycle.
- Test methods, criteria of decision-making by test results, accelerated tests, methods of reliability assessment of systems by test results, practical experience of reliability tests.

■ FUNCTIONAL RELIABILITY THE THEORY AND PRACTICE

- Object, subject and purposes of research, parameters of functional reliability, terminology, principles and calculation methods.
- Methods of assessment and forecasting of software reliability, methods of calculation of information processes reliability performance in software-hardware complexes taking into account faulty program errors, errors of operators, errors of input information.
- Technologies and methods of ensuring functional reliability – technologies of functionally reliable software development, methods of construction of algorithms of information processing and management tolerant to faulty errors and to errors of operators and methods and ways of error protection in input information, practical results.

■ FUNCTIONAL SAFETY OF SYSTEM THE THEORY AND PRACTICE

- Object, subject and the purposes of research, parameters of functional safety; functions of safety, completeness of safety, terminology in the field of functional safety.
- Risks, postulates and principles of safety, residual risks, methods of an estimation of risks, the proof of safety. Practical results of ranging of dangers and estimations of risks.
- Mathematical methods and models of the task of requirements to completeness of safety and admissible time of detection of dangerous refusal, model of functional safety of multichannel and multilevel systems.
- Technologies for ensuring functional safety of systems at all stages of life cycle.

■ FAULT TOLERANCE OF SYSTEMS THE THEORY AND PRACTICE

- Methods of passive protection against failures, mathematical models of structural redundancy, gradual degradation of redundant systems, fault masking, practical results of application of passive protection against failures.
- Methods of active protection against structural failures and errors in performance of information processes, principles and methods of active protection, theoretical bases of active protection, technical decisions, estimations of active protection efficiency.

■ CERTIFICATION THE THEORY AND PRACTICE

- Accreditation of certification bodies and test laboratories – a problem state in Russia and abroad. How to achieve mutual recognition of test results in Russia and abroad? Methods of certification of software – hardware complexes under requirements of international standards on functional safety.
- Obligatory and voluntary certifications – experience, opinions, offers.
- Certification in the field of quality and reliability of systems – requirements of standards, techniques of tests, practical results.
- Certification of functional safety of systems on the basis of V-technology – philosophy, certification methods, practical results of selective deep checks of a developer evidentiary base.

■ STANDARDIZATION IN THE FIELD OF RELIABILITY AND FUNCTIONAL SAFETY

- Influence of the law «Of technical regulation» on development of the theory and practice of reliability and functional safety.
- RAMS standards (IEC 62278, EN 50126, etc.) and their reflection in standards of GOST R, development of the standard GOST 27.002-89 in view of terms and definitions of RAMS standards.
- States and prospects of standardization in the field of reliability.
- Main principles and basic regulations of standards on functional safety GOST R/МЭК 61508, IEC 61511, EN 50126, IEC 62278, IEC 62280, EN 50128, IEC 62279, EN 50129, EN 50159 (1.2), etc.
- Condition and prospects of standardization in the field of functional safety.

ISSN 1729-2646

НАДЕЖНОСТЬ

DEPENDABILITY

04 | 2014
(51)

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ / SCIENTIFIC- TECHNICAL JOURNAL

В HOMEPE / IN THIS RELEASE:

- КАК НАМ ОПРЕДЕЛИТЬ ЧТО ТАКОЕ «НАДЕЖНОСТЬ»
HOW WE SHOULD DEFINE WHAT "DEPENDABILITY" IS
- О ПОКАЗАТЕЛЯХ НАДЕЖНОСТИ ТИПА СРЕДНЯЯ НАРАБОТКА
DEPENDABILITY INDICES OF MEAN TIME TYPE
- АНАЛИЗ ПРОЕКТНОЙ НАДЕЖНОСТИ ОТВЕТСТВЕННЫХ УЗЛОВ АРОЧНОГО ПРОЛЕТНОГО СТРОЕНИЯ ПЕШЕХОДНОГО ПУТЕПРОВОДА НА ОСНОВЕ ЧИСЛЕННЫХ И ИМИТАЦИОННЫХ МЕТОДОВ
ANALYSIS OF DESIGN DEPENDABILITY OF CRITICAL UNITS OF ARCH SPANS OF PEDESTRIAN OVERPASSES BASED ON NUMERICAL AND SIMULATION METHODS
- МЕТОД УСТРАНЕНИЯ ВЗАИМНОГО ПЕРЕСЕЧЕНИЯ ОЦЕНОК ЭЗАРИ-ПРОШАНА В ЗАДАЧАХ АНАЛИЗА СВЯЗНОСТИ ДВУХПОЛЮСНЫХ СЕТЕЙ
METHOD FOR ELIMINATION OF MUTUAL CROSSING OF ESARY-PROSCHAN ESTIMATES IN TASKS OF ANALYSIS OF BIPOLAR NETWORKS CONNECTIVITY
- ПРИМЕНЕНИЕ ТАКТИКИ ПОСЛЕДОВАТЕЛЬНЫХ КОНТРОЛЬНЫХ ИСПЫТАНИЙ НА НАДЕЖНОСТЬ ЭЛЕМЕНТОВ АСУ ТП И АВТОМАТИЧЕСКОЙ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ В УСЛОВИЯХ ЭКСПЛУАТАЦИИ ДЛЯ ЕЕ УЧЕТА ПРИ FMEA-АНАЛИЗЕ
APPLICATION OF THE TACTICS OF DEPENDABILITY CONSECUTIVE CHECK TESTS OF CAM ELEMENTS AND AUTOMATED SIS UNDER OPERATING CONDITIONS FOR USE OF RESULTS IN FMEA ANALYSIS
- МЕТОДЫ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ ПРОГРАММ
METHODS OF SOFTWARE FUNCTIONAL DEPENDABILITY ASSURANCE
- ГЕНЕТИЧЕСКИЙ АЛГОРИТМ ДЛЯ ОПТИМИЗАЦИИ АРХИТЕКТУРЫ БОРТОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
GENETIC ALGORITHM FOR OPTIMIZATION OF ONBOARD SOFTWARE ARCHITECTURE
- ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЙ ПРИ СОЗДАНИИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ И ЗАДАЧА ВЫБОРА АЛЬТЕРНАТИВ
PROCESS OF DECISION-MAKING IN DEVELOPMENT OF COMPLEX TECHNICAL SYSTEMS AND THE TASK OF CHOICE OF ALTERNATIVES

THE JOURNAL IS PUBLISHED WITH PARTICIPATION AND SUPPORT
OF JOINT-STOCK COMPANY RESEARCH & DESIGN INSTITUTE
FOR INFORMATION TECHNOLOGY, SIGNALLING AND TELECOMMUNICATIONS
ON RAILWAY TRANSPORT (JSC NIIAS)



JSC NIIAS is RZD's leading company in the field of development of train control and safety systems, traffic management systems, GIS support technology, railway fleet and infrastructure monitoring systems



Mission:

transportation

- ☐ efficiency,
- ☐ safety,
- ☐ reliability



Key areas of activity

- Intellectual control and management systems
- Transportation management systems and transport service technology
- Signalling and remote control systems
- Automated transportation management centers
- Railway transport information systems
- Geoinformation systems and satellite technology
- Transport safety systems
- Infrastructure management systems
- Power consumption and energy management systems
- Testing, certification and expert assessment
- Information security
- Regulatory support



www.vniias.ru

**ОСНОВНЫЕ НАПРАВЛЕНИЯ
ПУБЛИКАЦИЙ В ЖУРНАЛЕ «НАДЕЖНОСТЬ»**

**■ СТРУКТУРНАЯ НАДЕЖНОСТЬ
ТЕОРИЯ И ПРАКТИКА**

- Методы расчета, технологии и методы моделирования, пакеты прикладных программ, практические расчеты надежности сложных систем.
- Математическая теория технического обслуживания, практические результаты эксплуатации сложных систем, жизненный цикл систем, оптимизация надежности и стоимости на всех этапах жизненного цикла.
- Методы испытаний, критерии принятия решений по результатам испытаний, ускоренные испытания, методы оценки надежности систем по результатам испытаний, практический опыт испытаний на надежность.

**■ ФУНКЦИОНАЛЬНАЯ НАДЕЖНОСТЬ
ТЕОРИЯ И ПРАКТИКА**

- Объект, предмет и цели исследования, показатели функциональной надежности, терминология, принципы и методы расчета.
- Методы оценки и прогнозирования надежности программного обеспечения, методы расчета надежности выполнения информационных процессов в программно – аппаратных комплексах с учетом сбойных, программных ошибок, ошибок операторов, ошибок во входной информации.
- Технологии и методы обеспечения функциональной надежности – технологии построения функционально надежного программного обеспечения, методы построения нечувствительных к сбойным ошибкам и ошибкам операторов алгоритмов обработки информации и управления, методы и способы защиты от ошибок во входной информации, практические результаты.

**■ ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ
ТЕОРИЯ И ПРАКТИКА**

- Объект, предмет и цели исследования, показатели функциональной безопасности; функции безопасности, полнота безопасности, терминология в области функциональной безопасности.
- Риски, постулаты и принципы безопасности, остаточные риски, методы оценки рисков, доказательство безопасности. Практические результаты ранжирования опасностей и оценки рисков.
- Математические методы и модели задания требований к полноте безопасности и допустимому времени обнаружения опасного отказа, модели функциональной безопасности многоканальных и многоуровневых систем.
- Технологии обеспечения функциональной безопасности систем на всех этапах жизненного цикла.

**■ ОТКАЗОУСТОЙЧИВОСТЬ СИСТЕМ
ТЕОРИЯ И ПРАКТИКА**

- Методы пассивной защиты от отказов, математические модели структурного резервирования, постепенной деградации избыточных систем, маскирования неисправностей, практические результаты применения пассивной защиты от отказов.
- Методы активной защиты от структурных отказов и ошибок в выполнении информационных процессов, принципы и способы активной защиты, теоретические основы активной защиты, технические решения, оценки эффективности активной защиты.

**■ СЕРТИФИКАЦИЯ
ТЕОРИЯ И ПРАКТИКА**

- Аккредитация органов по сертификации и испытательных лабораторий – состояние проблемы в России и за рубежом. Как добиться взаимопризнания результатов испытаний в России и за рубежом? Пути сертификации программно – аппаратных комплексов по требованиям международных стандартов по функциональной безопасности.
- Обязательная и добровольная сертификации – опыт, мнения, предложения.
- Сертификация в области качества и надежности систем – требования стандартов, методики испытаний, практические результаты.
- Сертификация функциональной безопасности систем на основе V-технологии – философия, способы сертификации, практические результаты выборочных глубоких проверок доказательственной базы разработчика.

**■ СТАНДАРТИЗАЦИЯ В ОБЛАСТИ НАДЕЖНОСТИ
И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ**

- Влияние закона «О техническом регулировании» на развитие теории и практики надежности и функциональной безопасности.
- Стандарты RAMS (IEC 62278, EN 50126 и др.) и их отражение в стандартах ГОСТ Р, развитие стандарта ГОСТ 27.002-89 с учетом терминов и определений стандартов RAMS.
- Состояние и перспективы стандартизации в области надежности.
- Основные принципы и базовые положения стандартов по функциональной безопасности ГОСТ Р /МЭК 61508, IEC 61511, EN 50126, IEC 62278, IEC 62280, EN 50128, IEC 62279, EN 50129, EN 50159 (1.2) и др.
- Состояние и перспективы стандартизации в области функциональной безопасности.

УЧРЕДИТЕЛЬ ЖУРНАЛА:

ООО «Журнал «Надежность».

Зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Регистрационное свидетельство ПИ № 77-9782 от 11 сентября 2001 года.

Официальный печатный орган Российской академии надежности

Оформить подписку можно по каталогу «Пресса России» агентства «Книга-Сервис» 11804 – полугодовой индекс.

Главный редактор

Шубинский И.Б., д.т.н., проф.

Редколлегия

Бочков А.В., к.т.н.

Дзиркал Э.В., к.т.н.

Замышляев А.М., д.т.н.

Каштанов В.А., д.ф.-м.н., проф.

Кофанов Ю.Н., д.т.н., проф.

Лецкий Э.К., д.т.н., проф.

Нетес В.А., д.т.н., проф.

Розенберг И.Н., д.т.н., проф.

Стась К.Н., к.т.н.

Тарасов А.А., д.т.н., проф.

Уткин Л.В., д.т.н., проф.

Ушаков И.А., д.т.н., проф.

Черкесов Г.Н., д.т.н., проф.

Шебе Х., д.ф.-м.н.

Щербаков О.В., д.т.н., проф.

Юркевич Е.В., д.т.н., проф.

Выпускающий редактор

Патрикеева Е.В.

Издатель журнала

ООО «Журнал «Надежность»

Директор

Калинина И.В.

Адрес: 109029, г. Москва,
ул. Нижегородская, д. 27, стр. 1, оф. 209
ООО «Журнал «Надежность»
www.dependability.pro

Верстка

Куртиш Б.С.

Отпечатано в ОАО «Областная типография «Печатный двор».
432049, г. Ульяновск, ул. Пушкарева, 27.
Тираж 500 экз. Заказ

Статьи рецензируются.

Статьи опубликованы в авторской редакции. Мнение членов редакционного совета может не совпадать с точкой зрения авторов публикаций. Перепечатка материалов допускается только с письменного разрешения редакции. Рукописи не возвращаются.

**ЖУРНАЛ ВКЛЮЧЕН В ПЕРЕЧЕНЬ
ВЕДУЩИХ ЖУРНАЛОВ И ИЗДАНИЙ
ВЫСШЕЙ АТТЕСТАЦИОННОЙ
КОМИССИИ (ВАК)**

ISSN 1729-2646

**THE JOURNAL IS INCLUDED IN THE LIST
OF THE LEADING JOURNALS AND EDITIONS
OF THE HIGHER ATTESTATION COMMISSION (VAK)**

**ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ ОТКРЫТОГО
АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
И ПРОЕКТНО-КОНСТРУКТОРСКИЙ ИНСТИТУТ ИНФОРМАТИЗАЦИИ,
АВТОМАТИЗАЦИИ И СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ»
(ОАО «НИИАС»)
И ООО «ИЗДАТЕЛЬСКИЙ ДОМ «ТЕХНОЛОГИИ»**

**THE JOURNAL IS PUBLISHED WITH THE PARTICIPATION
AND SUPPORT OF THE JOINT-STOCK COMPANY «RESEARCH
AND DESIGN INSTITUTE OF INFORMATISATION, AUTOMATION
AND COMMUNICATION ON RAILWAY TRANSPORT»
(JSC «NIIAS») AND LLC PUBLISHING HOUSE «TECHNOLOGY»**

THE JOURNAL PROMOTER:

“Journal “Reliability” Ltd

It is registered in the Russian Ministry of Press, Broadcasting and Mass Communications. Registration certificate ПИ 77-9782, September, 11, 2001.

Official organ of the Russian Academy of Reliability

Subscription is possible under the catalogue “Press of Russia” of the agency “Book-service” 11804 – a semi-annual index.

Editor-in-chief

I. Shubinsky, Dr. Sci., prof.

Editorial board

A. Bochkov, PhD.

E. Dzirkal, PhD.

V. Kashtanov, Dr. of physical-mathematical science, prof.

J. Kofanov, Dr. Sci., prof.

E. Letsky, Dr. Sci., prof.

V. Netes, Dr. Sci., prof.

I. Rozenberg, Dr. Sci., prof.

K. Stas, Ph. D.

F. Tarasov, Dr. Sci., prof.

L. Utkin, Dr. Sci., prof.

I. Ushakov, Dr. Sci., prof.

G. Cherkesov, Dr. Sci., prof.

H. Schaebe, Dr. of physical and math. science, prof.

O. Shcherbakov, Dr. Sci., prof.

E. Jurkevich, Dr. Sci., prof.

A. Zamyshlaev, Dr. Sci.

Commissioning editor

E. Patrikeeva

Publisher of the journal

LLC Journal “Dependability”

Director

I. Kalinina

The address:

109029, Moscow,

Str. Nizhegorodskaya, 27,

Building 1, 1, office 209

Ltd Journal “Dependability”

www.dependability.pro

Make-up

B. Kurtish

Printed by JSC “Regional printing house, Printing place” 432049, Ulyanovsk, Pushkarev str., 27. Circulation: 500 copies.

Printing order

Papers are reviewed.

Papers are published in author's edition. The opinion of members of the editorial board may not coincide with the point of view of authors' publications. The reprint of materials is granted only with the written permission of the editorial board. Manuscripts are not returned.

СОДЕРЖАНИЕ/CONTENTS

Структурная надежность. Теория и практика / Structural reliability. The theory and practice

КАК НАМ ОПРЕДЕЛИТЬ ЧТО ТАКОЕ «НАДЕЖНОСТЬ» <i>Нетес В.А., Тарасьев Ю.И., Шпер В.Л.</i>	3
HOW WE SHOULD DEFINE WHAT “DEPENDABILITY” IS <i>Netes V.A., Tarasyev J.I., Shper V.L.</i>	15
О ПОКАЗАТЕЛЯХ НАДЕЖНОСТИ ТИПА СРЕДНЯЯ НАРАБОТКА <i>Викторова В.С., Степанянц А.С.</i>	27
DEPENDABILITY INDICES OF MEAN TIME TYPE <i>Viktorova V.S., Stepanyants A.S.</i>	37
АНАЛИЗ ПРОЕКТНОЙ НАДЕЖНОСТИ ОТВЕТСТВЕННЫХ УЗЛОВ АРОЧНОГО ПРОЛЕТНОГО СТРОЕНИЯ ПЕШЕХОДНОГО ПУТЕПРОВОДА НА ОСНОВЕ ЧИСЛЕННЫХ И ИМИТАЦИОННЫХ МЕТОДОВ <i>Майстренко И.Ю., Юсупов И.И., Зиннуров Т.А.</i>	47
ANALYSIS OF DESIGN DEPENDABILITY OF CRITICAL UNITS OF ARCH SPANS OF PEDESTRIAN OVERPASSES BASED ON NUMERICAL AND SIMULATION METHODS <i>Maystrenko I.Y., Zinnurov T.A., Yusupov I.I.</i>	54
МЕТОД УСТРАНЕНИЯ ВЗАИМНОГО ПЕРЕСЕЧЕНИЯ ОЦЕНОК ЭЗАРИ-ПРОШАНА В ЗАДАЧАХ АНАЛИЗА СВЯЗНОСТИ ДВУХПОЛЮСНЫХ СЕТЕЙ <i>Носов М.В.</i>	61
METHOD FOR ELIMINATION OF MUTUAL CROSSING OF ESARY-PROSCHAN ESTIMATES IN TASKS OF ANALYSIS OF BIPOLAR NETWORKS CONNECTIVITY <i>Nosov M.B.</i>	70
ПРИМЕНЕНИЕ ТАКТИКИ ПОСЛЕДОВАТЕЛЬНЫХ КОНТРОЛЬНЫХ ИСПЫТАНИЙ НА НАДЕЖНОСТЬ ЭЛЕМЕНТОВ АСУ ТП И АВТОМАТИЧЕСКОЙ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ В УСЛОВИЯХ ЭКСПЛУАТАЦИИ ДЛЯ ЕЕ УЧЕТА ПРИ FMEA-АНАЛИЗЕ <i>Пегушин С.Л., Шумихин А.Г.</i>	78
APPLICATION OF THE TACTICS OF DEPENDABILITY CONSECUTIVE CHECK TESTS OF CAM ELEMENTS AND AUTOMATED SIS UNDER OPERATING CONDITIONS FOR USE OF RESULTS IN FMEA ANALYSIS <i>Pegushin S.L., Shumikhin A.G.</i>	83

Функциональная надежность. Теория и практика / Functional reliability. The theory and practice

МЕТОДЫ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ ПРОГРАММ <i>Шубинский И.Б.</i>	87
METHODS OF SOFTWARE FUNCTIONAL DEPENDABILITY ASSURANCE <i>Shubinsky I.B.</i>	95
ГЕНЕТИЧЕСКИЙ АЛГОРИТМ ДЛЯ ОПТИМИЗАЦИИ АРХИТЕКТУРЫ БОРТОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ <i>Терсков В.А., Шеенок Д.А., Карцан И.Н.</i>	102
GENETIC ALGORITHM FOR OPTIMIZATION OF ONBOARD SOFTWARE ARCHITECTURE <i>Terskov V.A., Sheenok D.A., Kartsan I.N.</i>	112

Функциональная безопасность. Теория и практика / Functional safety. The theory and practice

ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЙ ПРИ СОЗДАНИИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ И ЗАДАЧА ВЫБОРА АЛЬТЕРНАТИВ <i>Семенов С.С., Полтавский А.В., Маклаков В.В.</i>	122
PROCESS OF DECISION-MAKING IN DEVELOPMENT OF COMPLEX TECHNICAL SYSTEMS AND THE TASK OF CHOICE OF ALTERNATIVES <i>Semenov S.S., Poltavsky A.V., Maklakov V.V.</i>	131
НЕКРОЛОГ	139
OBITUARY	141
КНИГА И.Б.ШУБИНСКОГО «СТРУКТУРНАЯ НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»	143
BOOK BY SHUBINSKY I.B. STRUCTURAL RELIABILITY OF INFORMATION SYSTEMS	143
КНИГА И.Б.ШУБИНСКОГО «ФУНКЦИОНАЛЬНАЯ НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»	144
BOOK BY SHUBINSKY I.B. FUNCTIONAL RELIABILITY OF INFORMATION SYSTEMS	144
ГНЕДЕНКО-ФОРУМ	145
GNEDENKO FORUM	146



Нетес В.А., Тарасьев Ю.И., Шпер В.Л.

КАК НАМ ОПРЕДЕЛИТЬ ЧТО ТАКОЕ «НАДЕЖНОСТЬ»

В настоящее время в Техническом комитете по стандартизации «Надежность в технике» (ТК 119) идет работа по созданию нового межгосударственного стандарта «Надёжность в технике. Термины и определения» взамен ГОСТ 27.002–89. Эта тема уже поднималась на страницах нашего журнала. В № 2 за этот год был опубликован отчет о заседании постоянно действующего научного семинара «Надёжность и качество функционирования систем», состоявшемся 30 января 2014 года, на котором обсуждались основные проблемы, связанные с разработкой этого стандарта. В том же номере была опубликована статья активных участников этой работы В.А. Нетеса, Ю.И. Тарасьева и В.Л. Шпера «Актуальные вопросы стандартизации терминологии в области надёжности», в которой было начато более детальное рассмотрение этой важной темы.

Сейчас мы публикуем статью этих же авторов, продолжающую обсуждение проблем терминологии в области надежности.

Редакция обращается ко всем заинтересованным читателям с просьбой высказать свое мнение по поднятым в этих статьях вопросам. Свои письма можно направлять в редакцию или непосредственно в ТК 119.

Когда я использую слово, оно значит именно то, что я хочу, чтоб оно значило – ни больше, ни меньше, – сказал Шалтай-Болтай Алисе.

Льюис Кэрролл «Алиса в зазеркалье»

1. Введение

В статье [1] мы кратко рассказали историю отмены стандарта ГОСТ Р 27.002–2009 [2] и возврата к ГОСТ 27.002–89 [3] – стандарту 25-летней давности, а также о начале работы над новой редакцией основополагающего терминологического стандарта и трудностях, с которыми столкнулась рабочая группа (РГ), взявшаяся за эту работу. Там же отмечалось, что одна из главных проблем – это вопрос о том, какое определение базового термина «надежность» положить в основу нового стандарта: старое из ГОСТ 27.002–89 или новое из подготовленного МЭК (IEC) международного стандарта (МС) [4] (его публикация ожидается в августе 2014 г.). В данной статье мы попытаемся изложить суть возникших среди членов РГ разногласий и причины, по которым мы считаем этот вопрос принципиально важным.

Но прежде, чем перейти к дискуссии, мы считаем целесообразным кратко напомнить читателям, как определялся термин «надежность» во всех предыдущих отечественных терминологических стандартах, и как он определяется в международных документах, в том числе и в последней редакции МС МЭК.

2. Определение термина «надежность» в стандартах советского периода

В табл. 1 приведены как сами определения основного термина в старых документах, начиная со Сборника рекомендуемых терминов АН СССР, выпущенного в 1962 году, так и примечания и пояснения к этому термину. Определения мы привели полностью, а пояснения и примечания даны в той части, которая связана с последующей дискуссией.

Таблица 1. Определения термина «надежность» в советских документах

№ п/п	Источник	Определение	Примечание к определению
1	Сборник рекомендуемых терминов. Вып. 60. 1962 [5]	Свойство системы (элемента системы), обусловленное главным образом её безотказностью и ремонтпригодностью и обеспечивающее выполнение задания в установленном для системы (элемента) объёме; количественно определяется вероятностными характеристиками и параметрами	
2	Сборник рекомендуемых терминов. Вып. 67. 1964 [6]	Свойство системы или изделия, обусловленное их безотказностью, долговечностью и ремонтпригодностью и обеспечивающее нормальное выполнение заданных функций системы (изделия); количественно оценивается, например, произведением вероятности безотказной работы на коэффициент технического использования (или на коэффициент готовности)	
3	ГОСТ 13377–67 [7]	Свойство изделия выполнять заданные функции, сохраняя свои эксплуатационные показатели в заданных пределах в течение требуемого промежутка времени или требуемой наработки	Надежность изделия обуславливается его «безотказностью», «ремонтпригодностью», «сохраняемостью», а также «долговечностью» его частей
4	ГОСТ 13377–75 [8]	Свойство объекта выполнять заданные функции, сохраняя во времени значения установленных эксплуатационных показателей в заданных пределах, соответствующих заданным режимам и условиям использования, технического обслуживания, ремонтов, хранения и транспортирования	Надежность является комплексным свойством, которое в зависимости от назначения объекта и условий его эксплуатации может включать безотказность, долговечность, ремонтпригодность и сохраняемость в отдельности или определенное сочетание этих свойств как для объекта, так и для его частей «Эксплуатационные показатели» – показатели производительности, скорости, расхода электроэнергии, топлива и т.п. <i>Из пояснения к термину:</i> «Под качеством продукции понимается совокупность её свойств, обуславливающая пригодность продукции для удовлетворения определенных потребностей в соответствии с её назначением. Одним из свойств этой совокупности является надежность»
5	ГОСТ 27.002–83 [9]	Свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортирования	Надежность является сложным свойством, которое в зависимости от назначения объекта и условий его применения состоит из сочетаний свойств: безотказности, долговечности, ремонтпригодности и сохраняемости

6	ГОСТ 27.002–89 [3]	Свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования	Надежность является комплексным свойством, которое в зависимости от назначения объекта и условий его применения может включать безотказность, долговечность, ремонтпригодность и сохраняемость или определенные сочетания этих свойств <i>Из пояснения к термину:</i> Терминология по надежности распространяется на любые технические объекты – изделия, сооружения и системы, а также их подсистемы. . . В качестве подсистем могут рассматриваться сборочные единицы, детали, компоненты или элементы. При необходимости в понятие «объект» могут быть включены информация и её носители, а также человеческий фактор (например, при рассмотрении надежности системы «машина-оператор»). ... Границ понятия «надежность» не изменяет следующее определение: надежность – Свойство объекта сохранять во времени способность к выполнению требуемых функций в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования. Это определение применяют тогда, когда параметрическое описание нецелесообразно (например, для простейших объектов, работоспособность которых характеризуется по типу «да-нет»), или невозможно (например, для систем «машина-оператор», т.е. таких систем, не все свойства которых могут быть охарактеризованы количественно). К параметрам, характеризующим способность выполнять требуемые функции, относят кинематические и динамические параметры, показатели конструкционной прочности, показатели точности функционирования, производительности, скорости и т.п.
---	--------------------	--	--

Из табл. 1 видно, что определение надежности изменялось с принятием каждого нового документа. В результате имеем следующую последовательность трансформаций определения надежности (мы упрощаем формулировки, оставляя смысл):

1962 год – свойство системы выполнять задание;

1964 год – свойство системы (изделия) выполнять заданные функции;

1967 год (первый ГОСТ) – свойство изделия выполнять заданные функции, сохраняя свои показатели в заданных пределах;

1975 год – свойство объекта выполнять заданные функции, сохраняя установленные показатели в заданных пределах;

1983, 1989 гг. – свойство объекта сохранять в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции;

1989 год (приложение) – свойство объекта сохранять способность выполнять требуемые функции.

Таким образом, в ГОСТ, начиная с 1983 года, способность выполнять заданные функции, стала трактоваться как сохранение в заданных пределах всех установленных в нормативно-технической

и (или) конструкторской (проектной) документации параметров. В целях краткости мы далее называем такое определение параметрическим.

Отметим, что в ныне действующем ГОСТ 27.002–89 есть фактически два определения надежности: в основном тексте стандарта и в справочном приложении, содержащем пояснения к терминам (табл. 1, п. 6). При этом указано, что второе определение не изменяет границ понятия «надежность» и его «применяют тогда, когда параметрическое описание нецелесообразно ... или невозможно ...».

В связи с этим, представляется целесообразным обсудить вопрос о том, какое определение стоит иметь как основное, а какое можно оставить в качестве вспомогательного. Мы вернемся к этому вопросу позже, а пока продолжим исторический обзор.

3. Определение термина надежность в международных стандартах и отечественных стандартах, основанных на международных

Вплоть до 1984 года в МС не было общего термина, эквивалентного русскому «надежность». Были лишь термины для отдельных более узких свойств: безотказности (reliability), готовности (availability) и др. В частности, Технический комитет (ТК) 56 МЭК, называемый сейчас «Надежность» (Dependability), назывался «Безотказность и ремонтпригодность» (Reliability and Maintainability). Возникали и более длинные словосочетания, например, Reliability, Availability, Maintainability and Safety (безотказность, готовность, ремонтпригодность и безопасность) – концепция, широко используемая, в частности, на железнодорожном транспорте, для которой обычно применяется аббревиатура RAMS.

Правда, еще в 1960 году американский исследователь Дж. Хосфорд ввел термин dependability и соответствующие показатели [10]. В общем случае они определялись как вероятность того, что система будет способна функционировать, когда это требуется. Он писал, что это одна из важнейших характеристик любых систем, в которых могут происходить отказы. В частных случаях эти показатели были коэффициентами готовности (мгновенным или усредненным интервальным) и вероятностью безотказной работы.

С конца 1970-х годов Ж.-К. Лапри из Департамента информационных и инженерных наук Французского национального центра научных исследований в Тулузе стал применять термин dependability для вычислительных систем [11, 12 и др.]. Он трактовался довольно широко и применительно к этой области стал переводиться на русский язык как «гарантоспособность» [13]. Это понятие определялось как свойство системы, позволяющее обоснованно полагаться на выполнение услуг, для которых она предназначена.

В 1984 году Международный консультативный комитет по телефонии и телеграфии (МККТТ) при Международном союзе электросвязи (МСЭ) принял Рекомендацию G.106 [14], содержащую термины и определения в области качества обслуживания и надежности, в которой появился общий термин «надежность» (dependability). Введенные в ней понятия вскоре стали активно использоваться специалистами отрасли, в том числе и в нашей стране [15].

Таким образом, расширение понятия «надежность» произошло по инициативе наиболее передовых и динамично развивающихся отраслей: вычислительной техники и электросвязи.

Затем термин dependability вошел в принятый в 1990 году МС МЭК 50-191, который МЭК разработал совместно с МСЭ. Впоследствии в связи с изменением системы обозначений МС он получил номер 60050-191. Поскольку все остальные ТК ИСО и МЭК признают ведущую роль МЭК/ТК 56 в вопросах надежности, этот стандарт является «горизонтальным» (межотраслевым, общетехническим), и определенные в нем термины используются во всех МС ИСО и МЭК, в которых упоминается надежность. Это обеспечивает согласованность всех МС в трактовке основных по-

ятий надежности. В этом плане они, как это будет видно из дальнейшего, отличаются в лучшую сторону от отечественных стандартов.

В табл. 2 приведены варианты перевода на русский язык определения термина “надежность” и примечания к нему из официальных документов: русских версий Рекомендации G.106 [14] и МС МЭК 50-191 [16], российских стандартов [17, 18] и межгосударственного стандарта [19].

Таблица 2. Переводы определения надежности из международных документов в отечественных документах

№ п/п	Источник	Определение	Примечание к определению
1	Рекомендация МККТТ G.106 [14]	Собирательный термин, используемый для характеристик готовности и факторов, ее обуславливающих: безотказности, ремонтнопригодности и обеспеченности объекта техническим обслуживанием	Данный термин используется только для общих описаний без количественных выражений
2	МС МЭК 50-191 [16]	Собирательный термин, применяемый для описания свойства готовности и влияющих на него свойств безотказности, ремонтнопригодности и обеспеченности технического обслуживания и ремонта	Данный термин применяется только для общего не количественного описания свойства готовности
3	ГОСТ ISO 9000–2011 [19]	То же	Термин «надежность» применяется только для общего не количественного описания свойства
4	ГОСТ Р 51901.3–2007 (МЭК 60300-2:2004) [17]	Свойство готовности и влияющие на него свойства безотказности, ремонтнопригодности и обеспеченности техническим обслуживанием и ремонтом	Данный термин применяется только для общего не количественного описания свойства готовности
5	ГОСТ Р 27.002–2009 [18]	Свойство готовности и влияющие на него свойства безотказности и ремонтнопригодности, и поддержка технического обслуживания	Данный термин используют только для общего не количественного описания надежности

По сравнению с отечественными стандартами в МС добавлена еще одна составляющая надежности: обеспеченность технического обслуживания и ремонта – способность организации, осуществляющей техническое обслуживание и ремонт, при заданных условиях по запросу обеспечивать ресурсы, необходимые для технического обслуживания и ремонта объекта, в соответствии с заданными правилами технического обслуживания и ремонта. Это сделано для того, чтобы помимо ремонтнопригодности, характеризующей внутренние свойства собственно технического объекта, отразить характеристики системы технического обслуживания и ремонта, относящейся к этому объекту. Вообще, систему технического обслуживания и ремонта в настоящее время часто рассматривают как неотъемлемую часть объекта, который она обслуживает [19].

Смысл примечания к определению состоит в том, что не существует показателей, количественно характеризующих надежность в целом, а все показатели характеризуют только составляющие надежности: готовность, безотказность и др.

Из табл. 2 видно, что определение надёжности в ГОСТ Р 27.002–2009, который основан на МЭК 60050-191, содержит серьезные ошибки: в нем упущена обеспеченность технического об-

служивания, влияющая на готовность, зато появилась не определённая в стандарте «поддержка технического обслуживания». В результате смысл термина исказился, а определение стало не вполне понятным. Как уже отмечалось [20], этот стандарт содержал и множество других ошибок и неточностей, что и послужило основанием для приостановки его действия и восстановления применения ГОСТ 27.002–89 [21].

Анализ табл. 2 позволяет сделать также следующие выводы:

- разработчики отечественных стандартов, к сожалению, не всегда учитывают существующие стандарты и иногда дают свои определения уже имеющимся в них терминам;
- несмотря на наличие действующего отечественного терминологического стандарта, при создании стандартов, гармонизированных с МС ИСО и МЭК, как и положено, используются термины и определения из МС.

Таким образом, возникают расхождения в определениях одних и тех же терминов в различных стандартах, что не может не создавать трудностей в их использовании. Более того, это вообще порождает недоверие и нигилизм по отношению к стандартам. В самом деле, стандарты призваны обеспечивать совместимость, согласованность и т.п., но как они могут решать эти задачи, если сами несогласованы между собой?! Это обстоятельство является немаловажным доводом в пользу гармонизации стандартов, поскольку она может если не совсем устранить, то, по крайней мере, существенно уменьшить расхождения между стандартами.

4. Гармонизация с МС: за и против

Формальные основания гармонизации стандартов:

- в соответствии со ст. 12 Федерального закона РФ «О техническом регулировании» «стандартизация осуществляется в соответствии с принципами: <...> применения международного стандарта как основы разработки национального стандарта...»;
- правила ВТО требуют при составлении национальных стандартов и технических норм брать за основу международные стандарты.

По существу гармонизация стандартов:

- обеспечивает техническую и информационную совместимость;
- облегчает взаимопонимание и взаимодействие с поставщиками, партнёрами, клиентами, коллегами (особенно, зарубежными);
- позволяет использовать опыт и знания всего мирового профессионального сообщества;
- снижает риск возникновения расхождений между стандартами, поскольку, как уже указывалось выше, другие системы стандартов (например, по системам менеджмента качества, менеджменту риска) используют терминологию и методологию надёжности МЭК.

Вместе с тем гармонизация стандартов порождает и некоторые проблемы. Во-первых, она может потребовать ломки стереотипов, отказа от старых взглядов и представлений. Однако и в прошлом наши представления не раз менялись (см. табл. 1). Во-вторых, могут возникать трудности перевода, особенно применительно к терминологическим стандартам. Они и стали одной из причин неудачи с ГОСТ Р 27.002–2009. Однако преодолевают же как-то эти трудности в других странах. В этой связи стоит сослаться на портал «Электропедия» (Electropedia), представляющий собой онлайн-версию Международного электротехнического словаря. Его часть 191 [22] и есть МС МЭК 60050-191 (1990). Так вот, в ней приведены термины на 10 языках (русского среди них, к сожалению, нет).

Конечно, далеко не всегда международные стандарты согласуются с опытом и взглядами отечественных специалистов и нашими реалиями, поэтому необходим тщательный, непредвзятый сопоставительный анализ основных положений международных и отечественных стандартов в тех случаях, когда между ними возникают расхождения.

5. Определение надежности в новом стандарте МЭК

Со временем стало понятно, что определение надежности в МЭК 60050-191:1990 имеет определенные недостатки. А именно:

- носит «перечислительный» характер, т.е. не дает собственного определения понятия «надежность», а лишь перечисляет составляющие это сложное понятие более простые свойства;
- не охватывает некоторые другие важные свойства, также относящиеся к надежности, например, долговечность.

Поэтому когда в ТК 56 МЭК началась работа по пересмотру МС 60050-191:1990, было решено обновить и определение надежности. Вначале предполагалось, что будет принята 2-я редакция того же стандарта, но затем он получил новый номер 60050-192. Вся эта работа шла достаточно долго и, наконец, вышла на завершающую стадию: в августе 2014 г. ожидается официальная публикация этого МС [4].

После долгих споров и обсуждений в нем было сформулировано следующее весьма общее определение надежности (dependability):

«ability (of an item) to perform as and when required».

Это можно перевести как «способность (объекта) выполнять как и когда требуется» или, что представляется более точным по смыслу, «способность (объекта) функционировать как и когда требуется».

Второй вариант перевода является более правильным с точки зрения грамматики. Глагол «выполнять» является переходным, т.е. требует после себя отсутствующее в этом определении прямое дополнение – объект действия (выполнять что?), а глагол «функционировать» – непереходный. Отметим, что английский глагол to perform, вообще говоря, может быть как переходным, так и непереходным, но в данном случае он является непереходным¹.

Первый же вариант способен исказить смысл определения, поскольку отсутствующее, но напрашивающееся после переходного глагола «выполнять» прямое дополнение может домысливаться читающим (например, выполнять задание), придавая определению смысл, который в него не заложен.

На первый взгляд определение надежности в МС 60050-192 кажется совсем непохожим на привычные определения из наших стандартов, приведенные в табл. 1. Однако более внимательный анализ показывает, что оно достаточно близко к основной части непараметрического определения из ГОСТ 27.002–89 (табл. 1, п. 6).

Прежде всего, отметим, что в ГОСТ 27.002–89 надежность – это свойство, а в МС 60050-192 – это способность. Однако, если обратиться к Толковому словарю русского языка под ред. Д.Н. Ушакова [23], мы увидим, что «способность – качество, свойство, состояние, дающее возможность производить те или иные действия, исполнять ту или иную работу», а «свойство – качество, признак, способность, характеризующие кого/что-нибудь, составляющие отличительную особенность кого/чего-нибудь». Таким образом, в числе значений слова «способность» есть «свойство» и наоборот, слово «свойство» имеет значение «способность». Но не это семантическое различие вызвало споры среди членов РГ. Суть возникших разногласий в следующем.

Одна из сторон считает, что «способность к выполнению требуемых функций» – это практически то же самое, что «способность функционировать, как... требуется», а «сохранять во времени» означает «когда требуется». Другая сторона считает, что это далеко не очевидно, и предлагаемая в

¹ Следует заметить, что официального русского перевода этого документа ещё нет, поэтому мы столь подробно объясняем свой вариант перевода.

МС формулировка может пониматься таким образом, что она будет определять вовсе не свойство надежности, а способность объекта выполнить требуемую задачу.

По мнению первой стороны, в определение надежности в МС только для краткости не включены некоторые уточнения, предполагая понятным, что критерий способности функционировать как требуется (или способности к выполнению требуемых функций) должен быть задан в нормативно-технической и (или) конструкторской (проектной) документации (как это было указано в ГОСТ 27.002–89). В частности, это может быть сделано заданием пределов для значений всех параметров, характеризующих способность выполнять требуемые функции, т.е. возможность параметрического подхода в тех случаях, когда он применим, не исключается. Также в документации обычно задаются режимы и условия применения, технического обслуживания, хранения и транспортирования, в которых только и рассматривается способность функционировать как требуется.

Кроме того, в МС общее понятие «надежность» традиционно рассматривается как чисто концептуальное, собирательное, не имеющее количественного описания (см. табл. 2). Для практического же применения важны отдельные составляющие надежность свойства (безотказность, ремонтпригодность, долговечность), которые характеризуются количественными показателями. В определениях этих свойств в МС оговорка «при данных условиях» непременно присутствует.

Если согласиться с первой точкой зрения о практической тождественности двух «функциональных» определений надежности, то оба эти определения не будут выходить за границы параметрического определения надежности по ГОСТ 27.002–89.

По мнению второй стороны, «способность функционировать как... требуется» по МС МЭК принципиально отличается от «способности к выполнению требуемых функций» по ГОСТ 27.002–89, поскольку в последнем есть явное указание на «условия и режимы применения», установленные в технической документации. Поэтому, можно утверждать, что старая формулировка в отличие от новой не учитывает внешние воздействия, не предусмотренные «условиями и режимами применения», т.е. характеризует то, что можно назвать «собственной» надежностью объекта.

Так, автомобиль, стоящий в «пробке» (или по любым другим причинам, не связанным с его характеристиками) не потерял свойство «сохранять... способность к выполнению требуемых функций в заданных режимах и условиях применения...». С другой стороны, поскольку в определении МС нет упоминания о «заданных режимах и условиях применения...», то «способность функционировать, как... требуется» может считаться зависящей, в том числе, и от наличия «пробки» (т.е. в этих условиях автомобиль эту способность теряет, если мы так понимаем смысл «способности функционировать как требуется»).

Иными словами, сторонники этой точки зрения полагают, что отсутствие в МС МЭК упоминания о «режимах и условиях...» создает возможность расширения понятия «надежность», которое при этом будет включать в себя не только жестко регламентированную «собственную» надежность объекта, но более широкую способность функционировать, «как надо, когда надо», т.е. выполнить задачу, в которой объект участвует.

В этом случае, речь может идти о том, чтобы рассматривать решение конечной задачи, которую должен выполнить объект (выполнить расчет – ЭВМ, обеспечить устойчивую связь – система связи, освещать темный подъезд – электрическая лампочка и т.п.). Поскольку потребителя, пользователя, заказчика интересует только конечный результат, вне зависимости от причин, по которым он может быть не достигнут (где «собственная» надежность объекта является только одной из них), такая интерпретация МС может представляться вполне оправданной с точки зрения конечного потребителя, не разбирающегося глубоко в проблемах надежности.

6. Параметрическое и функциональное определения термина «надежность»

Как уже говорилось, будем называть определение из п. 6 табл. 1 – параметрическим, а определение из того же пункта, но в столбце примечаний – функциональным (оно выделено курсивом). Также функциональным является определение МС МЭК, рассмотренное в предыдущем разделе. В итоге мы имеем три определения:

1) параметрическое: *надежность – это свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования;*

2) функциональное (отечественное): *надежность – это свойство объекта сохранять во времени способность к выполнению требуемых функций в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования;*

3) функциональное определение МС МЭК: *надежность – это способность объекта функционировать, как и когда требуется.*

Два функциональных определения сравнивались между собой в предыдущем разделе, а здесь сравним параметрический (ГОСТ 27.002–89) и функциональный (МС МЭК) подходы к определению надежности.

Прежде, чем перейти к обсуждению плюсов и минусов каждого из них, мы хотели бы сделать одно отступление и напомнить читателям о чрезвычайно важном понятии, которое редко звучит в русскоязычной технической литературе. Мы говорим о так называемых «операциональных определениях» (ОО) – термине, введенном в научно-техническую литературу XX века выдающимися американскими статистиками У. Шухартом и Е. Демингом [24]¹. Операциональным называют такое определение, которое:

а) понятно;

б) для которого указан *практический* способ его однозначной реализации/проверки.

Необходимость введения ОО вызвана тем простым фактом, что в любом языке существует множество неоднозначных слов, которые разные люди понимают по-разному, что, естественно, приводит к разной реакции на одни и те же слова. Естественно, что в терминологическом стандарте использование не операциональных определений особенно опасно: разное понимание основополагающих терминов может приводить к самым непредсказуемым последствиям².

Итак, возвращаемся к нашим определениям термина «надежность». Параметрическая формулировка определяет надежность через нахождение всех параметров объекта в заданных диапазонах. В ситуации, когда параметры объекта всегда перечислены в сопутствующей нормативно-технической документации, и диапазоны их изменения в заданных режимах указаны, это определение удовлетворяет требованию к ОО. Действительно, проверить практически, находятся ли параметры объекта в установленных пределах, можно всегда, и ответ на этот вопрос будет всегда однозначным: параметры либо внутри некоего диапазона, либо снаружи.

С другой стороны, как уже отмечалось и в самом ГОСТ 27.002–89, параметрическое определение не всегда пригодно, особенно, если применять его не в теории, а на практике. Чтобы понять это, достаточно попытаться составить перечень «всех параметров, характеризующих способность выполнять требуемые функции» и установить допустимые пределы их значений, например, для

¹ Сама концепция восходит к работам П.У. Бриджмена – см. [25].

² Мы намеренно выделили курсивом слова «практически» и «однозначно» при формулировке понятия об ОО в силу их принципиальной важности.

таких широко используемых изделий, как телевизор, компьютер, телефон, автомобиль и т.п. Сделать это будет весьма сложно даже специалистам соответствующих отраслей, а уж разобраться в этом пользователям будет практически невозможно.

С функциональным определением, в отношении операциональности, все гораздо хуже, потому что свойство объекта «функционировать, как и когда требуется», могут по-разному интерпретировать, например, изготовитель объекта и его потребитель. Действительно, для изготовителя эти слова означают то же самое, что и слова про параметры: работать как положено при установленных ограничениях. Но потребитель ничего про установленные параметры и их диапазоны, как правило, не знает и, что ещё важнее, знать не хочет. Для него слова «функционировать, как и когда требуется» могут означать, что он получает от объекта то, на что он рассчитывает, т.е. объект выполняет некоторую функцию в интересующих потребителя условиях. И здесь неизбежно возникает конфликт, связанный с тем, что выполнение некоей функции, удовлетворяющей потребителя, может во многих случаях отличаться от той функции, которую подразумевает изготовитель. Рассмотрим простейший пример, чтобы пояснить эти общие рассуждения.

У Вас на лестничной клетке есть осветительное устройство, освещающее коридор. Параметрическое определение надежности требует задания списка технических параметров устройства с указанием пределов, внутри которых каждый из параметров должен находиться. Функциональное определение надежности для изготовителя этого устройства совпадает с параметрическим: под функционированием, как и когда надо он будет понимать именно такое функционирование, при котором параметры, характеризующие работоспособность устройства находятся в заданных диапазонах. Но потребитель имеет совсем иное представление о работе данного прибора. Ему нужно, чтобы оно выполняло свою функцию – освещало коридор. Но освещение коридора зависит не только от собственно осветительного устройства, но и от многих других факторов, например, от электрика, который обслуживает данный дом, от ЖЭКа, который отвечает за освещение подъезда, и т.д. Ясно, что все эти факторы не имеют никакого отношения к надежности самого устройства. Но как быть с выполнением им своей функции? Если мы говорим, что надежность – это способность данного объекта «функционировать, как и когда требуется», то потребитель может понять это как «способность освещать коридор, как и когда требуется», что на деле будет зависеть и от нашего устройства, и от многих других факторов, непосредственно не связанных с освещающим прибором. Например, электрик становится фактором, влияющим на выполнение функции нашим устройством – он входит в систему его обслуживания, и, следовательно, влияет, например, на время его ремонта. Другими словами, функциональное определение надежности может приводить к размыванию границы между надежностью объекта и возможностью выполнения задачи.

Чтобы избежать этой неоднозначности, требуется, чтобы слова «*функционировать как и когда требуется*» сопровождалось операциональным описанием того, в чем состоит нужная функция, и какая система отвечает за её выполнение. Возвращаясь к нашему примеру: у осветительного устройства не может быть функции «освещать коридор» – оно изготавливается не для коридора или комнаты, а с целью создавать определенный световой поток при определенных условиях, а уж повесить его могут где угодно. Если потребитель говорит, что ему нужен свет в коридоре, то он должен понимать, что речь идет о системе, в которой само устройство, дающее свет – только одна из подсистем, и функция «освещать коридор» относится к задаче, решаемой системой, в которую входят и устройство, и электрик, и ЖЭК. Соответственно, если света нет, то нужно разбираться, по какой причине. Если эта причина не имеет отношения к самому устройству, то его надежность здесь не причем.

Иначе говоря, свойство сохранять параметры в каком-то диапазоне – это внутреннее свойство объекта, зависящее от его состояния в данный момент, а способность выполнять некую функцию

может пониматься и как его внутреннее свойство, и как результат его взаимодействия с внешним миром – все зависит от того, кем и как определено, что подразумевается под словами «*функционировать как и когда требуется*». Указанной выше неоднозначности можно было бы избежать, если бы существовало отдельное понятие «способность выполнить задачу» (СВЗ) и было бы определено, как оно соотносится с надежностью, безопасностью, эффективностью и т.д. К сожалению, авторам такое понятие, как общепринятый международный термин не известно.

Таким образом, мы имеем следующую дилемму: либо оставить более узкое параметрическое определение надежности из старого ГОСТ и получить матрицу его сильных и слабых сторон, показанную в табл. 3, либо согласиться с более общим функциональным определением, и получить матрицу, показанную в табл. 4.

Таблица 3. Параметрическое определение: плюсы и минусы

	Плюсы	Минусы
Внутренние факторы	Удовлетворяет условию операциональности	Не охватывает ситуации, когда параметрическое описание нецелесообразно или невозможно
Внешние факторы	Хорошо знакомо и привычно	Увеличивает разрыв между российскими и зарубежными специалистами и стандартами

Таблица 4. Функциональное определение: плюсы и минусы

	Плюсы	Минусы
Внутренние факторы	Годится для более широкого круга ситуаций, в том числе, когда параметрическое определение нецелесообразно или невозможно	Не удовлетворяет условию операциональности, т.е. может приводить к неоднозначной интерпретации надежности
Внешние факторы	Гармонизировано с МС	Требует более высокой грамотности в отношении надежности

Почему мы написали в табл. 4 про грамотность в отношении надежности? Причина проста: нужно, чтобы все, кто, так или иначе, могут соприкасаться с проблемами надежности, научились разделять функции (задачи), выполняемые (решаемые) системой, и функции, выполняемые её частями и/или элементами. При этом условии оба эти определения по своей сути совпадают – так считает одна группа специалистов. Другая группа полагает, что определение в МС МЭК допускает интерпретацию, определяющую вовсе не надежность, а СВЗ, поэтому нужно сохранить старое определение надежности по ГОСТ 27.002–89, а перевод МС МЭК издать как проект стандарта, определяющего понятие СВЗ.

Нами изложены доводы, отражающие позиции дискутирующих сторон. Мы сознательно уклонились от попытки дать какие-то окончательные рекомендации, с тем, чтобы специалисты в области надежности, проектирования, эксплуатации, ремонта элементов, систем, объектов высказались за тот или иной вариант определения надежности и связанных с нею терминов. Единственное, что стоило бы добавить: мы понимаем, что понятие надежности является очень широким, и какую бы сторону в данной дискуссии не занять, формальный подход не будет работать в каких-то случаях при любом выборе. Поэтому, в любом случае, мы должны уповать на грамотность тех, кто будет применять термины по надежности на практике.

Литература

1. **Нетес В.А., Тарасьев Ю.И., Шпер В.Л.** Актуальные вопросы стандартизации терминологии в области надёжности // *Надёжность*. 2014. № 2.
2. ГОСТ Р 27.002–2009. Надёжность в технике. Термины и определения.
3. ГОСТ 27.002–89. Надёжность в технике. Основные понятия, термины и определения.
4. IEC 60050-192/Ed. 1. International Electrotechnical Vocabulary – Part 192: Dependability.
5. Теория надёжности в области радиоэлектроники. Терминология / АН СССР. Ком. техн. терминологии. Ин-т радиотехники и электроники. Сб. рекомендуемых терминов. Вып. 60. – М.: Изд-во АН СССР, 1962.
6. Надёжность технических систем и изделий. Основные понятия. Терминология / АН СССР. Ком. техн. терминологии; ВСНТО. Ком. по надёжности и контролю качества продукции. Сб. рекомендуемых терминов. Вып. 67. – М.: Изд-во стандартов, 1964.
7. ГОСТ 13377–67. Надёжность в технике. Термины.
8. ГОСТ 13377–75. Надёжность в технике. Термины и определения.
9. ГОСТ 27.002–83. Надёжность в технике. Термины и определения.
10. **Hosford J.E.** Measures of dependability // *Operations Research*. 1960. Vol. 8. No 1.
11. **Laprie J.C., Costes A., Troy R.** Dependability: Requirements and Solutions // *Proc. SEE Congr. on Electrical and Electronical System Dependability*, Toulouse, France, 1979.
12. **Laprie J.C.** Dependable Computing and Fault Tolerance: Concepts and terminology // *Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing*, 1985.
13. **Авижиенис А., Лапри Ж.-К.** Гарантоспособные вычисления: от идеи до реализации в проектах // *ТИИЭР*. 1986. Т. 74. № 5. С. 8–21.
14. МККТТ. Рекомендация G.106. Термины и определения, относящиеся к качеству обслуживания, готовности и безотказности // МККТТ. Красная книга. Т. III. Вып. III.1. Общие характеристики международных телефонных соединений и цепей. Рекомендации G.101– G.181. 1984. С. 38–93.
15. Надёжность и техническое обслуживание АМТС с программным управлением: Справ. пособие / **Вегенер Р.Р., Дедоборщ В.Г., Зарецкий К.А.** и др.; Под ред. **Дедоборща В.Г.** и **Суторикина Н.Б.** – М.: Радио и связь, 1989.
16. Международный стандарт IEC 50-191. Международный электротехнический словарь. Глава 191. Надёжность и качество услуг. 1990.
17. ГОСТ ISO 9000–2011. Системы менеджмента качества. Основные положения и словарь.
18. ГОСТ Р 51901.3-2007 (МЭК 60300-2:2004). Менеджмент риска. Руководство по менеджменту надёжности.
19. **Ушаков И.А.** Курс теории надёжности систем. – М.: Дрофа, 2008.
20. **Нетес В.Н., Резиновский А.Я., Тарасьев Ю.И.** и др. Деградация вместо гармонизации. О новом стандарте по терминологии в области надёжности // *Стандарты и качество*. 2011. № 5. С. 40–44.
21. Приказ Росстандарта № 1843-ст от 29.11.2012 «О приостановлении применения национального стандарта и восстановлении применения на территории Российской Федерации межгосударственного стандарта».
22. **Electropedia**. Area 191: Dependability and quality of service (<http://www.electropedia.org/iev/iev.nsf/index?openform&part=191>)
23. Толковый словарь русского языка. Т. 4 / Под ред. **Д.Н. Ушакова**. – М.: ООО «Изд-во Астрель», ООО «Изд-во АСТ», 2000.
24. **Нив Г.** Пространство доктора Деминга: Принципы построения устойчивого бизнеса. – М.: Альпина Бизнес Букс, 2005.
25. **Bridgman P.W.** The logic of modern physics. – New York: Macmillan, 1927.



Netes V.A., Tarasyev J.I., Shper V.L.

HOW WE SHOULD DEFINE WHAT “DEPENDABILITY” IS

Currently, the Technical committee for standardization “Dependability in equipment” (TC 119) is developing a new interstate standard “Dependability in equipment. Terms and definitions” that will replace GOST 27.002–89. The issue was already discussed at the pages of our journal. In Issue 2 this year there was a report about the meeting of a permanent scientific seminar “Dependability and quality of system functioning” that took place on the 30th of January 2014 and was devoted to discussion of key issues related to the development of this standard. In the same issue there was a paper by active participants of the work V.A. Netes, J.I. Tarasyev, V.L. Shper Current issues of terminology standardization in dependability where the authors started a detailed consideration of this important topic.

Now we offer a new paper by the same authors that further discusses terminology issues in dependability. The editors invite all involved readers to express their opinions about issues put forth in the paper. Letters can be sent to the editors or directly to TC 119.

“When I use a word,” Humpty Dumpty said to Alice, “it means just what I choose it to mean – neither more nor less.”

Lewis Carroll “Alice in Wonderland”

1. Introduction

In the paper [1] we briefly told the history of cancellation of GOST R 27.002-2009 [2] and return to GOST 27.002-89 [3] – to the standard of 25-year remoteness, and also about the beginning of work on the new version of the fundamental terminology standard and difficulties the working group (WG) faced when undertaking this work. In the same work it was marked out that one of the main problems is a question about what definition of the fundamental term “dependability” should be taken as a basis of the new standard: the old definition from GOST 27.002-89 or the new one from the international standard (IS) prepared by IEC [4] (its publication was expected in August, 2014). In this study we shall try to state the essence of disagreements which have arisen among WG members and the reasons, which forced us to consider this issue as fundamental.

But before to proceed to discussion proper, we believe reasonable to briefly remind readers how the term “dependability” was defined in all previous domestic terminological standards and how it is defined in the international documents including the last edition of IEC IS.

2. Definition of the term “dependability” in standards of the Soviet period

Table 1 presents definitions of the fundamental term in old documents issued in 1962 and notes with explanations as to this term beginning from the Collection of recommended terms of the USSR Academy

of Sciences. We have cited definitions completely, and explanations and notes are given as pertaining to the subsequent discussion.

Table 1. Definitions of the term “dependability” in the Soviet documents

No.	Source	Definition	Note to the definition
1	The Collection of recommended terms. Issue 60.1962 [5]	System attribute (system element attribute), conditioned mainly by its reliability and maintainability and providing task performance in the volume established for the system (system element); it is quantitatively defined by probabilistic characteristics and parameters	
2	The collection of recommended terms. Issue 67.1964 [5]	System or product attribute, conditioned by their reliability, durability and maintainability, and providing normal performance of the specified system (product) functions; it is quantitatively estimated, for example, as a product of probability of non-failure operation by utilization factor use (or by availability factor)	
3	GOST 13377-67 [7]	Product attribute to perform the specified functions, retaining the operational parameters in the set limits during a required time or required non-failure operation time	Dependability of a product is conditioned by its “reliability”, “maintainability”, “storageability”, and also “durability” of its parts
4	GOST 13377-75 [8]	Product attribute to perform the specified functions, retaining in time values of the established operational parameters in the set limits corresponding to the specified modes and conditions of use, maintenance, repairs, storage and transportations	Dependability is complex property, which depending on object purpose and conditions of its operation can include reliability, durability, maintainability and storageability separately or a certain combination of these properties both for the object and for its parts. “Operational parameters” are parameters of productivity, rate, consumption of power, fuel, etc. <i>From the explanation to the term:</i> “Quality of production is understood as the aggregate of its properties conditioning production suitability for satisfaction of certain needs according to its purpose. One of properties of this aggregate is dependability”.
5	GOST 27.002-83 [9]	Object attribute to retain in time in the established limits the values of all parameters describing an ability to perform required functions in specified modes and conditions of application, maintenance, repairs, storage and transportation	Dependability is a complex property which depending on object purpose and conditions of its application consists of combinations of properties: reliability, durability, maintainability and storageability

6	GOST 27.002-89 [3]	Object attribute to retain in time in the established limits the values of all parameters describing ability to perform required functions in specified modes and conditions of application, maintenance, repairs, storage and transportation	Dependability is complex property, which depending on object purpose and conditions of its operation can include reliability, durability, maintainability and storage-ability separately or certain combination of these properties. <i>From the explanation to the term:</i> Terminology on dependability is applied to any technical objects – products, constructions and systems, and also to their subsystems ... Assembly units, parts, components or elements can be considered as subsystems. If necessary the information and its carrier and also the human factor can be included in concept “object” (for example, in case of dependability consideration of the system “machine – operator”). ... The following definition does not change boundaries of the concept “dependability”: <i>Dependability is an object’s attribute to retain in time an ability to perform required functions in specified modes and conditions of application, maintenance, repairs, storage and transportation.</i> This definition is applied when the parametrical description is unreasonable (for example, for the elementary objects, whose operability is characterized as “yes – no”), or it is impossible (for example, for systems “machine – operator”, i.e. for such systems, in which not all properties can be characterized quantitatively). Kinematic and dynamic parameters, parameters of structural strength, parameters of functioning accuracy, productivity, rate, etc. are applied to the parameters describing ability to perform required functions.
---	--------------------	--	--

From table 1 it is evident that dependability definition has changed with acceptance of each new document. As a result we have the following sequence of transformations of dependability definition (we simplify formulations, retaining the sense):

1962 – system attribute to perform the task;

1964 – system (product) attribute to perform specified functions;

1967 (the first GOST) – Product attribute to perform specified functions, retaining its parameters in the specified limits;

1975 – object attribute to perform specified functions, retaining the specified parameters in in the set limits;

1983, 1989 – object attribute to retain in the established limits the values of all parameters describing an ability to perform required functions;

1989 (appendix) – object attribute to retain ability to perform required functions.

Thus, in GOST, since 1983, the ability to perform required functions began to be interpreted as retention in the specified limits of all parameters established in normative and technical and (or) design (engineering) documentation. For the sake of brevity, we shall further on name such a definition as parametrical definition.

It should be noted that in currently acting GOST 27.002-89 there are actually two definitions of dependability: in the basic text of the standard and in the reference appendix containing the explanations to terms (table 1, clause 6). At the same time it is indicated that the second definition does not change boundaries of the concept “dependability” and it is “applied when the parametrical description is unreasonable ... or it is impossible ...”

In this connection, it is expedient to discuss the issue on what definition should be used as the fundamental one and what can be retained as auxiliary definition. We shall return to this issue later for now we shall continue the historical review.

3. Definition of the term dependability in the international standards and the domestic standards based on international ones

Right up to 1984 in IS there was no general term equivalent to Russian “dependability”. There were only terms for separate and narrower properties: reliability, availability etc. In particular, IEC Technical committee (TC) 56, named now “Dependability”, referred to as “Reliability and Maintainability”. There were also longer word-combinations, for example, Reliability, Availability, Maintainability and Safety (non-failure operation, readiness, maintainability and safety) – the concept widely used, in particular, on railway transport to which abbreviation RAMS is usually applied.

To tell the truth, in 1960 the American researcher J. Hosford introduced the term dependability and corresponding measures [10]. Generally they were defined as the probability that the system will be able to function, when it is required. He wrote that it is one of the important characteristics of any systems in which failures can occur. In special cases these measures were availability factors (instant or averaged interval) and probability of non-failure operation.

From the end of 1970th J.C. Laprie from the Department of information and engineering sciences of the French national center of scientific researches in Toulouse began to apply the term dependability to computing systems [11, 12, etc.]. It was interpreted rather widely and with reference to this area began to be translated into Russian as “ability to guarantee” [13]. This concept was defined as system property, allowing to rely on performance of services for which it is intended.

In 1984 the International advisory committee on telephony and telegraphy (IACTT) of the International Telecommunication Union (ITU) adopted Recommendation G.106 [14] containing terms and definitions in the field of service quality and dependability in which the general term “dependability” appeared. The concepts introduced in it soon began to be used actively by branch experts, including experts in our country [15].

Thus, expansion of concept “dependability” happened under the initiative of the most advanced and dynamically developing branches: computer facilities and telecommunication.

Then the term dependability was introduced in IEC IS 50-191 accepted in 1990 which IEC developed together with ITU. Afterwards, in connection with the change of IS notation system it received number 60050-191. As all others TCs of ISO and IEC recognize the leading role of IEC /TC56 in issues of dependability, this standard is “horizontal” (inter-branch and inter technological), and the terms defined in

it are used in all ISO and IEC standards where dependability is mentioned. It provides coordination of all ISs in interpretation of the dependability fundamental concepts. In this respect, as it will be obvious from the further, they differ on the positive side from domestic standards.

Table 2 presents Russian translation alternatives for “dependability” term definition and notes to it from official documents: Russian versions of Recommendation G.106 [14] and IEC IS 50-191 [16], Russian standards [17, 18] and the interstate standard [19].

Table 2. Translations of dependability term definition from the international documents in domestic documents

No.	Source	Definition	Note to the definition
1	Recommendation of IACTT G.106 [14]	The collective term used for characteristics of availability and factors of its conditioning: reliability, maintainability and ensuring of object maintenance	The given term is used only for the general descriptions without quantitative expressions
2	IEC IS 50-191 [16]	The collective term used for the description of availability attribute property and influencing it properties of reliability, maintainability and ensuring of maintenance and repair	The given term is applied only to the general not quantitative description of availability property
3	GOST ISO 9000-2011 [19]	The same	The term “dependability” is applied only to the general non-quantitative description of property
4	GOST R 51901.3-2007 (IEC 60300-2:2004) [17]	Property of availability and influencing it properties of reliability, maintainability and ensuring of maintenance and repair	The given term is applied only to the general non-quantitative description of availability property
5	GOST R 27.002-2009 [18]	Property of availability and influencing it properties of reliability and maintainability and maintenance support	The given term is used only to the general non-quantitative description of dependability

In comparison with domestic standards one more dependability component was added in IS: ensuring of maintenance and repair – the ability of the organization which is carrying out maintenance and repair, under the specified conditions on demand to provide the resources necessary for object maintenance and repair, according to the given rules of maintenance and repair. It is made in order to reflect the characteristics of maintenance and repair system, concerning to this object in addition to maintainability describing internal properties of a technical object proper. In general, a maintenance and repair system nowadays is frequently considered as integral part of an object which it maintains [19].

The sense of the note to definition consists in the fact that there are no measures quantitatively describing dependability as a whole, but all measures describe only components of dependability: availability, reliability, etc.

It is evident from table 2 that dependability definition in GOST R 27.002-2009 which is based on IEC 60050-191 contains serious mistakes: insuring of maintenance influencing availability is missed, but “maintenance support” appeared, which is not defined in the standard. As a result, the sense of the term was deformed, and its definition became not quite clear. As it has been already noticed in [20], this standard contained also a number of other mistakes and discrepancies that caused the suspension of its use and restoration of application of GOST 27.002-89 [21].

The analysis of Table 2 also allows us to draw the following conclusions:

- developers of domestic standards, unfortunately, not always take into account existing standards and sometimes give their own definitions to terms already available in them;
- despite of presence of domestic terminological standard currently in force, at creation of standards harmonized with IS ISO and IEC, terms and definitions from IS are used the way it should be.

Thus, there are disagreements in definitions of the same terms in various standards that should create difficulties in their use. Moreover, in general it generates mistrust and nihilism in relation to standards. Really, standards are intended to provide compatibility, coordination, etc. but how can they solve this problem if they are unmatched among themselves?! This circumstance is an important reason for the benefit of harmonization of standards, as it can if not absolutely remove, at least essentially reduce discrepancies between standards.

4. Harmonization with IS: pro et contra

The formal bases of standard harmonization:

- According to item 12 of Federal laws of the Russian Federation “About technical regulation” “standardization is put into practice according to principles: <...> applications of the international standard as the bases of the national standard development ...”;
- WTO rules require taking for a basis the international standards at preparation of national standards and technical norms.
- Standard harmonization in essence:
 - Provides technical and information compatibility;
 - Facilitates mutual understanding and interaction with suppliers, partners, clients, colleagues (particularly with foreign ones);
 - Allows using of experience and knowledge of all world professional community;
 - Reduces a risk of discrepancy occurrence between standards as it has been already specified above, other systems of standards (for example, systems of quality management, risk management) use terminology and methodology of dependability from IEC standard.

At the same time harmonization of standards generates also some problems. First, it can demand destruction of stereotypes, refusal of old convictions and conceptions. However even in the past our conceptions also changed from time to time (see Table 1). Second, difficulties of translation can occur, especially with reference to terminological standards. They just became one of the reasons of unsuccessful introduction of GOST R 27.002-2009. However these difficulties somehow are overcome in other countries. In this connection it is necessary to refer to portal “Electropedia” representing an online version of the International electrotechnical dictionary. Its part 191 [22] is just IS IEC 60050-191 (1990). So it should be noted that it presents terms in 10 languages (unfortunately, Russian among them is not present).

Certainly, the international standards not always coordinate with experience and convictions of domestic experts and our realities; therefore it is necessary to carry out a careful, unbiased comparative analysis of international and domestic standards fundamentals when there are disagreements between them.

5. Dependability definition in a new IEC standard

Over time it became clear that dependability definition in IEC 60050-191:1990 has certain shortcomings. Exactly it:

- has “enumerative” nature, i.e. does not provide its own definition of concept “dependability”, and only lists more simple properties making up these complex concept;

- does not cover some other important properties also concerning dependability, for example, durability.

Therefore, when work on revision of IC 60050-191:1990 began in IEC TC 56, it was decided to update also the dependability definition. In the beginning it was supposed that the 2-nd edition of the same standard would be accepted, but then it received new number 60050-192. All this work was carried out for long enough and, at last, came into a finishing stage: in August, 2014 the official publication of this standard is expected [4].

After long disputes and discussions the following rather general dependability definition has been formulated:

“an ability (of an item) to perform as and when required.”

It can be translated as “an ability (of an object) to perform as and when it is required.” Or, what seems more exact by implication, “an ability (of an object) to function as and when it is required.”

The second translation version is also more correct from the point of grammar. The verb “to perform” is a transitive verb, i.e. it demands after itself the direct object absent in this definition – an object of action (to perform what?), and the verb “to function” is an intransitive verb. It should be noted that an English verb to perform, generally speaking, can be both transitive and intransitive, but in this case it is an intransitive verb.¹

The first translation version is able to distort the sense of definition as the absent but suggesting itself direct object after the transitive verb “perform” can be thought up by a reader as missing (for example, to perform a task), giving to the definition a sense which is there.

At first sight, the dependability definition in IS 60050-192 seems absolutely unlike usual definitions of dependability in our standards, presented in Table 1. However, a more attentive analysis shows that it is close enough to the basic part of nonparametric definition in GOST 27.002-89 (table 1, item 6).

First of all, we shall note that in GOST 27.002-89 dependability is an attribute, but in IS 60050-192 it is an ability. However, if to address to the Explanatory dictionary of Russian under the editorship of D.N. Ushakov [23], we shall see, that “ability is a quality, property, condition giving an opportunity to make some actions, to execute this or that work” and “attribute is a quality, feature, ability, describing somebody/something, making up a distinctive feature of somebody/something”. Thus, among word meanings of “ability” there is “attribute” and on the contrary, the word “attribute” means “ability”. But not this semantic distinction has caused disputes among members of WG. The essence of the arisen disagreements is in the following.

One of the parties considers that “ability to perform required functions” is practically the same as “ability to function as ... it is required”, and “to retain in time” means “when it is required”. The other party considers that it is not obvious, and the offered formulation in IS can be understood in such a manner that it will define not dependability attribute, but an object ability to perform a required task (job).

In the first party’s judgment, the dependability definition in IS only for the sake of brevity does not include some refinements, assuming understandable that the ability criterion to function as it is required (or abilities to perform required functions) should be given in normative-technical and (or) in design (engineering) documentation (as it is specified in GOST 27.002-89). In particular, it can be made by specifying limits for values of all parameters describing the ability to perform required functions, i.e. possibility of the parametrical approach when applicable is not excluded. Also, as a rule, the documentation should have modes and conditions of application, maintenance, storage and transportation in which only the ability to function as it is required is considered.

¹ It should be noted that the official Russian translation of this document is still not available, therefore we explain our version of translation in such details.

In addition to that, the general concept “dependability” in IS it traditionally considered as only conceptual, aggregative, not having the quantitative description (see table 2). For practical application individual properties making up dependability are important (reliability, maintainability, durability), which are characterized by quantity measures. Stipulation “under the given conditions” certainly is present in definitions of these properties in IS.

If we agree with the first point of view about practical identity of two “functional” definitions of dependability, then both of these definitions will not overstep the boundaries of the parametrical definition of dependability in accordance with GOST 27.002-89.

In the second party’s judgment, “ability to function as ... it is required” in IS IEC essentially differs from “ability to performance of required functions” in accordance with GOST 27.002-89 as in the latter there is obvious indication on “conditions and modes of application” established in technical documentation. Therefore, it is possible to assert that the old formulation as opposed to new one does not take into account the external influences, which have not been specified by “conditions and modes of application” i.e. it characterizes what can be named as “own” dependability of an object.

So, the automobile standing in “traffic congestion” (or for any other reasons not connected to its characteristics) has not lost the attribute “to retain ... ability to perform required functions in specified modes and conditions of application ...” On the other hand, since in the international standard definition there is no reference to “specified modes and conditions of application ...” then “ability to function as ... it is required” can be considered dependent, on the presence of “traffic congestion” inclusive (i.e. in these conditions the automobile loses this ability if we understand the meaning of “ability to function as it is required” as mentioned above).

In other words, supporters of this point of view believe that the absence in IEC IS of reference to “modes and conditions ...” creates an opportunity of expansion of the concept “dependability” which in this case will include not only rigidly regulated “own” dependability of an object, but also a wider ability to function “as it is necessary, when it is necessary” i.e. to perform a task, in which the object participates.

In this case, discussion can lead to consideration of a final task solution, which should be performed by the object (to execute calculation – computer, to provide steady communication – communication system, to light a dark entrance – an electric bulb, etc.). As a consumer, a user, a customer is interested only in a final result, without dependence from any reasons, due to which the result can be not achieved (where “own” dependability of an object is only one of them), such interpretation of IS can be represented quite justified from the point of view of the end user who does not understand deeply problems of dependability.

6. Parametrical and functional definitions of the term “dependability”

As it was already said, we shall name the definition from clause 6 of table 1 as a parametrical definition, and the definition from the same clause, but in column of notes – a functional definition (it is highlighted in italics). The definition in IS IEC considered in the previous section is also functional. As a result, we have three definitions:

- parametrical: *dependability is an attribute of an object to retain in time in the established limits the values of all parameters describing ability to perform required functions in specified modes and conditions of application, maintenance, storage and transportation;*
- functional (domestic): *dependability is an object’s attribute to retain in time ability to perform required functions in specified modes and conditions of application, maintenance, repairs, storage and transportation;*
- functional definition in IS IEC: *dependability is ability of an object to function as and when it is required.*

Two functional definitions were compared among themselves in the previous section, and here we shall compare parametrical (GOST 27.002-89) and functional (IS IEC) approaches to dependability definition.

Before to switch over to discussion of advantages and disadvantages of each of them, we would like to make one back-off and to remind readers of an extremely important concept, which is seldom presented in the Russian technical literature. We mean so-called “operational definitions” (OD) – the term introduced into the scientific and technical literature of XX century by distinguished American statisticians U. Shuhartom and E. Demingom [24]¹. Definition is named as a operational definition, which:

- a) is understandable and;
- б) for which the *practical* way of its *unambiguous* realization / check is specified.

Necessity of OD introduction is caused by a simple fact that in any language there is a lot of ambiguous words, which various people understand differently, that, naturally, leads to different reaction to the same words. It is natural that in the terminological standard use of operational definitions is especially dangerous: the different understanding of fundamental terms can lead to the most unpredictable consequences².

So, we come back to our definitions of the term “dependability”. The parametrical formulation defines dependability through the finding of all object parameters in the specified ranges. In a situation when object parameters are always listed in the accompanying normative-technical documentation, and ranges of their change in modes are specified in the set modes, this definition meets requirement for OD. Indeed, it is always possible to check up practically whether these object parameters are in the established limits, and the answer to this question will be always unambiguous: parameters are either within a certain range, or outside.

On the other hand, as it was already mentioned in GOST 27.002-89, a parametrical definition is not always suitable, especially if we apply it not in theory, but in practice. To understand it, it is enough to try to make a list of “all parameters describing an ability to perform required functions” and to establish allowable limits of their values, for example, for such widely used products, as TV, a computer, a phone, an automobile, etc. It is rather difficult to make it even by experts of corresponding branches, and to understand it by users will be practically impossible.

With a functional definition, in relation to an ability to operate, everything is much worse, because an object’s attribute “to function, as and when it is required” can be interpreted differently, for example, by the manufacturer of an object and its consumer. Indeed, for the manufacturer these words mean the same, as words about parameters: to operate as it is necessary within the established limits. But the consumer, as a rule, does not know anything about the established parameters and their ranges, and what it is even more important, he does not want to know. For him words “to function, as and when it is required” can mean that he receives that from object what he expects, i.e. the object performs functions in conditions interesting to the consumer. Here again there is inevitably a conflict connected with the fact that performance of some functions, satisfying the consumer, can differ in many cases from the function which the manufacturer means. Let’s consider the elementary example to explain these general reasoning.

You have on your staircase the illuminating device lighting a passage. A parametrical definition of dependability demands the assignment of a list of unit technical parameters with indication of limits where each of the parameters should belong to. Functional definition of dependability for the manufacturer of this device coincides with a parametrical definition: the manufacturer will understand under the meaning of functioning “as and when it is required” such a functioning when parameters describing device operability are in the specified ranges. But the consumer has an absolutely different idea about operation of the given device. He wants that the device performs its function to illuminate a corridor. But

¹ The concept itself goes back to studies of P. U. Bridgman – see [25].

² We deliberately have italicized the word “practically” and “unambiguous” in the formulation of OD concept because of their fundamental importance.

illumination of a corridor depends not only on a lighting device itself, but also on many other factors, for example, on the electrician who serves the given house, on Housing office, which is responsible for entrance illumination, etc. Clearly, all these factors have no any relation to device dependability. But should we do with its performance of a function? If we say that dependability is an ability of the given object “to function, as and when it is required”, the consumer can understand it as “ability to illuminate a corridor as how and when it is required” that will depend actually on our device as well, and on many other factors which directly are not connected with an illuminating device. For example, the electrician becomes the factor influencing performance of a function by our device – it is included into the system of his service, and, hence, influences, for example, the period of its repair. In other words, a functional definition of dependability can lead to the blurring of boundaries between dependability of an object and an ability of performance of the task.

To avoid this ambiguity, it is required, that words “*to function as and when it is required*” should be accompanied by the operational description of what the necessary function consists, and which system is responsible for its performance. Coming back to our example: the illuminating device cannot have a function “to illuminate a corridor” – it is made not for a corridor or a room, but it is made with the purpose to create a certain light stream under specified conditions, and it can be installed anywhere. If the consumer says that he needs light in a corridor he should understand that it is addressed to the system where the device giving light presents only one of the subsystems, and a function “to illuminate a corridor” concerns the task solved by a system which includes both the device, the electrician, and Housing office. Accordingly, if there is no light, it is necessary to understand due to what reason. If this reason has no relation to the device, then its dependability here should be ignored.

In other words, a property to retain parameters in some range is the internal property of an object dependent on its condition at present, but an ability to perform a certain function can be understood both as its internal property or as a result of its interaction with an outside world – all depends on the fact who and how has defined what words “to function as and when it is required” means. The ambiguity mentioned above could be avoided if there would be a separate concept of “ability to perform a task” (APT) and it would be defined how it correlates with dependability, safety, efficiency, etc. Unfortunately, such concept as a standard international term is not known to authors.

Thus, we have the following dilemma: either to retain a narrower parametrical definition of dependability from the old GOST and to receive a matrix of its strong and weak sides, shown in Table 3, or to agree with a more general functional definition, and to receive a matrix shown in Table 4.

Table 3. Parametrical definition: advantages and disadvantages

	Advantages	Disadvantages
Internal factors	<i>Meet the condition of an ability to operate.</i>	Does not cover a situation when the parametrical description is inexpedient or it is impossible.
External factors	<i>Well familiar and usual.</i>	Increases disparity between Russian and foreign experts and standards

Table 4. Functional definition: advantages and disadvantages

	Advantages	Disadvantages
Internal factors	<i>Suits a more broad range of situations, including those when a parametrical definition is inexpedient or it is impossible.</i>	<i>Does not meet the condition of an ability to operate, i.e. can lead to the ambiguous interpretation of dependability.</i>
External factors	<i>It is harmonized with IS.</i>	<i>Requires higher competence concerning dependability.</i>

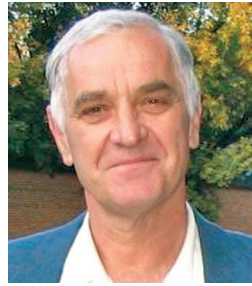
Why did we write in table 4 about competence concerning dependability? The reason is simple: it is necessary that everyone who can anyhow deal with problems of dependability has learned to divide functions (task), performed (solved) by a system, and functions, which are performed by its parts and/or elements. In this conditions both of these definitions inherently coincide. This is what one group of experts believes. The other group believes that the definition in IEC IS admits the interpretation determining not just dependability, but APT; therefore, it is necessary to keep the old definition of dependability in accordance with GOST 27.002-89, and the translation of IEC IS to issue as the draft standard determining the APT concept.

We have stated the arguments reflecting positions of the discussing parties. We have consciously avoided the attempt to give any final recommendations so that experts in the field of dependability, designing, operation, repair of elements, systems, and objects will support this or that version of a dependability definition and terms related to it. The only thing that it would be necessary to add: we understand that the concept of dependability is very wide and whatever side in the given discussion we take, the formalistic approach will not give the correct answer in some cases at any choice. Therefore, in any case we should hope for competence of those who will put dependability terms into practice.

References

1. **Netes V.A., Tarasjev Yu.I., Shper V.L.** Urgent issues of terminology standardization in the field of dependability // Dependability. 2014. # 2.
2. GOST R 27.002-2009. Dependability in technology. Terms and definitions.
3. GOST 27.002-89. Dependability in technology. The basic concepts, terms and definitions.
4. IEC 60050-192/Ed. 1. International Electrotechnical Vocabulary – Part 192: Dependability.
5. Dependability theory in the field of radio electronics. Terminology / Academy of Sciences of the USSR. Committee of technical terminology. Engineering and radio electronic Institute. Collection of recommended terms. Issue 60. – M.: Publishing house of the USSR Academy of Sciences 1962.
6. Dependability of technical systems and products. The basic concepts. Terminology / AS of the USSR. Committee of technical terminology. Committee on dependability and quality assurance of products. Collection of recommended terms. Issue 67. – M.: Publishing house of standards, 1964.
7. GOST 13377-67. Dependability in technology. Terms.
8. GOST 13377-75. Dependability in technology. Terms and definitions.
9. GOST 27.002-83. Dependability in technology. Terms and definitions.
10. **Hosford J.E.** Measures of dependability // Operations Research. 1960. Vol. 8. No 1.
11. **Laprie J.C., Costes A., Troy R.** Dependability: Requirements and Solutions // Proc. SEE Congr. on Electrical and Electronical System Dependability, Toulouse, France, 1979.
12. **Laprie J.C.** Dependable Computing and Fault Tolerance: Concepts and terminology // Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing, 1985.
13. **Fvigiény A., Laprie J.C.** Dependable calculations: from idea to realization in projects // IACTT. 1986. T. 74. No. 5. pp. 8-21.
14. IACTT. Recommendation G.106. Terms and definitions concerning to quality of service, availability and no failure operation // IACTT. Red Book. V. III. Issue III.1. General characteristics of the international calls and circuits. Recommendations G.101-G.181. 1984. pp. 38-93.
15. Dependability and maintenance service AMTC with program management: Reference Manual / **Vegener R.R., Dedoborshch V.G., Zaretskij K.A., etc.; Ed. Dedoborshcha V.G. and Sutorihina N.B.** – M.: Radio and communication 1989.

16. International standard IEC 50-191. The international electrotechnical dictionary. Chapter 191. Dependability and quality of services. 1990.
17. GOST ISO 9000-2011. Systems of a quality management. Fundamentals and the dictionary.
18. GOST R 51901.3-2007 (IEC 60300-2:2004). Risk management. Dependability management guidance.
19. **Ushakov I.A.** Course of the theory of system dependability. – M.: Drofa, 2008.
20. **Netes V.N., Rezinovskij A.J., Tarasjev J.I.**, at al. Degradation instead of harmonization. About the new standard on terminology in the field of dependability // Standards and quality. 2011. No 5. pp. 40-44.
21. Rosstandart Order No.1843 from 29.11.2012 “About stop of application of the national standard and restoration of the interstate standard application in territory of the Russian Federation”
22. Electropedia. Area 191: Dependability and quality of service ([http:// www.electropedia.org/iev/iev.nsf/index? openform*part=191](http://www.electropedia.org/iev/iev.nsf/index?openform*part=191)).
23. An explanatory dictionary of Russian. V. 4 / Ed. **D.N.Ushakov**. – M.: LLC “Publishing house Astrel”, LLC “NSP publishing house”, 2000.
24. **Niv G.** Prostranstvo’s Doctor Deming space: Principles of construction of steady business. – M.: Alpina Business Books, 2005.
25. **Bridgman P.W.** The logic of modern physics. – New York: Macmillan, 1927.



Викторова В.С., Степанянц А.С.

О ПОКАЗАТЕЛЯХ НАДЕЖНОСТИ ТИПА СРЕДНЯЯ НАРАБОТКА

Обсуждаются математические определения показателей средняя наработка до отказа, средняя наработка между отказами и средняя наработка на отказ, приведенные в основной нормативной и теоретической литературе по надежности. Описываются методы практического вычисления показателей при проектном анализе надежности систем. Показана некорректность определения и использования показателя средней наработки на отказ.

Ключевые слова: показатели надежности, средняя наработка до отказа, средняя наработка между отказами, средняя наработка на отказ, марковские модели.

Показатель надежности – техническая характеристика, количественным образом определяющая одно или несколько свойств, составляющих надежность объекта. Показатель надежности количественно характеризует, в какой степени данному объекту или данной группе объектов присущи определенные свойства, обуславливающие надежность. Показатели надежности могут иметь размерность или быть безразмерными. Исследуемые в рамках теории надежности объекты можно разделить на два больших класса – восстанавливаемые и невосстанавливаемые. Показатели надежности также можно разделить на два класса – показатели надежности невосстанавливаемых и восстанавливаемых объектов.

Вопросы выбора основных показателей надежности для различных объектов в достаточной мере проработаны и регламентируются в ГОСТ 27.003-90.

Важным понятием, присутствующим во многих формулировках показателей надежности, является *наработка*. Нарботка это продолжительность или объем работы объекта, т.е. наработка может измеряться не только в единицах времени, но и в единицах выработки продукции, пройденном расстоянии и пр. Например, в одном из зарубежных стандартов по расчету надежности устройств военно-морской техники частотные показатели имеют размерность 1/миллю.

Целью статьи является:

- анализ математических определений показателей средняя наработка до отказа, средняя наработка между отказами и средняя наработка на отказ [1-8];
- выявление допущенной ошибки в математическом определении показателя **средняя наработка на отказ** (это определение сформулировано в основополагающем ГОСТ 27.002-89 и другой литературе);

- обсуждение методов практического вычисления показателя средней наработки на отказ при проектном анализе;
- сравнение всех трех показателей между собой.

Приведем математические определения показателей средняя наработка до отказа, средняя наработка между отказами и средняя наработка на отказ.

1. Средняя наработка объекта до отказа (T_1)

Средняя наработка объекта до отказа определяется как математическое ожидание случайной наработки до первого отказа

$$T_1 = M[\xi_1] = \int_0^{\infty} \tau f(\tau) d\tau = \int_0^{\infty} \tau dQ(\tau) = \int_0^{\infty} P(\tau) d\tau, \quad (1)$$

где ξ_1 – случайная наработка объекта до первого отказа,

$P(t) = P(0, t) = \text{Pr ob}(\xi_1 \geq t) = 1 - F_1(t)$ – вероятность безотказной работы на интервале $(0, t)$,

$F(t)$, $f(t)$ – функция и плотность распределения случайной величины ξ_1 .

Выражение (1), является не только математическим определением, но и реальной вычислительной формулой получения значения показателя.

Этот показатель может характеризовать как невосстанавливаемые, так и восстанавливаемые объекты.

2. Средняя наработка между отказами ($T_{\text{между}}$)

Наработка между отказами (как случайная величина) определяется объемом работы (временем работы) объекта от k -го до $(k+1)$ -го отказа, где $k = 1, 2, \dots$. Отметим, что, во-первых, здесь говорится о **работе** объекта, т.е. время восстановления после k -го отказа не учитывается (поэтому можно говорить после k -го восстановления), а во-вторых, **наработка до первого отказа** не учитывается в данном показателе.

Процесс функционирования восстанавливаемого объекта на стационарном участке представляет собой последовательность чередующихся случайных интервалов работы (ψ_k) и простоя (θ_k) (рис. 1). Простой наступает после отказа объекта, когда над ним проводятся восстановительные операции. Восстановление работоспособности может быть как полным (замена на аналогичный новый объект), так и частичным (например, ремонт только неисправной части).

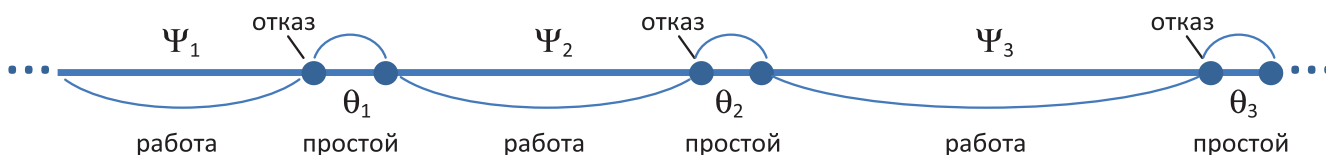


Рис. 1. Стационарный участок функционирования восстанавливаемого объекта

В общем случае, при неполном восстановлении случайные времена ψ_k работы после $k-1$ -го восстановления и до k -го отказа имеют разное распределение с плотностями $f_k(t)$. Если T_k – средняя наработка от момента окончания k -го восстановления до $(k+1)$ -го отказа, то

$$T_{\text{между}} = \lim_{k \rightarrow \infty} M[T_k] = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{i=1}^k T_i, \quad (2)$$

где каждая из средних наработок объекта от момента окончания $k-1$ -го восстановления до k -го отказа определяется как

$$T_k = M[\psi_k] = \int_0^{\infty} t f_k(t) dt. \quad (3)$$

Выражения (2), (3) являются лишь математическим определением, реальные вычисления показателя по ним не проводятся (да это практически и невозможно). Расчетные выражения основываются на вычисленных значениях стационарного коэффициента готовности (K_r) и среднего времени восстановления ($\tau_{восст}$) (если его можно определить), либо стационарных значениях коэффициента готовности и параметра потока отказов (ω). Показатели K_r и ω принципиально вычисляемы многими методами, например, формулами, использующими теоремы для вероятности суммы, произведения событий и теорему полной вероятности, логико-вероятностными, марковскими, асимптотическими. Приведем эти выражения.

Из известного выражения для стационарного коэффициента готовности $K_r = \frac{T_{МЕЖДУ}}{T_{МЕЖДУ} + \tau_{ВОССТ}}$, по вычисленным значениям K_r и $\tau_{восст}$ получаем

$$T_{МЕЖДУ} = \frac{K_r \cdot \tau_{ВОССТ}}{1 - K_r}; \quad (4)$$

Из известных выражений для стационарного коэффициента готовности и параметра потока отказов $\omega = \frac{1}{T_{МЕЖДУ} + \tau_{ВОССТ}}$, по вычисленным значениям K_r и ω получаем

$$T_{МЕЖДУ} = \frac{K_r}{\omega}. \quad (5)$$

Формула (5) совместно с приближенным (при $T_{между} \gg \tau_{восст}$) выражением (6) для вероятности безотказной работы $P(t)$ восстанавливаемых систем обобщает значительную часть результатов асимптотической теории

$$P(t) \approx \exp^{-\frac{t}{T_{МЕЖДУ}}}. \quad (6)$$

Отметим, что $T_{МЕЖДУ} \leq T_1$, так как по определениям для показателей безотказности $P(t)$ и T_1 система начинает функционировать из исправного состояния.

Этот показатель относится только к восстанавливаемым объектам.

3. Средняя наработка на отказ ($T_{на}$)

В нормативной (например, ГОСТ 27.002-89, ГОСТ 27.003-90) и справочной литературе [1] приводится определение ещё одного показателя, относящегося к усреднению наработок, а именно средняя наработка на отказ, который регламентируется как один из основных показателей безотказности для восстанавливаемых объектов,

$$T_{на}(t_n) = \frac{t_n}{M\{n(t_n)\}}, \quad (7)$$

т.е., отношение суммарной наработки объекта (t_n) к математическому ожиданию числа отказов $n(t_n)$ за эту наработку.

Этот показатель внесен в нормативную литературу в начале 80-х годов не в качестве показателя, дополняющего список основных показателей надежности и характеризующего какую-либо особенность применения объекта, которую не отражают другие показатели, а взамен средней наработки между отказами. Приведем результаты критического анализа показателя $T_{на}$.

Показатель $T_{\text{на}}$ является функцией наработки, поэтому нормировать и вычислять его необходимо на заданной наработке, т.е. правильно обозначать его не $T_{\text{на}}$, а $T_{\text{на}}(t_n)$.

Сравним наработку на отказ с другими наработками, фигурирующими в определениях показателей. Средняя наработка до отказа (T_1) характеризует только наработки до первого отказа. Так как все показатели (в нормативной документации) определены для полностью исправного начального состояния объекта, то для распределений с неубывающей функцией интенсивности отказов средняя наработка до первого отказа будет наибольшей. Средняя наработка между отказами ($T_{\text{между}}$) не охватывает наработки до первого отказа, а усредняет (на бесконечности) наработки после первого отказа. Для распределений с неубывающей функцией интенсивности отказов средняя наработка между отказами будет наименьшей. Отметим, что все резервированные структуры имеют возрастающую функцию интенсивности отказов. Средняя наработка на отказ ($T_{\text{на}}(t_n)$) включает в общем случае и наработку до отказа и наработки между отказами. Таким образом, из приведенных объяснений должно следовать следующее соотношение между показателями $T_1 \geq T_{\text{на}}(t_n) \geq T_{\text{между}}$. Но данное неравенство не выполняется, что будет продемонстрировано на примерах.

Методов вычисления $T_{\text{на}}(t_n)$ нет ни в одной известной нам (и частично приведенной в конце книги) литературе. Имеется в виду, что нет четко сформулированного способа получения значений показателя и примеров его вычисления для резервированных восстанавливаемых структур. Связано это с тем, что наработка на заданном календарном времени функционирования объекта является случайной величиной.

Практически всегда, когда нормируется или вычисляется показатель $T_{\text{на}}$ имеется в виду показатель $T_{\text{между}}$ – средняя наработка между отказами, а иногда – средняя наработка до отказа T_1 .

При $t_n \rightarrow \infty$ $T_{\text{на}}(t_n) \rightarrow T_{\text{между}}$, именно поэтому (возможно и не понимая) говорят и пишут $T_{\text{на}}$, хотя определяют его асимптотическое (стационарное) значение, равное $T_{\text{между}}$.

При $t_n \rightarrow 0$ показатель $T_{\text{на}}(t_n)$ растет, в том числе до бесконечности.

Показатель средняя наработка на отказ ($T_{\text{на}}(t_n)$), если и должен присутствовать в нормативной литературе, то только в качестве специального показателя для объектов, функционирующих строго определённую наработку (по истечении которой объект снимается с эксплуатации, даже если не закончено выполнение им определённого задания). Из основных показателей он должен быть убран, а показатель средняя наработка между отказами введен в список основных показателей надежности.

Ещё раз подчеркнем, что практически всегда записывается в требованиях и оценивается при проектном анализе средняя наработка между отказами, а называют её средней наработкой на отказ! **Никогда не указывают наработку, на которой необходимо определить среднюю наработку на отказ.**

В зарубежной нормативной и технической литературе показателя аналогичного $T_{\text{на}}(t_n)$ нет. В стандартах, литературе США, Англии, Германии присутствуют показатели MTTF – среднее время до отказа, который определяется также как и T_1 – средняя наработка до отказа (для показателей безотказности, определяемых до первого отказа, т.е. с поглощением в состояниях, соответствующих отказу, наработка, если она выражена в единицах времени, совпадает со временем до отказа), и показатель MTBF – среднее **время** между отказами. Показатель MTBF равен сумме средней наработки между отказами и среднего времени восстановления $MTBF = T_{\text{между}} + \tau_{\text{восст}}$. У нас часто в литературе, в проектных материалах, требованиях записывают MTBF, но подразумевается и вычисляется $T_{\text{между}}$, что неверно!

Приведем примеры вычисления средней наработки на отказ.

Пример 1

Рассмотрим дублированный блок с восстановлением, марковская модель надежности которого приведена ниже.

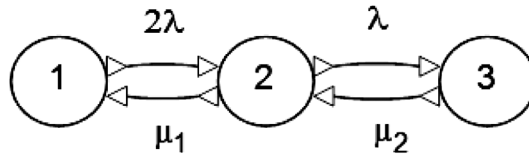


Рис. 2. Марковская модель надежности дублированного блока с восстановлением

Состояние 1 – оба блока работоспособны; состояние 2 – один из блоков отказал, другой работоспособен; состояние 3 – оба блока отказали. Состояния 1 и 2 соответствуют работоспособности резервированной структуры, состояние 3 – отказ резервированной структуры. Интенсивность отказов каждого из блоков равна λ , интенсивность восстановления одного любого блока из состояния 2 равна μ_1 , а из состояния 3 – μ_2 .

Способ вычисления $T_{\text{на}}(t_n)$ состоит в следующем. Получим аналитическое выражение для среднего числа отказов $N_1(t)$ с использованием марковских процессов с доходами (t календарное время функционирования структуры, которое состоит из безотказной наработки t_n и времени пребывания в неработоспособном для структуры состоянии 3). Устремим μ_2 в бесконечность, тогда восстановление из состояния отказа структуры будет мгновенным и время, проведенное в состоянии 3, будет равно нулю. Поэтому всё время моделирования t окажется равным безотказной наработке t_n . Далее проведем вычисления по (7), разделив t на $N_1(t)$.

В конце статьи в приложении кратко изложены основные соотношения по марковским процессам с доходами. Наиболее полно методология марковских процессов с доходами приведена в [9,10].

Система дифференциальных уравнений для среднего числа отказов имеет вид

$$\begin{aligned}\dot{N}_1(t) &= -2\lambda N_1(t) + 2\lambda N_2(t) \\ \dot{N}_2(t) &= \mu_1 N_1(t) - (\lambda + \mu_1) N_2(t) + \lambda N_3(t) + \lambda \\ \dot{N}_3(t) &= \mu_2 N_2(t) - \mu_2 N_3(t).\end{aligned}\quad (8)$$

Напомним (см. приложение), что $N_i(t)$ – среднее число отказов (определяемое выбором матрицы доходов с единицей на месте перехода из состояния 2 в состояние 3 (в матрице W элемент $w_{23}=1$, остальные $w_{ij}=0$)) при условии начального состояния i .

Решая систему уравнений (8), получим неоднородное дифференциальное уравнение третьего порядка

$$\ddot{N}_1(t) + (3\lambda + \mu_1 + \mu_2)\dot{N}_1(t) + (2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2)N_1(t) = 2\lambda^2\mu_2, \quad (9)$$

общее решение которого имеет вид

$$N_1(t) = C_1 + C_2 e^{x_1 t} + C_3 e^{x_2 t} + \frac{2\lambda^2\mu_2 t}{2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2}, \quad (10)$$

где первые три слагаемых с константами C_i и корнями характеристического уравнения $x_0=0$, x_1 , x_2 представляют собой общее решение однородного дифференциального уравнения, соответствующего системе (8), а четвертое слагаемое – частное решение неоднородного уравнения (9).

Исследуя решение (10), константы C_i и корни x_j при $\mu_2 \rightarrow \infty$ получим предельное решение

$$N_1(t) \xrightarrow{\mu_2 \rightarrow \infty} \frac{2\lambda^2 t}{(2\lambda + \mu_1)} + \frac{2\lambda^2}{(2\lambda + \mu_1)^2} e^{-(2\lambda + \mu_1)t} - \frac{2\lambda^2}{(2\lambda + \mu_1)^2}. \quad (11)$$

Приведем выражения (они получены решением алгебраических уравнений обычного марковского процесса) для вычисления показателей T_1 и $T_{\text{между}}$ по модели рис. 2:

$$T_1 = \frac{3\lambda + \mu_1}{2\lambda^2}; \quad K_r = \frac{2\lambda\mu_2 + \mu_1\mu_2}{2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2};$$

$$\omega = \frac{2\lambda^2\mu_2}{2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2}; \quad T_{\text{между}} = \frac{2\lambda + \mu_1}{2\lambda^2}.$$
(12)

Проведем некоторые численные расчеты для $T_{\text{на}}(t_n)$. Пусть $\lambda = 0,001 \text{ час}^{-1}$ (соответствует средней наработке до отказа $T_{\text{до}} = 1000 \text{ час}$), $\mu_1 = 0,1 \text{ час}^{-1}$ (соответствует среднему времени восстановления $\tau_v = 10 \text{ час}$). В таблице 1 приведены значения (в часах) $T_{\text{на}}(t_n)$ для разных t_n , средняя наработка между отказами $T_{\text{между}}$ и средняя наработка до отказа T_1 .

Таблица 1. Результаты расчетов показателей $T_{\text{на}}(t_n)$, $T_{\text{между}}$, T_1

	$t_n = 0,1$	$t_n = 1$	$t_n = 10$	$t_n = 100$	$t_n = 2000$
$T_{\text{на}}(t_n)$	14285714,3	1030927,8	136680,8	56543,2	51252,2
$T_{\text{между}}$	51000				
T_1	51500				

Пример 2

Рассмотрим один восстанавливаемый элемент с экспоненциально распределенными наработкой до отказа (с интенсивностью λ) и временем восстановления (с интенсивностью μ). Приведем формулы для вычисления основных показателей надежности.

Вероятность безотказной работы	$P(t) = e^{-\lambda t}$
Средняя наработка до отказа	$T_1 = T_{\text{до}} = 1/\lambda$
Стационарный коэффициент готовности	$K_r = \mu/(\lambda + \mu)$
Стационарный параметр потока отказов	$\omega = \mu \cdot \lambda/(\lambda + \mu)$
Средняя наработка между отказами	$T = T_{\text{между}} = 1/\lambda;$
Среднее число отказов	$N_1(t) = [\mu \cdot \lambda \cdot t/(\lambda + \mu)] + [\lambda^2/(\lambda + \mu)^2] \cdot [1 - e^{-(\lambda + \mu) \cdot t}]$
Средняя наработка на отказ	$T_{\text{на}}(t_n) = 1/\lambda$, т.к. при $\mu \rightarrow \infty$ $N_1(t) \rightarrow \lambda t$

Для данного примера (одного элемента) $T_1 = T_{\text{на}}(t_n) = T_{\text{между}}$.

Пример 3

Рассмотрим дублированный блок, аналогичный описанному в примере 1, но в данном случае предположим невозможность восстановления в процессе функционирования. А именно, система

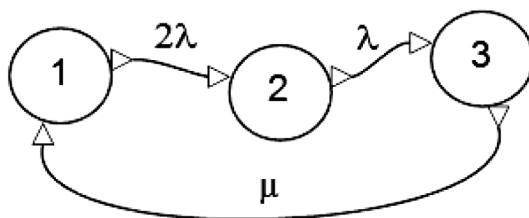


Рис. 3. Марковская модель надежности дублированного блока с восстановлением из состояния отказа

работает до отказа, после чего восстанавливается в полностью исправное состояние. Модель изображена на рис. 3.

Приведем выражения для вычисления показателей T_1 и $T_{\text{между}}$ по модели рис. 3:

$$T_{\text{до}} = \frac{3}{2\lambda}; \quad K_e = \frac{3\mu}{2\lambda + 3\mu}; \quad \omega = \frac{2\lambda\mu}{2\lambda + 3\mu}; \quad T_{\text{между}} = \frac{3}{2\lambda}, \quad (13)$$

т.е. $T_{\text{между}}$ совпадает с $T_{\text{до}}$, что и должно быть, так как все средние наработки между отказами и средняя наработка до первого отказа одинаковые (система после восстановления начинает функционирование всегда из состояния 1).

Для определения $T_{\text{на}}(t_n)$ сделаем то же, что и в примере 1. Система уравнений марковского процесса с доходами для определения среднего числа отказов имеет вид:

$$\begin{aligned} \dot{N}_1 &= -2\lambda \cdot N_1 + 2\lambda \cdot N_2 \\ \dot{N}_2 &= -\lambda \cdot N_2 + \lambda \cdot N_3 + \lambda \\ \dot{N}_3 &= \mu \cdot N_1 - \mu \cdot N_3. \end{aligned} \quad (14)$$

Приведем конечный результат без промежуточных выкладок, тем более, что мы его получим и другим способом. Решая уравнения и устремляя μ к бесконечности, получим

$$N_1(t) \xrightarrow{\mu \rightarrow \infty} \frac{2}{9} e^{-3\lambda \cdot t} + \frac{2}{3} \lambda t - \frac{2}{9}. \quad (15)$$

Продemonстрируем ещё один способ вычисления. Выражение (15) может быть получено и другим способом, если применить результаты теории восстановления. Известна такая модель как *простой процесс восстановления*. Суть этого процесса заключается в том, что новый элемент, начав функционировать в момент $t=0$, при отказе в момент t_1 мгновенно заменяется новым, который, проработав время t_2 и отказав, также мгновенно заменяется следующим и т.д. Плотности распределения времени безотказной работы элементов одинаковы и равны $f(t)$. Для функции восстановления – среднего числа восстановлений за время t – известно выражение (для простого процесса восстановления) в форме преобразования Лапласа [11]. Это выражение имеет вид:

$$N(s) = \frac{f(s)}{s \cdot (1 - f(s))}, \quad (16)$$

где $N(s)$ – преобразование Лапласа от функции восстановления; $f(s)$, s – преобразование Лапласа от плотности распределения и переменная преобразования, соответственно.

Отметим, что, во-первых, все время t является суммарной наработкой, т.к. время восстановления равно нулю, и, во-вторых, число восстановлений равно числу отказов, т.к. момент $t=0$ не считается восстановлением, а момент последнего отказа (в момент t) является и моментом восстановления из-за мгновенного восстановления.

Найдем плотность распределения для примера 3. Так как это обычное дублирование без восстановления из работоспособного состояния с одним отказом, то можно не решать систему дифференциальных уравнений для модели рис. 3 с «поглощающим экраном», а непосредственно написать формулу для функции и плотности распределения $F(t)$, $f(t)$:

$$\begin{aligned} F(t) &= (1 - e^{-\lambda \cdot t})^2 \\ f(t) &= F'(t) = 2\lambda \cdot (1 - e^{-\lambda \cdot t}) \cdot e^{-\lambda \cdot t}. \end{aligned} \quad (17)$$

Преобразование Лапласа от $f(t)$ имеет вид:

$$f(s) = \frac{2\lambda}{s + \lambda} - \frac{2\lambda}{s + 2\lambda}. \quad (18)$$

Подставляя в (16) и делая обратное преобразование Лапласа, получаем

$$N(s) = \frac{2\lambda^2}{s^2 \cdot (s + 3\lambda)} \Rightarrow \frac{2}{9} \cdot e^{-3\lambda \cdot t} + \frac{2}{3} \cdot \lambda t - \frac{2}{9} = N(t), \quad (19)$$

что совпадает с (15) и говорит о правильности подхода с использованием моделей марковских процессов с доходами.

Окончательно для примера 3 имеем:

$$T_{\text{на}} = \frac{t}{\frac{2}{9} \cdot e^{-3\lambda \cdot t} + \frac{2}{3} \cdot \lambda t - \frac{2}{9}}. \quad (20)$$

Очевидно, что при $t \rightarrow \infty$ $T_{\text{на}} \rightarrow (3/2\lambda) = T_{\text{между}} = T_{\text{до}}$. А при $t \rightarrow 0$, $T_{\text{на}} \rightarrow \infty$ (предварительно по правилу Лопиталя продифференцировав числитель и знаменатель).

Приложение А

В Институте Проблем Управления РАН в лаборатории №5 в середине 80-х годов были разработаны для моделирования многоуровневых систем метод и алгоритмы вычисления показателей на основе марковских процессов с доходами [9,10]. Метод марковских процессов с доходами (МПД – метод) в некотором смысле обобщает классический метод марковских процессов с непрерывным временем и дискретным пространством состояний. Его применение позволяет вычислять ряд показателей, вычисление которых в обычных (классических) марковских процессах не может быть осуществлено напрямую.

Приведем основные соотношения для вычисления показателей надежности, технической эффективности. Математическое ожидание дохода $H(t)$ удовлетворяет системе дифференциальных уравнений:

$$\frac{dH(t)}{dt} = \Lambda H(t) + R, \quad (A.1)$$

где $H(t)$ – вектор-столбец математических ожиданий дохода; $H^T(t) = (H_1(t), H_2(t), \dots, H_n(t))$ – транспонированный вектор столбец; n – число состояний системы; $H_i(t)$ – математическое ожидание дохода системы за время функционирования t , если в момент $t=0$ система находилась в состоянии i ; Λ – матрица интенсивности переходов из i -го состояния в j -е.

R – вектор столбец свободных членов:

$$R_i = w_i + \sum_{j, j \neq i} \lambda_{ij} w_{ij}; \quad (A.2)$$

w_{ij} ($i \neq j$) – доход, получаемый в системе при переходе из i -го состояния в j -е;

w_i – доход в единицу времени, если система находится в состоянии i .

Стационарные значения показателей (если они существуют) получают из системы уравнений

$$\Lambda \cdot H + R = 0 \quad (A.3)$$

Специальным выбором матрицы доходов $W=(w_{ij})$ достигается возможность вычисления большого спектра показателей надежности и эффективности (практически любых встречающихся в нормативно-технических документах). Перечислять здесь все виды матрицы доходов для всех показателей мы не будем, это можно посмотреть в [9].

Для примера укажем лишь некоторые:

1. Вероятность отказа Q системы за время t

При вычислении $Q(t)$ необходимо взять матрицу доходов W , у которой элементы столбца (столбцов), соответствующие состоянию (состояниям) отказа системы, равны единице, а все остальные элементы равны нулю. При этом состояния отказа надо сделать поглощающими, поскольку данный показатель характеризует поведение системы до первого попадания ее в состояние отказа. Вычисления проводятся по (A1).

2. Средняя наработка до отказа $T_{ср}$

Матрица W должна иметь диагональные элементы w_{ii} , соответствующие работоспособным состояниям, равные единице, остальные – нулю. Состояния отказа необходимо сделать поглощающими. Так как этот показатель определяется на $(0, \infty)$, то расчет выполняется по (A3).

Первые два показателя вычисляются и в обычных марковских процессах с непрерывным временем, а следующий показатель ($N(t)$) непосредственно без дополнительного интегрирования можно вычислить только с использованием модели с «доходами».

3. Параметр потока отказов $\omega(t)$ и среднее число отказов $N(t)$

Параметр потока отказов $\omega(t)$ является дифференциальным показателем по отношению к интегральному показателю $N(t)$ (среднему числу отказов на $(0, t)$). То есть $\omega(t) = dN(t)/dt$ и определяется в момент t . Вычисление $\omega(t)$ производится в два этапа. Сначала по (A1) определяется $N(t)$. В матрице W для этого необходимо положить элементы w_{ij} равные единице ($i \neq j$), если i – состояние работоспособности, а j – состояние отказа. Остальные элементы равны нулю. Затем полученный вектор $N(t)$ подставляется в (A1) и находят производную, равную в этом случае параметру потока отказов.

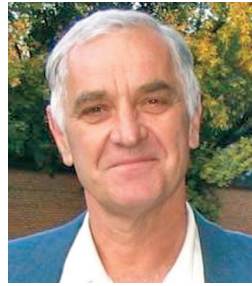
$$\frac{dH(t)}{dt} = \frac{dN(t)}{dt} = \omega(t). \quad (A.4)$$

В модели МПД разработано также вычисление следующих показателей надежности и эффективности (в том числе в многоуровневых моделях системы):

- среднее время восстановления;
- интенсивность отказов системы в момент t ;
- дисперсия (и все другие моменты) времени безотказной работы;
- вероятность пребывания в момент времени t на i -ом уровне функционирования (в двухуровневой модели (работоспособность/отказ) этот показатель является коэффициентом готовности/простоя);
- вероятность застать систему в момент времени t на i -ом уровне функционирования и не опуститься ниже этого уровня за время τ от момента t (в двухуровневой модели этот показатель называется коэффициентом оперативной готовности);
- среднее число переходов с i -го на j -ый уровень работоспособности (в двухуровневой модели среднее число отказов/восстановлений);
- среднее суммарное время пребывания системы на i -ом уровне функционирования на интервале $(0, t)$;
- математическое ожидание эффективности (уровня функционирования) в момент времени t ;
- математическое ожидание интегральной эффективности функционирования на интервале $(0, t)$;
- усредненное значение эффективности функционирования на интервале $(0, t)$;
- коэффициент сохранения эффективности на интервале функционирования $(0, t)$;
- показатели, усредненные на интервале времени $(0, t)$.

Литература

1. Надежность технических систем: Справочник / **Ю.К. Беляев, В.А. Богатырев, В.В. Болотин** и др.; под ред. И.А. Ушакова. М.: Радио и связь, 1985. – 606 с.
2. **Половко А.М., Гуров С.М.** Основы теории надежности. ВНУ- Санкт-Петербург, 2006. – 560 с.
3. **Шубинский И.Б.** Основы анализа сложных систем. – Пушкин: ПВУРЭ, 1988.–206 с.
4. **Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д.** Математические методы в теории надежности. – М.: Наука, 1965. – 524 с.
5. **Дружинин Г.В.** Надежность автоматизированных производственных систем. М.: Энергоатомиздат, 1986. – 480 с.
6. **Рябинин И.А.** Основы теории и расчета судовых электроэнергетических систем. Л.: Судостроение, 1971. – 456 с.
7. **Черкесов Г.Н.** Основы теории надежности автоматизированных систем управления. – Л.: ЛПИ, 1975. – 219 с.
8. **Острейковский В.А.** Теория Надежности. М.: “Высшая Школа”, 2003. – с.463.
9. **Буянов Б.Б., Злобинский В.И., Лубков Н.В., Степанянц А.С.** АСУ ТП. Оценка надежности и эффективности на основе моделей марковских процессов с доходами (МПД-метод). РМ 25431-87, М.: Минприбор, 1987, с.36.
10. **Волик Б.Г., Буянов Б.Б., Лубков Н.В.** и др. Методы анализа и синтеза структур управляющих систем. – М.: Энергоатомиздат, 1988. – 296 с.
11. **Кокс Д.Р., Смит В.Л.** Теория восстановления. – М.: Советское Радио, 1967. – 300 с.



Viktorova V.S., Stepanyants A.S.

DEPENDABILITY INDICES OF MEAN TIME TYPE

The paper discusses mathematical definitions of such dependability indices as mean time to failure, mean time between failures and mean time before failure introduced in basic standards and theoretical literature related to dependability. The paper also describes methods for practical calculation of indices for design analysis of system dependability. It is demonstrated that the definition and use of such parameter as mean time before failure are incorrect.

Keywords: *dependability, mean time to failure, mean time between failures, mean time before failure, Markov models.*

The dependability index is a technical parameter that quantitatively determines one or several properties making up an object's dependability. The dependability index quantitatively describes to what degree certain properties specifying dependability are inherent in the given object or given group of objects. Dependability indices can have dimensions or can be dimensionless. Objects studied within the dependability theory can be divided into two large classes – recoverable and non-recoverable types. Dependability indices can also be divided into two classes – dependability indices of recoverable and non-recoverable objects.

Issues of the selection of basic dependability indices for various objects are sufficiently elaborated and regulated in GOST 27.003-90.

The important concept presented in many formulations of dependability parameters is *operation time*. Operation time is duration or volume of object work, i.e. operating time can be measured not only in time units but also in units of output, traveled distance and so forth. For example, in one of the foreign standards related to calculation of dependability of naval technical equipment, frequency parameters have dimension of 1/mile.

The purpose of the paper consists in the following:

- analysis of mathematical definitions of such indices as mean time to failure, mean time between failures and mean time before failure [1-8];
- identification of a mistake made in the mathematical definition of the index **mean time before failure** (this definition is offered in the generic GOST 27.002-89 and other literature);
- discussion of practical methods for calculation of mean time before failure index at the design analysis stage;
- comparison of all three indices among themselves.

Let us introduce mathematical definitions for such indices as mean time to failure, mean time between failures and mean time before failure.

1. Mean time to failure (T_1)

An object's mean time to failure is defined as expectation of random mean time to the first failure

$$T_1 = M[\xi_1] = \int_0^{\infty} \tau f(\tau) d\tau = \int_0^{\infty} \tau dQ(\tau) = \int_0^{\infty} P(\tau) d\tau, \quad (1)$$

where ξ_1 is an object's random mean time to the first failure, $P(t) = P(0, t) = \text{Prob}(\xi_1 \geq t) = 1 - F_1(t)$ is the probability of mean time to failure in the interval $(0, t)$,

$F(t)$, $f(t)$ is the function and density of random distribution ξ_1 .

Expression (1) is a mathematical definition as well as a real computing formula for obtaining a parameter value.

This parameter can characterize both recoverable and non-recoverable objects.

2. Mean time between failures (T_{between})

Mean time between failures (as a random variable) is defined by a volume of object work (operating time) from the k -th up to $(k+1)$ -th failure, where $k = 1, 2, \dots$. It should be noted that, first, here the definition says about object **operation**, i.e. recovery time after the k -th failure is not taken into account (therefore, it is possible to say "after the k -th recovery"), and second, mean time before the first failure is not taken into account in the given parameter.

Process of recoverable object operation on a stationary section represents a sequence of alternating casual intervals of work (ψ_k) and downtime (fig. 1). Downtimes take place after an object's failure when it undergoes recovery work. Recovery of operability can be complete (replacement by a similar new object) or partial (for example, repair of a faulty part only).

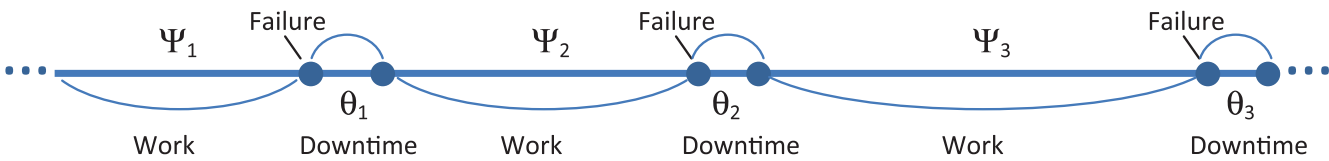


Fig. 1. Stationary section of recoverable object functioning

In general, in case of incomplete recovery, random times ψ_k of work after the $k-1$ -th recovery and up to the k -th failure have a different distribution with densities $f_k(t)$. If T_k is mean time from the moment of termination of the k -th recovery up to $(k+1)$ -th failure, then T_{between} can be expressed as follows

$$T_{\text{between}} = \lim_{k \rightarrow \infty} M[T_k] = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{i=1}^k T_i, \quad (2)$$

where each of mean times of an object from the moment of termination of the $k-1$ -th recovery up to the k -th failure is determined as follows

$$T_k = M[\psi_k] = \int_0^{\infty} t f_k(t) dt. \quad (3)$$

Expressions (2), (3) are just a mathematical definition, real calculations of an index as per them are not carried out (it is practically impossible). Estimated expressions are based on the calculated values of stationary availability (K_A) and mean time to recovery (τ_{recov}) (if it can be determined), or stationary values of availability and parameter of failure rate (ω). Parameters K_A and ω are in essence computable by many methods, for example, by formulas using theorems for the probability of the sum, product of events and the theorem of total probability, and also using logical and probabilistic, Markov and asymptotic techniques. Let us introduce these expressions:

From the known expression for stationary availability $K_A = \frac{T_{\text{BETWEEN}}}{T_{\text{BETWEEN}} + \tau_{\text{RECOV}}}$, by using calculated values of K_A and τ_{recov} we obtain the following:

$$T_{\text{BETWEEN}} = \frac{K_A \cdot \tau_{\text{RECOV}}}{1 - K_A}; \quad (4)$$

From the known expressions for stationary availability and parameter of a failure rate $\omega = \frac{1}{T_{\text{BETWEEN}} + \tau_{\text{RECOV}}}$, by using calculated values of K_A and ω we obtain the value of T_{between} :

$$T_{\text{BETWEEN}} = \frac{K_A}{\omega}. \quad (5)$$

Formula (5) together with approximated (for $T_{\text{between}} \gg \tau_{\text{recov}}$) expression (6) for the probability of non-failure operation $P(t)$ of recoverable systems generalizes a significant part of results in asymptotic theory.

$$P(t) \approx \exp \left(-\frac{t}{T_{\text{BETWEEN}}} \right). \quad (6)$$

It should be noted that $T_{\text{BETWEEN}} \leq T_1$, as by definitions for reliability parameters $P(t)$ and T_1 the system starts to function from the state of operability.

This parameter applies only to recoverable objects.

3. Mean time before failure (T_{before})

Normative (for example, GOST 27.002-89, GOST 27.003-90) and reference literature [1] introduces the definition of one more parameter related to the averaging of operating time, namely mean time before failure which is regulated as one of the basic parameters of dependability for recoverable objects,

$$T_{\text{before}}(t) = \frac{t}{M\{n(t)\}}, \quad (7)$$

i.e., the relation of an object's total operating time (t) to expectation of the failure number $n(t)$ for this operating time.

This parameter was brought in the normative literature in the beginning of 80th not as a parameter supplementing the list of the basic parameters of dependability and describing any feature of object application which is not reflected by other parameters, but instead of mean time between failures. Let us present the results of the critical analysis of parameter T_{before} .

a) Parameter T_{before} is a function of operating time, therefore it should be normalized and calculated for the time, i.e. it would be more correct to designate it as $T_{\text{before}}(t)$ rather than T_{before} .

b) Let us compare mean time before failure with other operating times appearing in definitions of indices. Mean time to failure (T_1) describes only operating time to the first failure. As all parameters (in normative documentation) are determined for completely operable initial state of an object, then mean

time to the first failure will be maximal for distributions with the non-decreasing function of a failure rate. Mean time between failures (T_{between}) does not cover operating times to the first failure, but averages (on infinity) operating times after the first failure. For distributions with the non-decreasing function of a failure rate, mean time between failures will be the smallest one. Note that all reserved structures have the increasing function of a failure rate. Mean time before failure ($T_{\text{before}}(t)$) includes generally both mean time to failure and mean time between failures. Thus, the given explanations should result in the following relations between the considered parameters $T_1 \geq T_{\text{to}}(t) \geq T_{\text{between}}$. But it is not fulfilled and that will be shown by examples.

There are no methods for calculation of $T_{\text{before}}(t)$ in any literature known to us (and referred to partially in the end of the paper). It means that there is no precisely formulated method for obtaining parameter values and examples of its calculation for reserved recoverable structures. It is related to the fact that operating time for specified calendar time of object operation is a random variable.

c) Practically always when parameter T_{before} is normalized or calculated, one keeps in mind T_{between} , i.e. mean time between failures, and sometimes T_1 , i.e. mean time to failure.

d) For $t \rightarrow \infty$, $T_{\text{before}}(t) \rightarrow T_{\text{between}}$, for this reason (probably even not understanding) one says and writes T_{before} , though an asymptotic (stationary) value equal to T_{between} is defined.

e) For $t \rightarrow 0$, parameter $T_{\text{before}}(t)$ grows, to infinity as well.

f) If should be, mean time before failure index ($T_{\text{before}}(t)$) should be present in normative literature only as a special parameter for objects, functioning strictly over certain operating time (after which the object is removed from operation even if it does not finish certain task performance). It should be removed from the basic parameters, and the mean time between failures index should be included into the list of the basic dependability parameters.

Once again it is necessary to emphasize that practically always mean time between failures is specified in requirements and estimated at the design analysis, but it is named as mean time before failure!

You never specify any operating time where it is necessary to define mean time before failure.

In the foreign normative and technical literature there is no parameter similar to $T_{\text{before}}(t)$. In standards and literature of USA, England, Germany there are such parameters as MTTF – mean time to failure which is defined in the same way as T_1 – mean operating time to failure (for the parameters of reliability determined up to the first failure, i.e. with absorption in states corresponding to failure, operating time if it is expressed in terms of time, coincides with mean time to failure), and parameter MTBF – mean time between failures. Parameter MTBF is equal to the sum of mean operating time between failures and mean time of recovery $MTBF = T_{\text{between}} + \tau_{\text{recov}}$. In our literature, in design materials, requirements MTBF is often specified, but T_{between} is meant and calculated, and that is incorrect!

Let us consider the examples of calculation of mean time before failure.

Example 1

Let us consider a redundant unit with recovery, whose Markov model of dependability is presented below

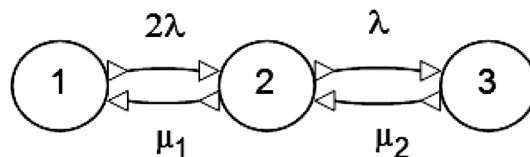


Fig. 2. Markov model for dependability of a redundant unit with recovery

State 1 – both units are in upstate; state 2 – one of the units fails, and the other one is in upstate; state 3 – both units fail. States 1 and 2 correspond to operability of a redundant structure, state 3 – failure of a

redundant structure. Failure rate of each unit is equal to λ , repair rate of any unit in state 2 is equal to μ_1 , and repair rate of any unit in state 3 is equal to μ_2 .

The method of calculation of $T_{\text{before}}(t)$ will consist in the following. First, we shall obtain an analytical expression for the mean number of failures $N_1(t)$ using Markov income processes (t is the calendar time of structure operation, which consists of non-failure operating time t_i and time of being in nonserviceable state 3). Let us head μ_2 for infinity, then recovery from a structure failure state will be instant and time of being in state 3 will be equal to zero. Therefore, all modeling time t will appear to be equal to non-failure operating time t_i . Further we shall carry out calculations as to formula (7) dividing t by $N_1(t)$.

The basic ratios for Markov income processes are briefly stated in the appendix of this paper. In the most detailed way, the methodology of Markov income processes is given in [9,10].

The system of differential equations for the mean number of failures has the following form:

$$\begin{aligned}\dot{N}_1(t) &= -2\lambda N_1(t) + 2\lambda N_2(t) \\ \dot{N}_2(t) &= \mu_1 N_1(t) - (\lambda + \mu_1) N_2(t) + \lambda N_3(t) + \lambda \\ \dot{N}_3(t) &= \mu_2 N_2(t) - \mu_2 N_3(t).\end{aligned}\quad (8)$$

It should be reminded (see Appendix) that $N_i(t)$ is the mean number of failures (determined by a choice of the gain matrix with unit at the point of transition from state 2 into state 3 (in W matrix, element $w_{23}=1$, others $w_{ij}=0$)) for the initial state i .

By solving the system of equations (8), we shall obtain a non-homogeneous differential equation of the third order

$$\ddot{N}_1(t) + (3\lambda + \mu_1 + \mu_2)\dot{N}_1(t) + (2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2)N_1(t) = 2\lambda^2\mu_2, \quad (9)$$

whose common solution has the following form

$$N_1(t) = C_1 + C_2 e^{x_1 t} + C_3 e^{x_2 t} + \frac{2\lambda^2\mu_2 t}{2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2}, \quad (10)$$

where the first three summands with constants C_i and roots of the characteristic equation $x_0=0$, and x_1, x_2 represent the general solution of the homogeneous differential equation corresponding to the system of equations (8), and the fourth summand is the partial solution of heterogeneous equation (9).

By studying solution (10), constants C_i and roots of the characteristic equation x_j for $\mu_2 \rightarrow \infty$ we shall obtain the finite solution

$$N_1(t) \xrightarrow{\mu_2 \rightarrow \infty} \frac{2\lambda^2 t}{(2\lambda + \mu_1)} + \frac{2\lambda^2}{(2\lambda + \mu_1)^2} e^{-(2\lambda + \mu_1)t} - \frac{2\lambda^2}{(2\lambda + \mu_1)^2}. \quad (11)$$

Now we shall give expressions (they are obtained by solving algebraic equations of typical Markov process) for calculation of parameters T_1 and T_{between} using the model presented in fig. 2:

$$\begin{aligned}T_1 &= \frac{3\lambda + \mu_1}{2\lambda^2}; \quad K_r = \frac{2\lambda\mu_2 + \mu_1\mu_2}{2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2}; \\ \omega &= \frac{2\lambda^2\mu_2}{2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2}; \quad T_{\text{междю}} = \frac{2\lambda + \mu_1}{2\lambda^2}.\end{aligned}\quad (12)$$

Let us make some numerical calculations for $T_{\text{before}}(t_t)$. Let $\lambda = 0,001 \text{ hour}^{-1}$ (it corresponds to mean time to failure $T_{\text{to}}=1000 \text{ hour}$), $\mu_1 = 0,1 \text{ hour}^{-1}$ (it corresponds to mean time to repair $\tau_r=10 \text{ hour}$). Values (in hours) of $T_{\text{before}}(t_t)$ for different t_t , mean time between failures T_{between} and mean time to failure T_1 are presented in table 1.

Table 1. Results of calculation of parameters $T_{\text{before}}(t_t)$, T_{between} and T_1

	$t_t = 0,1$	$t_t = 1$	$t_t = 10$	$t_t = 100$	$t_t = 2000$
$T_{\text{before}}(t_t)$	14285714,3	1030927,8	136680,8	56543,2	51252,2
T_{between}	51000				
T_1	51500				

Example 2

Let us consider one recoverable element with exponentially distributed time to failure (with λ rate) and recovery time (with μ rate). Now we shall give formulas for calculation of dependability basic parameters.

Probability of non-failure operation	$P(t) = e^{-\lambda t}$
Mean time to failure	$T_1 = T_{\text{to}} = 1/\lambda$
Stationary availability	$K_a = \mu/(\lambda + \mu)$
Stationary failure rate parameter	$\omega = \mu \cdot \lambda / (\lambda + \mu)$
Mean time between failures	$T = T_{\text{between}} = 1/\lambda$
Mean number of failures	$N_1(t) = [\mu \cdot \lambda \cdot t / (\lambda + \mu)] + [\lambda^2 / (\lambda + \mu)^2] \cdot [1 - e^{-(\lambda + \mu) \cdot t}]$
Mean time before failure	$T_{\text{before}}(t_t) = 1/\lambda$, as for $\mu \rightarrow \infty$ $N_1(t) \rightarrow \lambda t$

For the given example (one element) $T_1 = T_{\text{before}}(t_t) = T_{\text{between}}$.

Example 3

Let us consider a redundant unit similar to the unit described in example 1, but in this case we shall assume impossibility of recovery during functioning. Namely, the system operates before fails, and then recovers into completely operable state. The model is represented in fig. 3.

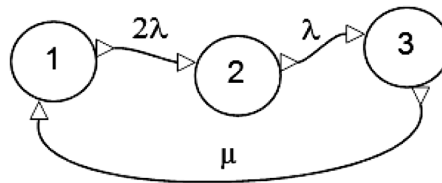


Fig. 3. Markov model of dependability for the redundancy unit with recovery from failure state

Let us give expressions for calculation of parameters T_1 and T_{between} according to the model in fig. 3:

$$T_{\text{oo}} = \frac{3}{2\lambda}; \quad K_e = \frac{3\mu}{2\lambda + 3\mu}; \quad \omega = \frac{2\lambda\mu}{2\lambda + 3\mu}; \quad T_{\text{мезжоду}} = \frac{3}{2\lambda}, \quad (13)$$

i.e. T_{between} coincides with T_{to} , as it should be, since all mean times between failures and mean times to the first failure are identical (the system after recovery always begins operating from state 1).

To define $T_{\text{before}}(t_i)$ we shall make the same, as in example 1. The system of equations of Markov income processes for definition of the failure number has the following form:

$$\begin{aligned}\dot{N}_1 &= -2\lambda \cdot N_1 + 2\lambda \cdot N_2 \\ \dot{N}_2 &= -\lambda \cdot N_2 + \lambda \cdot N_3 + \lambda \\ \dot{N}_3 &= \mu \cdot N_1 - \mu \cdot N_3.\end{aligned}\quad (14)$$

Let us introduce the final result without intermediate calculations, since we shall obtain it by another way as well. By solving the equations and heading μ for infinity, we shall obtain the following:

$$N_1(t) \xrightarrow{\mu \rightarrow \infty} \frac{2}{9} e^{-3\lambda \cdot t} + \frac{2}{3} \lambda t - \frac{2}{9}. \quad (15)$$

Now we will show one more method of calculation. Expression (15) can be obtained by another technique if to apply results of renewal theory. There is a model known as *simple renewal process*. The essence of this process consists in the fact that a new element that started to function at the moment $t=0$, and if failed during the moment t_1 , then it is instantly replaced by a new one, which having worked during the time t_2 and failed, is also instantly replaced by the following new one, etc. Density function of time for elements of non-failure operation is identical and equal to $f(t)$. There is a known expression for renewal function – mean number of recoveries over the time t – (for simple renewal process) in the form of Laplace transform [11]. This expression has the following form:

$$N(s) = \frac{f(s)}{s \cdot (1 - f(s))}, \quad (16)$$

where $N(s)$ is the Laplace transform from renewal function; $f(s)$, s is the Laplace transform from density function and a variable of transformation, accordingly.

It should be noted that, first, the entire time t is total operating time since recovery time is equal to zero, and, second, the number of recoveries is equal to the number of failures since the moment $t=0$ is not considered as recovery, and the moment of last failure (during the moment t) is also the moment of recovery because of instant recovery.

Let us find density of distribution for example 3. As this is usual redundancy without recovery from operable state with one failure, we may not solve a system of differential equations for the model shown in fig. 3 with “absorbing screen” and directly write the formula for the function and density of distribution $F(t)$, $f(t)$:

$$\begin{aligned}F(t) &= (1 - e^{-\lambda \cdot t})^2 \\ f(t) = F'(t) &= 2\lambda \cdot (1 - e^{-\lambda \cdot t}) \cdot e^{-\lambda \cdot t}.\end{aligned}\quad (17)$$

The Laplace transform from $f(t)$ has the following form:

$$f(s) = \frac{2\lambda}{s + \lambda} - \frac{2\lambda}{s + 2\lambda}. \quad (18)$$

By substituting in (16) and making an inverse Laplace transform, we obtain the following

$$N(s) = \frac{2\lambda^2}{s^2 \cdot (s + 3\lambda)} \Rightarrow \frac{2}{9} \cdot e^{-3\lambda \cdot t} + \frac{2}{3} \cdot \lambda t - \frac{2}{9} = N(t), \quad (19)$$

and that coincides with (15) and indicates the correctness of the approach using Markov income process models.

Finally, for example 3 we have:

$$T_{na} = \frac{t}{\frac{2}{9} \cdot e^{-3\lambda \cdot t} + \frac{2}{3} \cdot \lambda t - \frac{2}{9}}. \quad (20)$$

It is obvious that for $t \rightarrow \infty$, $T_{\text{before}} \rightarrow (3/2\lambda) = T_{\text{between}} = T_{\text{to}}$. And for $t \rightarrow 0$, $T_{\text{before}} \rightarrow \infty$ (differentiating the numerator and the denominator before it by L'Hospital rule).

Appendix A

Laboratory No.5 in the Institute of Management of the Russian Academy of Science in the middle of 80th developed the method and algorithms of parameters' calculation for modeling multilevel systems based on Markov income processes [9, 10]. The method of Markov income processes (MIP method) somewhat generalizes the classical method of Markov processes with continuous time and discrete space of states. Its application allows us to calculate a number of parameters, which computation cannot be carried out directly in usual (classical) Markov processes.

Now we shall give the basic relations for calculation of dependability parameters and technical efficiency. The expectation of income $H(t)$ satisfies to the system of differential equations:

$$\frac{dH(t)}{dt} = \Lambda H(t) + R, \quad (A.1)$$

where $H(t)$ is the column vector of income expectation; $H^T(t) = (H_1(t), H_2(t), \dots, H_n(t))$ is the transposed column vector; n is the number of system states; $H_i(t)$ is the expectation of income of the system during the operation time t if during the moment $t=0$ the system was in state i ; Λ is the matrix of transfer rate from the i -th state into the j -th state.

R is the column vector of absolute terms:

$$R_i = w_i + \sum_{j, j \neq i} \lambda_{ij} w_{ij}; \quad (A.2)$$

w_{ij} is the income received in the system at transition from the i -th state into the j -th state;
 w_i is the income per unit of time if the system is in state i .

Stationary values of parameters (if they exist) are obtained from the system of equations

$$\Lambda \cdot H + R = 0. \quad (A.3)$$

The possibility of calculating the large spectrum of dependability parameters and efficiency (practically any parameter, which is met in normative and technical documents) is achieved by a special choice of income matrix $W = (w_{ij})$. We shall not list here all types of income matrixes for all parameters; it can be found in [9].

As an example, we shall note only some parameters:

1. Probability of system failure Q over the time t

For calculation $Q(t)$ it is necessary to take a matrix of incomes W whose elements of columns, corresponding to system failure state are equal to unit value, and all other elements are equal to zero. And failure states should be made absorbing as the given parameter characterizes system behavior to its first failure. Calculations are carried out as to formula (A1).

2. Mean time to failure T_m

Matrix W should have diagonal elements w_{ii} , corresponding to operable states, equal to unit, and other elements are equal to zero. Failure states should be made absorbing. As this parameter is determined by $(0, \infty)$, calculation is carried out as to formula (A3).

The first two parameters are also calculated in common Markov processes with continuous time, and the following parameter ($N(t)$) can be calculated directly without additional integration only with the use of «income» model.

3. Failure rate $\omega(t)$ and mean failure number $N(t)$

Failure rate $\omega(t)$ is a differential parameter in relation to integrated parameter $N(t)$ (to mean failure number for $(0, t)$). That is $\omega(t) = dN(t)/dt$ and it is determined during the moment t . Calculation of $\omega(t)$ is carried out in two stages. First, $N(t)$ is determined as to formula (A1). For this purpose we should put in W matrix elements w_{ij} equal to unit ($i \neq j$), if i is operable state and j is failure state. Other elements are equal to zero. Then, the obtained vector $N(t)$ is substituted in (A1) and a derivative is defined, which in this case is equal to failure rate.

$$\frac{dH(t)}{dt} = \frac{dN(t)}{dt} = \omega(t). \quad (A.4)$$

In MIP model, calculation of the following dependability and efficiency parameters is also developed (including multilevel models of a system):

- mean time of recovery;
- system failure rate at the moment t ;
- dispersion (and all other moments) of time of non-failure operation;
- probability of being at the i -th level of functioning at the moment of time t (in two-level model (operability/failure) this parameter is availability/unavailability (downtime));
- probability to find a system at the i -th level of functioning at the moment of time t and not to step down below this level in time τ from the moment t (in two-level model, this parameter refers to operational availability);
- mean number of transitions from the i -th onto the j -th level of operability (in two-level model, this parameter refers to mean number of failures /recoveries);
- mean total time of a system being at the i -th level of functioning on the interval $(0, t)$;
- expectation of efficiency (level of functioning) at the moment of time t ;
- expectation of integral efficiency of functioning on the interval $(0, t)$;
- value of functioning efficiency averaged on the interval $(0, t)$;
- factor of efficiency retention on the interval of functioning $(0, t)$;
- parameters averaged on the interval of time $(0, t)$.

References

1. Dependability of engineering systems/ Reference book / **Y.K. Belyaev, V.A. Bogatyryov, V.V. Bolotin, etc.**; ed **I.A. Ushakov. M.**: Radio and communication, 1985. – 606 p.
2. **Polovko A.M., Gurov S.M.** Fundamentals of dependability theory. BHV-Saint Petersburg, 2006. – 560 p.
3. **Shubinsky I.B.** Fundamentals of complex systems analysis. – Pushkin: PVURE, 1988.-206 p.
4. **Gnedenko B.V., Beljaev J.K., Solobiev A.D.** Mathematical methods in the theory of dependability. – M.: Science, 1965. – 524 p.

5. **Druzhinin G.V.** Dependability of automated production systems. M.: Energoatomizdat, 1986. – 480 p.
6. **Ryabinin I.A.** Fundamentals of the theory and calculation of ship electrical power systems. L.: Shipbuilding, 1971. – 456 p.
7. **Cherkesov G.N.** Fundamentals of dependability theory of the automated control systems. – L.: LPI, 1975. – 219 p.
8. **Ostreykovsky V.A.** Dependability theory. M.: “Higher school”, 2003. – 463p.
9. **Buyanov B.B., Zlobinske V.I., Lubkov N.V., Stepanyants A.S.** Industrial control. Dependability and efficiency estimation based on models of Markov processes with incomes (MPI-method). PM 25431-87, M.: Minpribor, 1987, p. 36.
10. **Volik B.G., Buyanov B.B., Lubkov N.V., etc.** Methods of analysis and synthesis of structures of management systems. – M.: Energoizdat, 1988. – 296 p.
11. **Koks D.R., Smith V.L.** Renewal theory. – M.: the Soviet Radio, 1967. – 300 p.



Майстренко И.Ю., Юсупов И.И., Зиннуров Т.А.

АНАЛИЗ ПРОЕКТНОЙ НАДЕЖНОСТИ ОТВЕТСТВЕННЫХ УЗЛОВ АРОЧНОГО ПРОЛЕТНОГО СТРОЕНИЯ ПЕШЕХОДНОГО ПУТЕПРОВОДА НА ОСНОВЕ ЧИСЛЕННЫХ И ИМИТАЦИОННЫХ МЕТОДОВ

В данной работе рассматривается анализ проектной надежности узла сопряжения «арка – затяжка – домкратная балка» в пролетном строении проектируемого пешеходного путепровода. При оценке надежности, потребовалось выполнение ряда отдельных процедур имитационного эксперимента, который включает в себя пять основных ступеней. Критерием принятия решения об отказе являлось исчерпание удельной прочности в одном из элементов ответственного узла «арка – затяжка – домкратная балка».

Ключевые слова: проектная надёжность, имитационный эксперимент, пешеходный путепровод, нагрузки, доверительные интервалы.

Введение

Уровень надежности конструктивной системы обычно выбирается на стадии концепции и формирования требований к продукции. При проектировании мостовых конструкций в черте крупных городов конструирование, как правило, ведут с учетом создания архитектурной выразительности сооружений, что неизбежно приводит к намеренному усложнению узлов сопряжений отдельных элементов. Это обстоятельство влечет необходимость всестороннего обоснования принятых проектных решений, так как ошибочные конструктивные решения могут приводить к катастрофическим последствиям с большим числом пострадавших.

В данной работе приведены результаты анализа надежности на стадии компоновки ответственного узла сопряжения «арка – затяжка – домкратная балка» в пролетном строении пешеходного путепровода на дороге I-ой технической категории в Московской области. По конструктивному решению пролетная часть пешеходного перехода выполнена в виде однопролетной наклонной арки переменного коробчатого сечения размером от 1600х500 мм до 1000х500 мм с подвесками из трубы $\varnothing 203 \times 10$ мм, в поперечном сечении две плоскости арок имеют наклон внутрь на 14 градусов к вертикали, домкратная балка коробчатого сечения размером 750х1000 мм. Длина арочного пролета пешеходного перехода составляет 77 м, ширина проходной части 4 м. Для изготовления конструктивных элементов узла сопряжения «арка – затяжка – домкратная балка» используется сталь 15ХСНД по ГОСТ 6713. Проектный срок службы сооружения не менее 100 лет.

Для анализа проектной надежности узла сопряжения «арка – затяжка – домкратная балка» в пролетном строении проектируемого пешеходного путепровода потребовалось выполнение ряда отдельных процедур, включающих пять основных ступеней.

На **первой ступени**, с использованием детерминированных характеристик входных параметров, выполнена оценка ожидаемых границ изменчивости нагрузок на основе метода доверительных интервалов с надежностью $\beta = 0,995$. Статистические характеристики отдельных компонент нагрузок получены на основе статистической информации, обобщенной в работах [1, 2], и общих правил применения нормативных значений и системы коэффициентов в разрешающих уравнениях метода предельных состояний, изложенных в работах [3, 4].

Для получения границ изменчивости суммарной постоянной нагрузки авторами проведен комплекс имитационных экспериментов. В ходе многократных прогонов имитационной модели для создания выборок из реализаций случайных величин отдельных компонент постоянной нагрузки использованы генераторы случайных чисел вычислительной системы MathCAD и разработанные авторами программные модули во взаимодействии с рациональными алгоритмами построчной трансформации числовых множеств, преимущества которых доказаны в работе [5]. На основании проведенного комплекса имитационных экспериментов, к дальнейшему расчету приняты наиболее невыгодные границы изменчивости суммарной постоянной нагрузки $[q_{\Sigma, \text{inf}}; q_{\Sigma, \text{sup}}] \sim F_{q_{\Sigma}} [60,69; 83,91] \text{ кН/м}$.

Ожидаемые границы изменчивости временной нагрузки от пешеходов представлены интервалом $[p_{\text{inf}}; p_{\text{sup}}] \sim F_p [3,15; 28,85] \text{ кН/м}$. Ожидаемые границы изменчивости прочих нагрузок [6, 7] оценены интервалами: ветровое давление для района строительства $[w_{0, \text{inf}}; w_{0, \text{sup}}] \sim F_w [0,000; 1,581] \text{ кН/м}^2$; вес снегового покрова – $[S_{0, \text{inf}}; S_{0, \text{sup}}] \sim F_S [0,096 \cdot \mu; 1,864 \cdot \mu] \text{ кН/м}^2$, μ – коэффициент перехода от веса снегового покрова земли к снеговой нагрузке.

На **второй ступени**, с использованием ожидаемых границ изменчивости нагрузок, полученных на первой ступени, методом конечного элемента в перемещениях в программном комплексе «ЛИРА», выполнен комплекс статических расчетов пролетного строения пешеходного путепровода. При оценке напряженно-деформированного состояния (НДС) узла сопряжения «арка – затяжка – домкратная балка» учитывались компоненты напряженного состояния в самих элементах

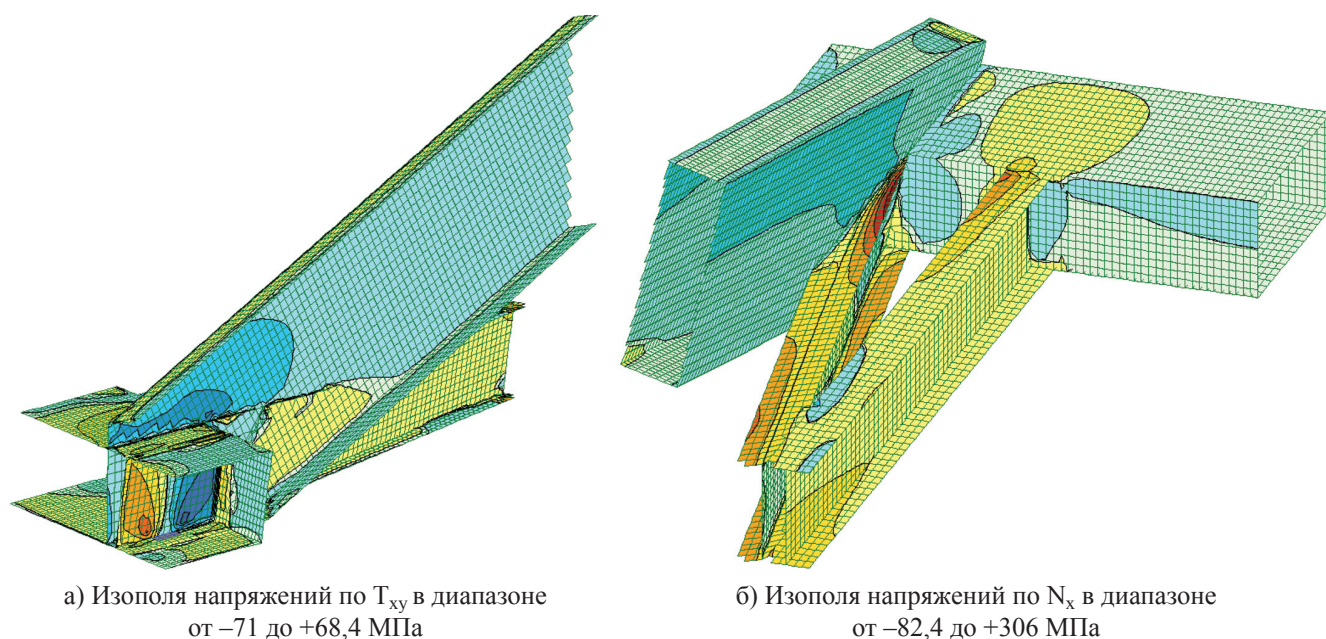


Рис. 1. Фрагменты отдельных вариантов загрузок с изополями напряжений в элементах узла сопряжения «арка – затяжка – домкратная балка»

сопряжения и в прилегающих к ним участках: верхний и нижний пояса арки, верхний и нижний пояса затяжки, нижний пояс и стенка (диафрагма) домкратной балки, элементы поперечных связей в опорном сечении. В комплексе статических расчетов задействовано 138 наиболее характерных комбинаций загрузки, как отдельными видами нагрузок, так и их возможными сочетаниями в пределах ожидаемых границ изменчивости.

На рис. 1 приведены фрагменты отдельных загрузок с изополями напряжений в элементах узла сопряжения «арка – затяжка – домкратная балка».

На **третьей ступени** проведен статистический анализ результатов оценки НДС узла сопряжения «арка – затяжка – домкратная балка» на основании выборочных данных, полученных в ходе задействованных на второй ступени комбинаций загрузки.

Таблица 1. Статистические характеристики отдельных компонент НДС в узлах сопряжения «арка – затяжка – домкратная балка»

№ п.п.	Компоненты НДС	Статистические характеристики						
		Объем выборки	Среднее арифметическое значение	Среднее квадратическое отклонение	Коэффициент вариации	Экспесс множества	Наименьшее значение	Наибольшее значение
1.	Нормальные напряжения вдоль вертикальной оси	138	122,4 МПа	23,9 МПа	0,195	–0,857	90,0 МПа	155,6 МПа
2.	Нормальные напряжения вдоль горизонтальной оси	138	130,1 МПа	27,1 МПа	0,208	–0,832	102,0 МПа	174,9 МПа
3.	Касательные напряжения	138	82,3 МПа	17,3 МПа	0,210	–0,838	58,0 МПа	90,4 МПа

Общий взгляд на полученные статистические характеристики отдельных компонент НДС (табл. 1) показывает, что имеет место деформация формы итогового распределения вероятностей в части её сравнения со статистическими характеристиками для нормального закона распределения случайной величины.

Для оценки вероятности возможных «выбросов» случайной величины каждого k -го промежуточного параметра (отдельной компоненты НДС) за уровень невыгодной границы энтропийного интервала неопределенности, авторами разработаны логические и аналитические программные модули в среде MathCAD. Для этого рассчитана частота $\phi_k | N$ ожидаемых «выбросов» случайной величины k -го параметра, которая определялась путем регистрации случаев отдельных превышений i -ых реализаций k -го параметра $\sigma_{k,i}(N)$ уровня верхней границы энтропийного интервала неопределенности $\sigma_{k,sup}$ для того же параметра в течение имитационного эксперимента объемом N :

$$\phi_k | N = \frac{n_k | (\sigma_{k,i}(N) > \sigma_{k,sup})}{N}, \quad (1)$$

$$\sigma_{k,sup} = \bar{\sigma}_k + \epsilon_{k,\beta}, \quad (2)$$

где $\epsilon_{k,\beta}$ – точность оценки k -го параметра, рассчитанная с достоверностью β .

С использованием статистических характеристик отдельных компонент НДС в узлах сопряжения «арка – затяжка – домкратная балка» (табл. 1) проведены тестовые прогоны имитационных моделей для определения требуемого объема моделирования напряжений в расчетных сечениях. Объем исходных числовых множеств (отдельных компонент НДС) задан на уровне $N \sim 10^4 \dots 10^7$ реализаций. В качестве критерия, подтверждающего адекватность принятой имитационной модели, принята сходимость по вероятности P_β :

$$\phi_k | N \xrightarrow{P_\beta} Q_{k,\lim}(t), t \leq T_\Theta, \quad (3)$$

где $Q_{\lim}(t)$ – предельное значение фактора риска, оцениваемое исходя из требований к сохранению надежности системы за время эксплуатации t в пределах ожидаемого проектного срока службы сооружения T_Θ .

Тестовые прогоны имитационных моделей показали, что для удовлетворения требований к адекватности плана имитационного эксперимента требуется искусственно регулировать объем исходных числовых множеств N , зависящий от принимаемого уровня достоверности расчетного параметра. В рамках решения задачи исследования к дальнейшей разработке принят план имитационного эксперимента с объемом исходных числовых множеств $N = 10^7$ реализаций при уровне достоверности $\beta = 0,995$, при этом требование к предельному значению фактора риска на уровне $Q_{\lim}(t) = 5 \cdot 10^{-6}$ соблюдается.

На **четвертой ступени** проведен комплекс имитационных экспериментов по оценке проектной надежности узла сопряжения «арка – затяжка – домкратная балка» по критерию отказа вследствие исчерпания удельной прочности. Под отказом понимается событие, состоящее в превышении значения случайной реализации отдельных или совместно действующих напряжений в расчетных сечениях над случайной реализацией значения удельной прочности материала.

Предварительно, после изучения результатов статистических исследований механических свойств использованного конструкционного материала, к дальнейшему использованию приняты статистические данные 969 контрольных испытаний на растяжение стандартных образцов, представленных в работе [8]. В комплексе имитационных экспериментов по оценке надежности узла сопряжения «арка – затяжка – домкратная балка» использованная сталь 15ХСНД представлена следующими статистическими характеристиками: предел текучести – выборочное среднее 386,9 МПа, коэффициент вариации 0,0835, стандартное отклонение 32,4 МПа; временное сопротивление – выборочное среднее 558,5 МПа, коэффициент вариации 0,0745, стандартное отклонение 41,7 МПа.

Таблица 2. Расчетные интервальные оценки для компонентов НДС узла сопряжения

№ п.п.	Компоненты НДС	Расчетные интервальные оценки	
		Нижняя граница (inf)	Верхняя граница (sup)
1.	Нормальные напряжения вдоль вертикальной оси, $\sigma_x \sim f[\sigma_{x,\text{inf}}; \sigma_{x,\text{sup}}]$	90,0 МПа	280,9
2.	Нормальные напряжения вдоль горизонтальной оси, $\sigma_y \sim f[\sigma_{y,\text{inf}}; \sigma_{y,\text{sup}}]$	102,0 МПа	590,6
3.	Касательные напряжения, $\tau_{xy} \sim f[\tau_{xy,\text{inf}}; \tau_{xy,\text{sup}}]$	58,0 МПа	183,5

Для решения задач этой ступени с использованием результатов статистического анализа результатов оценки НДС рассматриваемого узла сопряжения, полученных на третьей ступени расчета, составлены расчетные интервальные оценки для компонентов НДС в соответствие принятого

плана имитационного эксперимента (табл. 2). При этом нижняя граница принята по наименьшему значению соответствующей компоненты НДС (см. табл. 1), которое получено при загрузке только постоянными нагрузками, а верхняя граница рассчитана исходя из характеристик плана имитационного эксперимента (по верхней границе доверительного интервала с обеспеченностью 0,995 при объеме выборки 138, квантиль 2,853, число прогонов модели 400).

Условие оценки по критерию отказа вследствие истощения удельной прочности:

$$Q_{\Omega} \Rightarrow \begin{cases} R_y(j) < \sigma_x(j) \\ R_y(j) < \sigma_y(j) \\ R_s(j) < \tau_{xy}(j) \\ R_y(j) < \sqrt{[\sigma_x(j)^2 - \sigma_x(j) \cdot \sigma_y(j) + \sigma_y(j)^2 + 3 \cdot \tau_{xy}(j)^2]} \end{cases}, \text{ при } j \in [1; N], \quad (4)$$

где $R_y(j)$, $R_s(j) = 0,58 \cdot R_s(j)$ – массивы случайных реализаций предела текучести и сопротивления стали сдвигу; $\sigma_x(j)$, $\sigma_y(j)$, $\tau_{xy}(j)$ – массивы случайных реализаций отдельных компонент НДС (нормальных и касательных напряжений).

В результате проведения имитационного эксперимента по оценке проектной надежности узла сопряжения «арка – затяжка – домкратная балка» по критерию отказа вследствие истощения удельной прочности не выявлено случаев превышения значений случайных реализаций отдельно моделируемых нормальных и касательных напряжений над случайными реализациями значений удельной прочности материала. Установлено, что при учете совместного действия напряжений в ходе оценки по четвертой модели в условии (4), наблюдается устойчивая регистрация отказов с наибольшей частотой появления $2,4 \cdot 10^{-6}$, что не противоречит предельному значению фактора риска на уровне $Q_{\lim}(t) = 5 \cdot 10^{-6}$.

Таким образом, с позиции достаточности показателей надежности для стадии проектирования, можно оставить принятые конструктивные решения без изменений.

На **пятой ступени** проведен комплекс имитационных экспериментов по оценке возможной изменчивости показателей надежности узла сопряжения «арка – затяжка – домкратная балка» на стадии эксплуатации.

Очевидно, что при эксплуатации технической системы неизбежно влияние различных неблагоприятных процессов (например, деградация элементов, недостаточно качественное и/или несвоевременное выполнение ремонтно-восстановительных мероприятий). Как правило, на этапе проектирования конструктор сталкивается с некоторыми внешне непреодолимыми сложностями, в частности, с самим отсутствием проектируемой конструкции, а иногда и с отсутствием её аналогов. В таких условиях дать идеальный прогноз изменения надежности системы за проектный срок службы затруднительно, а порой и невозможно. Для решения задач этой ступени использованы аналитические модели формализации процесса изменчивости показателей надежности, изложенные в работе [9], а также модели описания процессов износа стальных конструкций в смежных областях науки, например, в работе [10].

При разработке модели изменчивости показателей надежности в течение проектного срока эксплуатации важным показателем является конечное значение определяющего показателя надежности (например, вероятность отказа) к моменту истощения ресурса безопасной эксплуатации. Запишем условие, при котором техническая система не истощила свой ресурс за время эксплуатации t :

$$Q_{\Omega}(t) \leq [Q(t)], \quad t \leq T_{\Theta}, \quad (5)$$

где $Q_{\Omega}(t)$ – вероятность опасных отказов по предельному состоянию с условием Ω ; $[Q(t)]$ – допустимое значение вероятности рассматриваемого отказа.

С учетом условия (5) формула оценки (4) по критерию отказа вследствие исчерпания удельной прочности переписывается в виде:

$$\{Q_{lim}(t)\} \leq Q_{\Omega}(t) \Rightarrow \begin{cases} R_{yt}(j) < \sigma_{xt}(j) \\ R_{yt}(j) < \sigma_{yt}(j) \\ R_{st}(j) < \tau_{xyt}(j) \\ R_{yt}(j) < \sqrt{[\sigma_{xt}(j)^2 - \sigma_{xt}(j) \cdot \sigma_{yt}(j) + \sigma_{yt}(j)^2 + 3 \cdot \tau_{xyt}(j)^2]} \end{cases}, \quad (6)$$

где $R_{yt}(j)$, $R_{st}(j)$ – области случайных реализаций предела текучести и сопротивления стали сдвигу с разверткой во времени t ; $\sigma_{xt}(j)$, $\sigma_{yt}(j)$, $\tau_{xyt}(j)$ – тоже, отдельных компонент НДС.

Рассмотрим простую линейную модель, характеризующую изменчивость отдельного i -го расчетного параметра, входящего в формулы (4):

$$\Phi_i(t) = \Phi_{i,0} \cdot (1 + t \cdot \Delta_i), \quad (7)$$

где $\Phi_{i,0}$ – значение отдельного i -го расчетного параметра в начальный момент времени ($t=0$); $\Delta_i = \frac{d}{dt} \Phi_i(t)$ – комплексный показатель, учитывающий влияние различных неблагоприятных процессов во времени t в пределах ожидаемого проектного срока службы сооружения.

На примере рассматриваемого узла сопряжения «арка – затяжка – домкратная балка» в пролетном строении пешеходного путепровода, рассмотрены различные значения комплексного показателя Δ_i , принятые в диапазоне значений $1 \cdot 10^{-4} \dots 5 \cdot 10^{-5}$, с использованием которых, выполнен комплекс имитационных экспериментов для определения изменчивости вероятности отказов системы во времени (рис. 2).

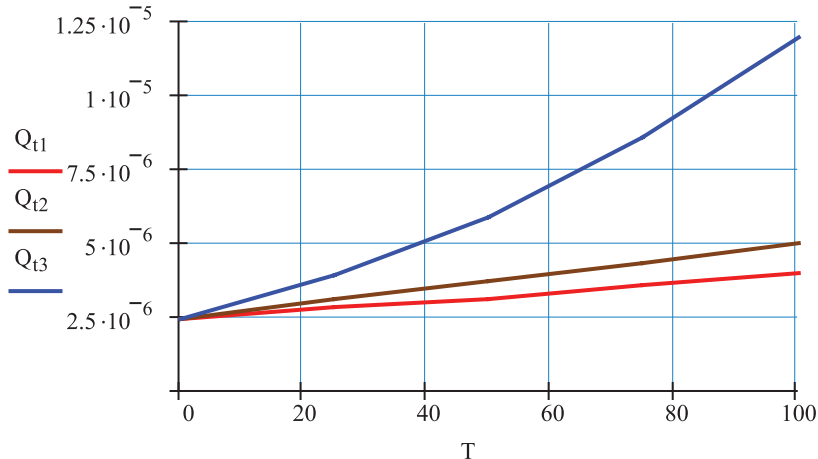


Рис. 2. Графики изменчивости вероятности отказов системы во времени T в зависимости от принятого значения комплексного показателя Δ_i , при $\Delta_i = 5 \cdot 10^{-4}$ вероятность отказов Q_{t1} , при $\Delta_i = 2.5 \cdot 10^{-4}$ – Q_{t2} и при $\Delta_i = 1 \cdot 10^{-4}$ – Q_{t3}

Полученные результаты показали, что для сохранения показателей надежности на стадии эксплуатации при неизменности принятых конструктивных решений, изменчивость расчетных параметров во времени (увеличение напряжений) не должно превышать $\Delta_i = 2.5 \cdot 10^{-4}$ в год.

Выводы

По результатам проведенного анализа надежности ответственного узла сопряжения «арка – затяжка – домкратная балка» в пролетном строении пешеходного путепровода установлено, что при

уровне достоверности расчетных оценок $\beta = 0,995$, вид отказа по критерию исчерпания удельной прочности одного из элементов характеризуется как практически невероятный отказ.

Для критерия исчерпания удельной прочности от совместного действия напряжений в узлах сопряжения «арка – затяжка – домкратная балка» при имитации их загрузки характерными комбинациями внешних воздействий наблюдается устойчивая регистрация отказов с наибольшей частотой появления $2,4 \cdot 10^{-6}$, что не противоречит предельному значению фактора риска на уровне $Q_{\text{lim}}(t) = 5 \cdot 10^{-6}$.

Для оценки надёжности авторами были разработаны и апробированы на конкретной инженерной задаче специальные алгоритмы, основанные на структурных, статистических и имитационных методах, а также на приемах регрессионного анализа, позволяющие оценивать как проектную надёжность, так и прогнозировать допустимый уровень изменчивости показателей надёжности на стадии эксплуатации системы в зависимости от ответственности решаемой задачи.

Литература

1. **Манапов А.З.** Расчет надёжности и ресурса строительных конструкций методом статистического моделирования: Учебное пособие. Казань: КГАСУ, 2010. – 131 с.
2. Пособие по проектированию стальных конструкций (к СНиП II-23-81 «Стальные конструкции») / ЦНИИСК им. Кучеренко Госстроя СССР. – М.: ЦИТП Госстроя СССР, 1989. – 148 с.
3. **Шпете Г.** Надёжность несущих строительных конструкций / Пер. с нем. О.О. Андреева. – М.: Стройиздат, 1994. – 288 с.
4. **Райзер В.Д.** Методы теории надёжности в задачах нормирования расчетных параметров строительных конструкций / В.Д. Райзер; науч. изд. – М.: Стройиздат, 1986. – 192 с.
5. **Майстренко И.Ю., Манапов А.З.** Статистическое моделирование работы строительных конструкций методом Монте-Карло. Работа с числовыми множествами // Известия КГАСУ № 2 (20), 2012. – С. 84-93.
6. Свод правил СП.35.13339.2011. Мосты и трубы. Актуализированная редакция СНиП 2.05.03-84* // Утвержден Приказом Минрегиона России от 28 декабря 2010 г. №82.
7. Свод правил СП 20.13330.2011. Нагрузки и воздействия. Актуализированная редакция СНиП 2.01.07-85* // Утвержден Приказом Минрегиона России от 27 декабря 2010 г. №787.
8. **Кошутин Б.Н., Уваров Б.Ю.** Статистическое исследование механических свойств некоторых строительных сталей // Сб. трудов №96 МИСИ им. В.В. Куйбышева / Под. Общ. ред. Е.И. Беленя. – М., 1973. – С. 13-22.
9. **Майстренко И.Ю., Манапов А.З.** Моделирование процесса изменения во времени уровня надёжности конструктивной системы // Известия КазГАСУ № 1 (13), 2010. – С. 132-140.
10. Долговечность стальных конструкций в условиях реконструкции / **Е.В. Горохов, Я. Брудка, М. Лубиньски** и др.; Под ред. Е.В. Горохова. – М.: Стройиздат, 1994. – 488 с.



Maystrenko I.Y., Zinnurov T.A., Yusupov I.I.

ANALYSIS OF DESIGN DEPENDABILITY OF CRITICAL UNITS OF ARCH SPANS OF PEDESTRIAN OVERPASSES BASED ON NUMERICAL AND SIMULATION METHODS

The paper deals with the design dependability of the grip-arm interface “arch – bowstring – jack beam” in spans of pedestrian overpasses. Dependability estimation required the performance of a number of simulation procedures that include five basic steps. Exhaustion of weight strength in one of the critical element of the arch – bowstring – jack beam joint was the criterion of making a decision about failure.

Keywords: design dependability, simulation, pedestrian overpass, load, confidence interval.

Introduction

The level of constructive system dependability is usually selected at the concept and requirements specification stage. Designing bridges for large cities generally involves the requirement of aesthetic expressiveness that inevitably leads to the intentional complication of junctions. That, in turn, requires comprehensive substantiation of the adopted design decisions, design flaws can lead to catastrophic consequences with large casualties.

This paper presents the results of dependability analysis at the stage of arrangement of the critical joint “arch – bowstring – jack beam” in spans of a designed pedestrian overpass on a road of the first engineering category in the Moscow Region. According to the construction solution, a span of the pedestrian overpass is implemented as a single-span inclined arch of variable box-shaped section with dimensions from 1600x500 mm to 1000x500 mm with pipe hangers of 203x10 mm. In cross-section, the two planes of arches have an inward tilt of 14 degrees to vertical. The jack beam is box shaped and measures 750x1000 mm. The length of arch span of the pedestrian overpass is 77 m, the walking part is 4 m in width. Structural components of the critical joint “arch – bowstring – jack beam” are made of 15HSND steel as per GOST 6713. The designed service life of the structure is not less than 100 years.

The analysis of the design dependability of the critical arch – bowstring – jack beam joint in spans of a designed pedestrian overpass required the performance of a number of procedures that included five basic steps.

At the first step, using determined input parameters, an estimation of expected boundaries of loads' variability was carried out based on the method of confidence intervals with validity $\beta = 0,995$. Statistical characteristics of individual load components were obtained based on statistical information generalized

in studies [1, 2], as well as the general rules of application of normative values and system of factors in the allowing equations of the limiting conditions method stated in studies [3, 4].

In order to identify the boundaries of variation of the total constant load, the authors carried out a series of simulations. Over a number of repeated simulations, in order to create samples of realizations of random variables of constant load components, MathCAD random numbers generators and program modules developed by the authors were used along with rational algorithms of line-by-line transformation of numerical sets the advantages of which are outlined in [5]. Upon the performance of the series of simulations, the most disadvantageous boundaries of variation of total constant load $[q_{\Sigma, \text{inf}}; q_{\Sigma, \text{sup}}] \sim F_{q\Sigma}$ [60,69; 83,91] kN/m were chosen for subsequent calculation.

The expected boundaries of variation of live load from pedestrians are presented by an interval $[p_{\text{inf}}; p_{\text{sup}}] \sim F_p$ [3,15; 28,85] N/m. The expected boundaries of variation of other loads [6, 7] are estimated within the following intervals: wind pressure in the construction area $[w_{0, \text{inf}}; w_{0, \text{sup}}] \sim F_w$ [0,000; 1,581] kN/m²; weight of snow $[S_{0, \text{inf}}; S_{0, \text{sup}}] \sim F_s$ [0,096· μ ; 1,864· μ] kN/m², μ being the factor of transit from weight of snow cover to snow load.

At the second step, using the expected boundaries of variation of loads obtained at the first step, as well as finite element displacement method in the LIRA software system, a set of static calculations of spans of pedestrian overpass was executed. In order to evaluate the stress-strain state (SSS) of the arch – bowstring – jack beam joint, account was taken of stress components in elements of the joint and in adjacent elements: top and bottom booms of the arch, top and bottom chords of the bowstring, bottom zone and the wall (diaphragm) of the jack beam, elements of bowstrings in the supporting section. 138 most typical combinations of loading are involved in the set of static calculations, both individual loads, and their possible combinations within the limits of expected boundaries of variation.

Fig. 1 shows fragments of individual loadings with stress izofields in elements of the arch – bowstring – jack beam joint.

At the third step, a statistical analysis of SSS estimation results of the arch – bowstring – jack beam joint is carried out based on the selective data obtained from the loading combinations at the second step.

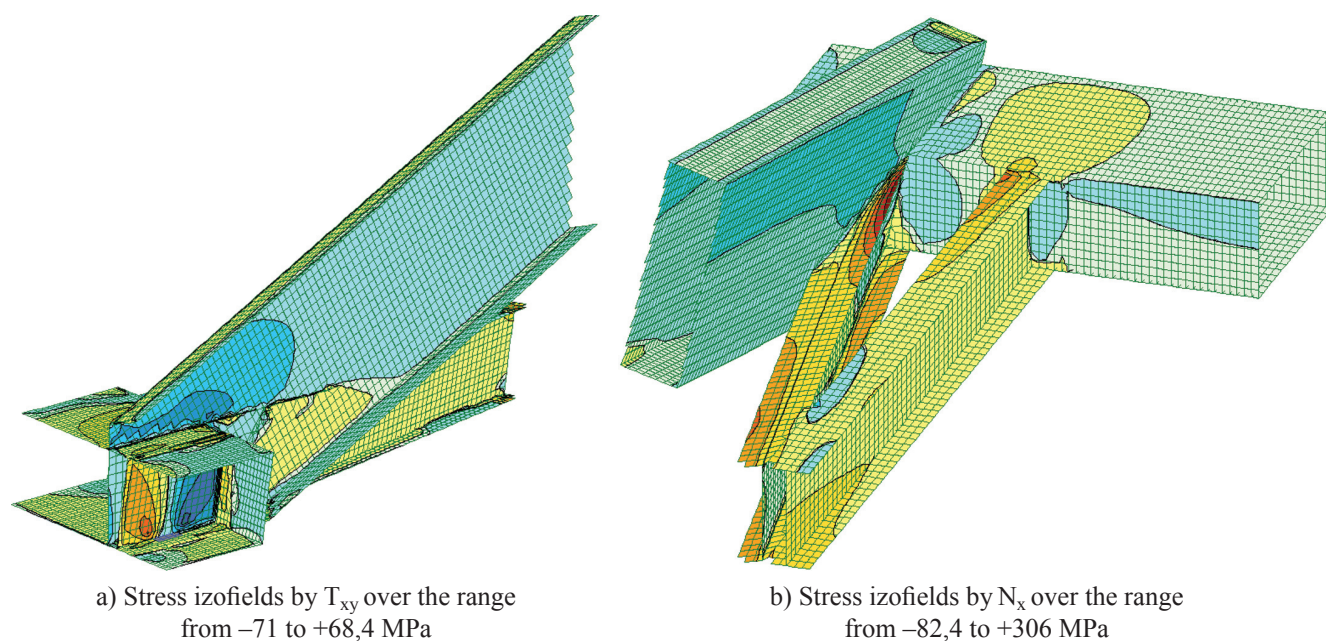


Fig. 1. Fragments of individual alternative loadings with stress izofields in elements of the arch – bowstring – jack beam joint

**Table 1. Statistical characteristics of individual components
in the arch – bowstring – jack beam joint**

Item number	SSS components	Statistical characteristics						
		Sample size	Arithmetic mean value	Root-mean-square deviation	Coefficient of variation	Set excess	Least value	Largest value
1.	Normal stress along vertical axis	138	122,4 MPa	23,9 MPa	0,195	−0,857	90,0 MPa	155,6 MPa
2.	Normal stress along horizontal axis	138	130,1 MPa	27,1 MPa	0,208	−0,832	102,0 MPa	174,9 MPa
3.	Shear stresses	138 MPa	82,3 MPa	17,3 MPa	0,210	−0,838	58,0 MPa	90,4 MPa

The general view of the obtained statistical characteristics of individual SSS components (table 1) shows the deformation of the form of final distribution of probabilities regarding its comparison with statistical characteristics of random variable for the normal distribution law.

The authors have developed logic and analytical MathCAD program modules in order to estimate the probability of a possible «surge» of the random variable of each k-th intermediate parameter (individual SSS components) beyond the level of disadvantageous boundary in uncertainty entropic interval. For this purpose, the frequency $\phi_k|N$ of the expected “surge” of k-th parameter random variable, which was determined by registration of cases with individual excess of i-th realizations of k-th parameter $\sigma_{k,i}(N)$ in the level of the upper boundary of uncertainty entropic interval $\sigma_{k,sup}$, for the same parameter during simulation of volume N:

$$\phi_k|N = \frac{n_k \left(\sigma_{k,i}(N) > \sigma_{k,sup} \right)}{N}, \quad (1)$$

$$\sigma_{k,sup} = \bar{\sigma}_k + \varepsilon_{k,\beta}, \quad (2)$$

where $\varepsilon_{k,\beta}$ is the estimation accuracy of k- th parameter calculated with confidence β .

Test runs of simulation models were carried out for definition of the required amount of stress simulation in calculated sections using statistical characteristics of individual SSS components in arch – bowstring – jack beam joints (table 1). The volume of initial numerical sets (individual SSS components) is specified at the level of $N \sim 10^4 \dots 10^7$ realizations. As the criterion confirming the adequacy of accepted simulation model, convergence by probability P_β is accepted:

$$\phi_k|N \xrightarrow{P_\beta} Q_{k,lim}(t), t \leq T_\Theta, \quad (3)$$

where $Q_{lim}(t)$ is the limit value of the risk factor, estimated based on the requirements of system dependability during operation t within the limits of expected designed service life T_Θ of construction.

Test runs of simulation models have shown that meeting the requirements to adequacy of the simulation plan, it is required to artificially regulate the volume of initial numerical sets N that depends on the accepted confidence level of the calculated parameter. For the purpose of the research task, the plan of simulation featured the volume of initial numerical sets $N = 10^7$ realizations at confidence level $\beta = 0,995$. The requirement to the limit risk factor of $Q_{lim}(t) = 5 \cdot 10^{-6}$ is observed.

At the fourth step, a set of simulations to estimate the design dependability of an arch – bowstring – jack beam joint was carried out according to the criterion of failure due to exhaustion of weight strength. Failure is the event consisting in the excess value of random realization of individual or simultaneous stresses in design sections over the random realization of the weight strength value of the material.

Initially, after studying the results of statistical research of the mechanical properties of the used structural material, it was decided to further use statistical data regarding 969 control tensile tests of standard samples presented in study [8]. In the set of simulations aimed at estimating the dependability of the arch – bowstring – jack beam joint, the used 15HSND steel features the following statistical characteristics: selective average yield stress of 386,9 MPa, variation coefficient of 0,0835, mean difference of 32,4 MPa; selective average breaking strength of 558,5 MPa, variation coefficient of 0,0745, mean difference of 41,7 MPa.

Table 2. Calculated interval estimates for joint SSS components

Item number	SSS components	Calculated interval estimates	
		Lower boundary (inf)	Upper boundary (sup)
1.	Normal stresses along vertical axis, $\sigma_x \sim f[\sigma_{x,inf}; \sigma_{x,sup}]$	90,0 MPa	280,9
2.	Normal stresses along horizontal axis, $\sigma_y \sim f[\sigma_{y,inf}; \sigma_{y,sup}]$	102,0 MPa	590,6
3.	Shear stresses, $\tau_{xy} \sim f[\tau_{xy,inf}; \tau_{xy,sup}]$	58,0 MPa	183,5

Solving the tasks of this step with the use of the results of statistical analysis of junction SSS evaluations obtained at the third step involved the generation of interval estimates for SSS components according to the accepted simulation plan (table 2). The lower border is specified as the least value of the respective SSS component (see table 1) that corresponds to constant loads only, while the upper boundary is calculated based on the characteristics of the simulation plan (at the upper boundary of the confidential interval with the probability of 995, sample size of 138, quantile of 2,853 and number of model runs of 400).

The condition of estimation according to the criterion of failure due to exhaustion of weight strength is follows:

$$Q_{\Omega} \Rightarrow \begin{cases} R_y(j) < \sigma_x(j) \\ R_y(j) < \sigma_y(j) \\ R_s(j) < \tau_{xy}(j) \\ R_y(j) < \sqrt{[\sigma_x(j)^2 - \sigma_x(j) \cdot \sigma_y(j) + \sigma_y(j)^2 + 3 \cdot \tau_{xy}(j)^2]} \end{cases}, \text{ for } j \in [1; N], (4)$$

where $R_y(j)$, $R_s(j) = 0,58 \cdot R_y(j)$ are sets of random realizations of yield point and shear resistance of steel, $\sigma_x(j)$, $\sigma_y(j)$, $\tau_{xy}(j)$ are sets of random realizations of individual SSS components (normal and shearing stresses).

Simulations of design dependability of the arch – bowstring – jack beam joint according to the criterion of failure due to exhaustion of weight strength did not identify the values of random realizations of indi-

vidually simulated normal and shearing stresses to exceed random realizations of values of material weight strength. It was established, that subject to composite action of stresses during the estimation according to the fourth model in condition (4), there was a consistent registration of failures with the maximum frequency of $2,4 \cdot 10^{-6}$ that does not contradict the limiting value of risk factor at $Q_{lim}(t) = 5 \cdot 10^{-6}$.

Thus, from the standpoint of sufficient dependability parameters for the design stage, the accepted design solutions can be left unchanged.

At the fifth step, a series of simulations was carried out to estimate the possible variability of dependability parameters of the arch – bowstring – jack beam joint at the stage of operation.

Obviously, in the course of systems operation, the effects of various adverse processes are inevitable (i.e. deterioration of elements, substandard and/or untimely maintenance). As a rule, at the design stage, the designer has to face certain seemingly insurmountable difficulties that are caused, in particular, by the fact that the designed structure or sometimes even comparable projects are nonexistent. In this situation it is difficult or even impossible to provide an accurate assessment of system dependability evolution over the course of design life time. In order to solve the tasks of this step, analytical models for formalization of variability process of dependability parameters outlined in [9] and the model for description of deterioration processes of steel structures from allied sciences (for example, [10]) were used.

In the development of the variability model of dependability parameters during designed operation life time one of the more important indicators is the final value of dependability determinative parameter (for example, failure probability) by the moment of exhaustion of safe operation life. Let's write down the condition at which the technical system has not exhausted the life during operation time t :

$$Q_{\Omega}(t) \leq [Q(t)], \quad t \leq T_{\Theta}, \quad (5)$$

where $Q_{\Omega}(t)$ is the probability of hazardous failures according to limiting state with the condition Ω ; $[Q_{\Omega}(t)]$ is the acceptable value of probability of the failure in question.

In view of condition (5), the formula of estimation (4) by failure criterion due to exhaustion of weight strength is rewritten as follows:

$$\{Q_{lim}(t)\} \leq Q_{\Omega}(t) \Rightarrow \begin{cases} R_{yt}(j) < \sigma_{xt}(j) \\ R_{yt}(j) < \sigma_{yt}(j) \\ R_{st}(j) < \tau_{xyt}(j) \\ R_{yt}(j) < \sqrt{|\sigma_{xt}(j)^2 - \sigma_{xt}(j) \cdot \sigma_{yt}(j) + \sigma_{yt}(j)^2 + 3 \cdot \tau_{xyt}(j)^2|} \end{cases}, \quad (6)$$

where $R_{yt}(j)$, $R_{st}(j)$ are the areas of random realizations of yield point and steel shear resistance with time-base sweep t ; $\sigma_{xt}(j)$, $\sigma_{yt}(j)$, $\tau_{xyt}(j)$ are the same for individual SSS components.

Now let's consider a simple linear model describing variability of individual i -th calculated parameter, included in formulas (4):

$$\Phi_i(t) = \Phi_{i,0} \cdot (1 + t \cdot \Delta_i), \quad (7)$$

where $\Phi_{i,0}$ is the initial-time value of an individual i -th calculated parameter ($t=0$); $\Delta_i = \frac{d}{dt} \Phi_i(t)$ is the composite indicator that takes into account the effects of various adverse processes in time t within the limits of expected designed life time of a structure.

Various values of a complex parameter Δ_t adopted in the range of $1 \cdot 10^{-4} \dots 5 \cdot 10^{-5}$ are examined using the example of the arch – bowstring – jack beam joint in spans of pedestrian overpasses. The values of the composite indicator Δ_t were used in simulations to define the variability of probability of system failures in time (by a fig. 2).

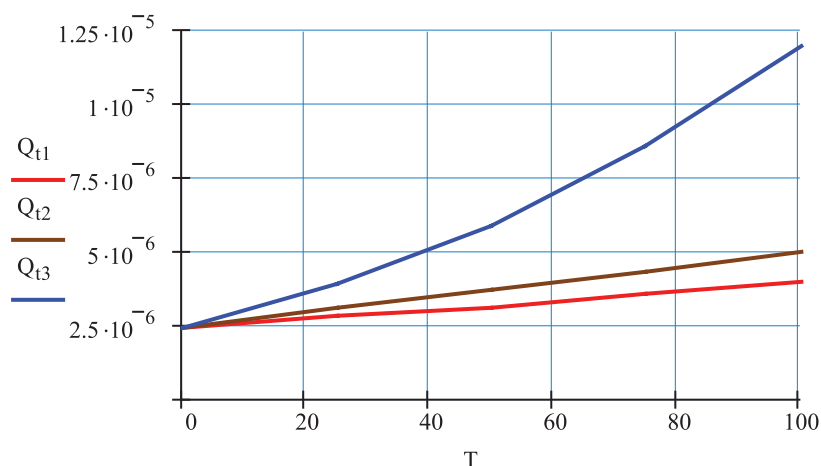


Fig. 2. Variability diagrams of probability of system failures in time T depending on the accepted value of the composite indicator Δ_t , for $\Delta_{t1} = 5 \cdot 10^{-4}$ the probability of failures is Q_{t1} , $\Delta_{t2} = 2,5 \cdot 10^{-4}$, the probability of failures is Q_{t2} and for $\Delta_{t3} = 1 \cdot 10^{-4}$ the probability of failures is Q_{t3}

The obtained results show, that in order to retain the dependability parameters in operation, provided that the accepted design solutions remain unchanged, the variability of calculated parameters in time (increase of stresses) must not exceed $\Delta_t = 2,5 \cdot 10^{-4}$ per year.

Conclusions

According to the results of dependability analysis of the critical arch – bowstring – jack beam joint in spans of a designed pedestrian overpasses, it was established, that subject to confidence level of calculated estimations $\beta = 0,995$, a failure under criterion of one of the elements exhaustion appears to be practically improbable.

For the criterion of weight strength exhaustion from cumulative action of stresses in the simulation of typical combinations of external loadings in the arch – bowstring – jack beam joint, there was a consistent registration of failures with the maximum frequency of $2,4 \cdot 10^{-6}$ that does not contradict the limiting value of risk factor of $Q_{lim}(t) = 5 \cdot 10^{-6}$.

The authors have developed and practically tested special dependability estimation algorithms based on structural, statistical and simulation methods, as well as regression analysis techniques that allow both estimating design dependability and predicting the acceptable level of dependability parameters variation over the course of system operation subject to the criticality of the function.

References

1. **Manapov A.Z.** Dependability and engineering structures lifetime calculation by means of statistical modeling: Textbook. Kazan: KSABU, 2010. – 131 p.
2. Manual on the design of steel constructions (Construction regulations II-23-81 “Steel constructions”) / TsNIISK Kucherenko Gosstroy of the USSR. – M.: CiTP Gosstroy of the USSR, 1989. – 148 p.

3. **Shpete G.** Dependability of load-bearing structures / Tr. From German by O.O.Andreev. – M.: Stroyizdat, 1994. – 288 p.
4. **Rayzer V.D.** Methods of dependability theory in normalization of calculated parameters of building structures / V.D.Rajzer; – M.: Stroyizdat., 1986. – 192 p.
5. **Maystrenko I.Yu., Manapov A.Z.** Statistical modeling of building structures by Monte Carlo method. Work with numerical sets // KSABU News # 2 (20), 2012. – pp. 84-93.
6. Body of rules BR.35.13339.2011. Bridges and conduits. Updated edition of Construction regulations.05.03-84* // Approved by Order of the Ministry of Regional Development of Russia as of December, 28, 2010 #82.
7. Body of rules BR. 20.13330.2011. Loads and impacts. Updated edition of Construction regulations 2.01.07-85* // Approved by Order of the Ministry of Regional Development of Russia as of December, 27, 2010 #787.
8. **Koshutin B.N., Uvarov B.Yu.** Statistical research of mechanical properties of some construction steels // Collected papers #96 IISS V.V. Kuibyshev / ed. E.I.Belenja. – M., 1973. – pp. 13-22.
9. **Maystrenko I.Yu., Manapov A.Z.** Modeling of structural systems dependability variation in time // News of KazSACU # 1 (13), 2010. – pp. 132-140.
10. Durability of steel structures under conditions of reconstruction / **Gorokhov, E.V., Brudka J., Lubinski, M., etc.; ed. Gorokhov, E.V.** – M.: Stroyizdat, 1994. – 488 p.

**Носов М.В.**

МЕТОД УСТРАНЕНИЯ ВЗАИМНОГО ПЕРЕСЕЧЕНИЯ ОЦЕНОК ЭЗАРИ-ПРОШАНА В ЗАДАЧАХ АНАЛИЗА СВЯЗНОСТИ ДВУХПОЛЮСНЫХ СЕТЕЙ

Рассматривается содержание метода, обеспечивающего устранение взаимного пересечения и уменьшение значений погрешностей оценок Эзари-Прошана.

Ключевые слова: вероятность связности, вероятность несвязности, двухполюсная сеть, случайный граф двухполюсной сети, простая цепь, простой разрез, верхняя оценка, нижняя оценка, точное значение, оценки Эзари-Прошана, двухсторонние оценки, элементарные конструкции.

1. Общие положения и постановка задачи

В настоящее время наиболее известными оценками вероятности связности (ВС) двухполюсных сетей (ДС) являются оценки Эзари-Прошана (ОЭП). [1,3,7,8,9].

В ОЭП в качестве оценочных случайных графов двухполюсных сетей (СГ ДС) используются [3]:

- для расчета верхней границы оценок – оценочный СГ ДС, состоящий из полного множества параллельно соединенных простых цепей (ПЦ) с учетом того, что взаимная зависимость между ПЦ не учитывается;

- для расчета нижней границы оценок – оценочный СГ ДС, состоящий из полного множества последовательно соединенных простых разрезов (ПР) с учетом того, что взаимная зависимость между ПР не учитывается.

Однако наличие зависимостей между ПЦ или ПР в соответствующих оценочных СГ ДС увеличивает погрешность ОЭП относительно точного значения ВС ДС [2, 3].

Кроме того ОЭП при неполном использовании теоретически возможного множества ПЦ и ПР в оценочных СГ ДС взаимно пересекаются, что также является существенным недостатком ОЭП [3,6] (см. рис. 6).

Вследствие этого ОЭП сохраняют «исторический и методический интерес», но не востребованы для практического применения [9].

Поэтому ниже рассматривается метод, позволяющий устранить взаимное пересечение и получить монотонную сходящуюся ОЭП к точному значению ВС СГ ДС, а также снизить погрешность ОЭП.

Допустим, что анализируемая ДС будет представлена в виде СГ ДС, в котором между вершинами-полюсами S и t передается некоторое сообщение.

Будем полагать, что математическая модель СГ ДС формально задана, если помимо вершин-полюсов S и t определено и ограничение на число ϕ транзитных вершин в путях связи между S и t такое, что $0 \leq \phi \leq (m_v - 2)$, где $m_v = |V| = \left\{ v_{i=1, |V|} \right\}$ – мощность множества вершин СГ ДС.

Для принятых условий требуется представить теоретическое обоснование метода, обеспечивающего монотонную (не пересекаемую) сходимость ОЭП к точному значению ВС СГ ДС, а также снижение погрешности ОЭП.

2. Содержание метода

Для раскрытия содержания метода воспользуемся некоторыми теоретическими положениями работ [10,11] и сформулируем следующую теорему.

Теорема. Путь структура анализируемого СГ ДС состоит из множества вершин $V = \{v_i\}$, $i = 1, |m_v|$, где $|m_v|$ – мощность множества вершин, и множества ребер $L = \{l_\xi\}$, $\xi = 1, |m_L|$, где $|m_L|$ – мощность множества ребер, в составе которых имеется подмножество общих (мостиковых) ребер $L^0 = \{l_\xi^0\}$, $\xi = 1, |m_{L^0}|$, $L^0 \in L$. Допустим, что вершины СГ ДС абсолютно надежны. Надежность мостикового ребра l_ξ^0 характеризуется двумя состояниями: работоспособным – l_ξ^0 или неработоспособным $\bar{l}_\xi^0$, соответственно с вероятностями $p(l_\xi^0)$ и $q(l_\xi^0) = 1 - p(l_\xi^0)$. С учетом этого положения, число всевозможных состояний (гипотез) мостиковых ребер определим как:

$$\Gamma^0 = 2^{m_{L^0}} = \{\Gamma_i^0\}, i = 1, |m_{\Gamma^0}|, \quad (1)$$

где $|m_{\Gamma^0}|$ – мощность множества состояний (гипотез) общих ребер.

Анализируемый СГ ДС характеризуется множеством ПЦ $M = \{\mu_n\}$, $n = 1, |m_M|$, где $|m_M|$ – мощность множества ПЦ, и множеством ПР $R = \{r_n\}$, $n = 1, |m_R|$, где $|m_R|$ – мощность множества ПР, которые соответственно образуют структуру оценочного СГ ДС по ПЦ – $G_{s,t}^{ПЦ}$ и структуру оценочного СГ ДС по ПР – $G_{s,t}^{ПР}$.

Оценочные СГ ДС $G_{s,t}^{ПЦ}$ и $G_{s,t}^{ПР}$ при нахождении подмножества их мостиковых ребер $L^0 = \{l_\xi^0\}$ в состоянии Γ_i^0 преобразуются соответственно в условные оценочные СГ ДС $G_{s,t(i)}^{ПЦ}$ и $G_{s,t(i)}^{ПР}$, т.е.

$$\begin{cases} G_{s,t}^{ПЦ} / \Gamma_i^0 = G_{s,t(i)}^{ПЦ} \\ G_{s,t}^{ПР} / \Gamma_i^0 = G_{s,t(i)}^{ПР} \end{cases} \quad (2)$$

В работах [3,4] показано, что для расчета верхней ОЭП должно быть применено равенство:

$$P_{s,t}^{BO} = 1 - P_{s,t}^{HO}, \quad (3)$$

где $P_{s,t}^{HO}$ – нижняя оценка вероятности несвязности вершин s и t в СГ ДС.

Для указанных условий требуется доказать справедливость применения для расчета верхней и нижней оценок ВС анализируемого СГ ДС соответствующих формул следующего вида:

$$P_{s,t}^{BO} = 1 - \left[P_{s,t}^{HO} = \sum_{i=1}^{m_{L^0}} P_{s,t(i)}^{HO} = \sum_{i=1}^{m_{L^0}} P(\Gamma_i^0) P(G_{s,t(i)}^{ПЦ} / \Gamma_i^0) \right], \quad (Т. 1)$$

$$P_{s,t}^{HO} = \sum_{i=1}^{m_{\Gamma^0}} P_{s,t_i}^{HO} = \sum_{i=1}^{m_{\Gamma^0}} P(\Gamma_i^0) P(G_{s,t_i}^{PP} / \Gamma_i^0), \quad (Т. 2)$$

где $P(\Gamma_i^0)$ – вероятность i -го состояния подмножества мостиковых ребер

$$L^0 = \{\Gamma_{\xi}^0\}, \xi = \overline{1, m_{L^0}};$$

$\overline{P(G_{s,t}^{ПП} / \Gamma_i^0)}$ – условная вероятность несвязности вершин S и t СГ ДС по ПЦ, соответствующая гипотезе Γ_i^0 . Для краткости написания обозначим эту вероятность как $P(G_{s,t_i}^{ПП})$, где $G_{s,t_i}^{ПП} = G_{s,t_i}^{ПП} / \Gamma_i^0$;

$P(G_{s,t}^{PP} / \Gamma_i^0)$ – условная вероятность связности вершин S и t СГ ДС по ПР, соответствующая гипотезе Γ_i^0 . Эту оценку обозначим как $P(G_{s,t_i}^{PP})$, где $G_{s,t_i}^{PP} = G_{s,t_i}^{PP} / \Gamma_i^0$;

$$P_{s,t_i}^{HO} = P(\Gamma_i^0) \overline{P(G_{s,t_i}^{ПП} / \Gamma_i^0)} \quad (Т.3)$$

- вероятность несвязности вершин S и t анализируемого СГ ДС по ПЦ при условии, что СГ ДС находится в состоянии Γ_i^0 .

Доказательство. Так как множество гипотез (состояний) $\Gamma_i^0 = \{\Gamma_i^0\}, i = \overline{1, m_{\Gamma^0}}$ подмножества мостиковых ребер $L^0 = \{\Gamma_{\xi}^0\}, \xi = \overline{1, m_{L^0}}$, образуют полную группу несовместных событий, а условные СГ ДС (2) могут быть образованы только в соответствии с одной из гипотез $\Gamma_i^0, i = \overline{1, m_{\Gamma^0}}$, то согласно содержания формулы полной вероятности [2], равенства (Т.1) и (Т. 2) определены верно. Теорема доказана.

Следствие. При $\xi=1, \Gamma^0=2^1=2: \Gamma_1^0=l_1, \Gamma_2^0=\bar{l}_1$.

Тогда:

$$P_{s,t}^{BO} = 1 - \left[P_{s,t}^{HO} = \sum_{i=1}^2 P_{s,t_i}^{HO} = \sum_{i=1}^2 P(\Gamma_i^0) \overline{P(G_{s,t_i}^{ПП} / \Gamma_i^0)} \right], \quad (4)$$

$$\text{где } P_{s,t_i}^{HO} = P(\Gamma_i^0) P(G_{s,t_i}^{ПП} / \Gamma_i^0), \quad (5)$$

$$P_{s,t}^{HO} = \sum_{i=1}^2 P_{s,t_i}^{HO} = \sum_{i=1}^2 P(\Gamma_i^0) P(G_{s,t_i}^{ПП} / \Gamma_i^0), \quad (6)$$

При $\xi=2, \Gamma^0=2^2=4: \Gamma_1^0=l_1 \cdot l_2; \Gamma_2^0=\bar{l}_1 \cdot l_2; \Gamma_3^0=l_1 \cdot \bar{l}_2; \Gamma_4^0=\bar{l}_1 \cdot \bar{l}_2$.

Для этого варианта:

$$P_{s,t}^{BO} = 1 - \left[P_{s,t}^{HO} = \sum_{i=1}^4 P_{s,t_i}^{HO} = \sum_{i=1}^4 P(\Gamma_i^0) \overline{P(G_{s,t_i}^{ПП} / \Gamma_i^0)} \right], \quad (7)$$

$$\text{где } P_{s,t}^{HO} = \sum_{i=1}^4 P_{s,t_i}^{HO} = \sum_{i=1}^4 P(\Gamma_i^0) P(G_{s,t_i}^{ПП} / \Gamma_i^0), \quad (8)$$

и т.д.

Вероятность гипотезы Γ_i^0 определим как:

$$P(\Gamma_i^0) = \prod_{\xi \in \beta_1} P(l_\xi^0) \prod_{\xi \in \beta_2} q(l_\xi^0), \quad (9)$$

где β_1 и β_2 – обозначения соответственно подмножеств работоспособных и отказавших мостиковых ребер, составляющих гипотезу Γ_i^0 ;

$P(l_\xi^0)$ – вероятность нахождения общего ребра l_ξ^0 в работоспособном состоянии, $q(l_\xi^0) = 1 - P(l_\xi^0)$.

Расчет условных вероятностей $P(G_{s,t_i}^{III})$ и $P(G_{s,t_i}^{PP})$ выполним согласно структур условных оценочных СГ ДС по ПЦ – G_{s,t_i}^{III} и по ПР – G_{s,t_i}^{PP} , полученных соответственно из оценочных СГ ДС $G_{s,t}^{III}$ и $G_{s,t}^{PP}$ при условии, что подмножество $L^0 = \{l_\xi^0\}$ общих ребер находится в состоянии i .

Покажем, что применение комбинаторного метода устраняет взаимное пересечение ОЭП. С этой целью сформулируем и докажем следующее утверждение.

Утверждение. Дано: исходный СГ ДС (рис. 1) и его оценочные СГ ДС (рис. 2а и рис. 2б) для расчета соответственно верхней оценки $P_{s,t}^{BO}$ и нижней оценки $P_{s,t}^{HO}$ вероятности связности. Если для расчета $P_{s,t}^{BO}$ и $P_{s,t}^{HO}$ применяется предложенный комбинаторный метод, то получаемые при этом двухсторонние оценки ВС на i -х итерационных шагах не пересекаются.

Требуется доказать:

$$P_{s,t}^{BO}(\Gamma_i^0) > P_{s,t}^{HO}(\Gamma_i^0), \quad (У. 1)$$

для всех значений $0 < p(l_\xi) < 1$.

Доказательство. Поскольку всевозможные гипотезы $\Gamma^0 = \{\Gamma_i^0\}$, используемые для определения верхней и нижней ОЭП, являются одинаковыми и составляют полную группу, то согласно формулы разложения Мура-Шеннона для каждой i -й гипотезы справедливо неравенство $P_{s,t}^{BO}(\Gamma_i^0) > P_{s,t}^{HO}(\Gamma_i^0)$ для всех значений $0 < p(l_\xi) < 1$ [12]. Утверждение доказано.

Для иллюстрации содержания предложенного метода анализа двухсторонних ОЭП воспользуемся двухмостиковым СГ ДС, со сквозной нумерацией элементов, рис. 1. [3]

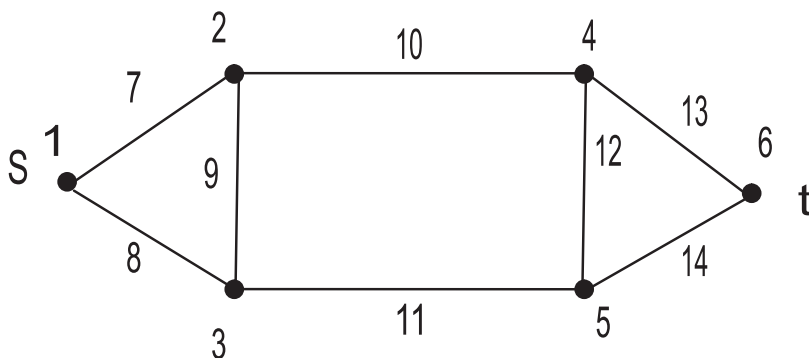


Рис. 1. Двухмостиковый СГ ДС со сквозной нумерацией элементов

Структурные элементы на рис. 1 имеют только цифровые обозначения. Этот СГ ДС характеризуется множеством ПЦ (рис. 2а) вида:

$$M_{s,t} = \left\{ \begin{aligned} &M_{n=1} = (7,10,13), M_{n=2} = (8,11,14), M_{n=3} = (7,10,12,14), M_{n=4} = (7,9,11,14), \\ &M_{n=5} = (8,9,10,13), M_{n=6} = (8,11,12,13), M_{n=7} = (7,9,11,12,13), M_{n=8} = (8,9,10,12,14) \end{aligned} \right\}, \quad (10)$$

определяющее верхнюю ОЭП, а также множеством ПР (рис. 2б) вида:

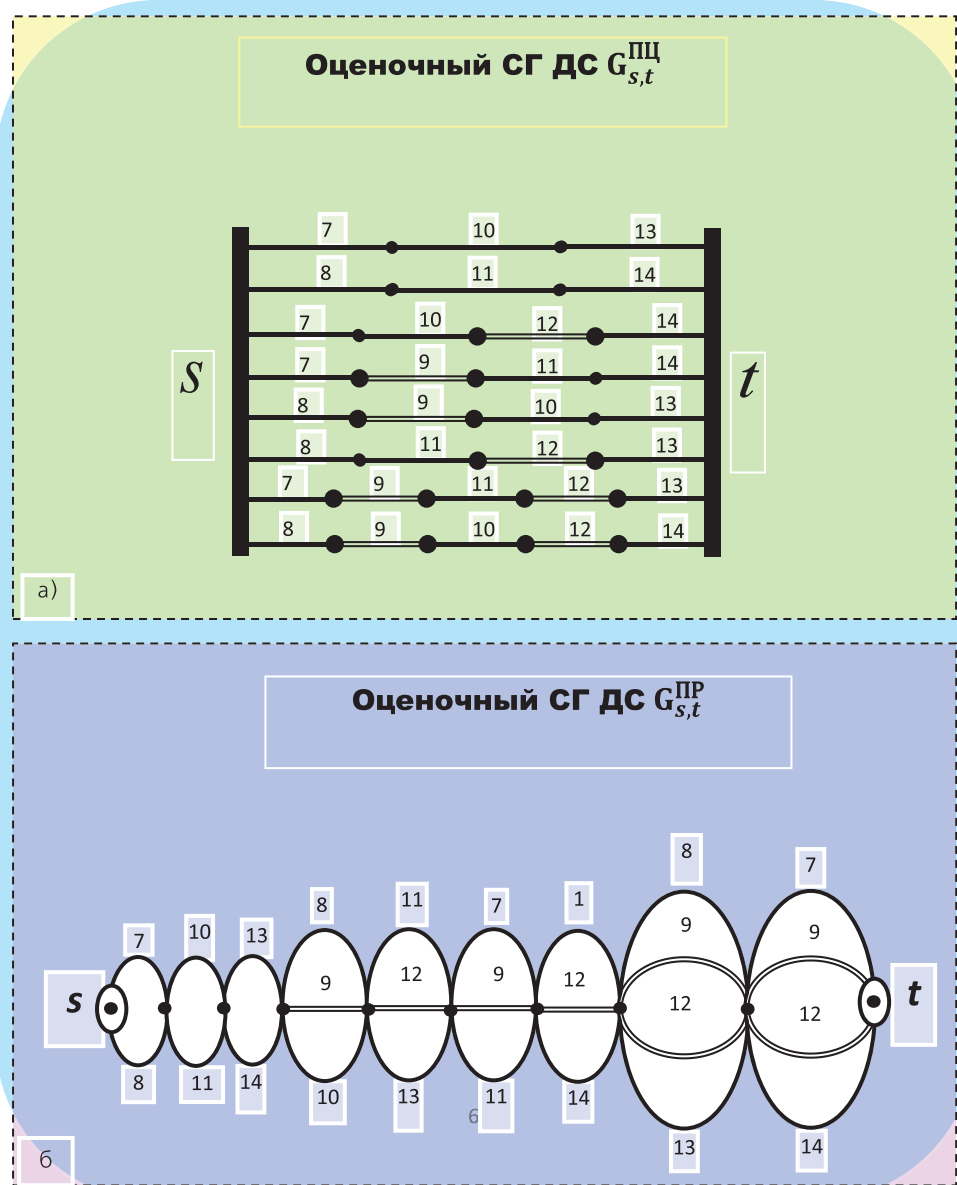


Рис. 2. Схемы оценочных СГ ДС для ОЭП: а) – по ПЦ; б) - по ПР

$$R_{s,t} = \left\{ \begin{array}{l} r_{n=1} = (7,8), r_{n=2} = (10,11), r_{n=3} = (13,14), r_{n=4} = (8,9,10), r_{n=5} = (11,12,13), \\ r_{n=6} = (7,9,11), r_{n=7} = (10,12,14), r_{n=8} = (8,9,12,13), r_{n=9} = (7,9,12,14) \end{array} \right\}, \quad (11)$$

определяющее нижнюю ОЭП.

На рис. 2а и 2б мостиковые ребра 9 и 12 выделены тонкими двойными линиями.

Поскольку в структуре исходного СГДС (рис. 1) имеется два мостиковых ребра (9 и 12), то полная группа несовместных состояний (гипотез) этих ребер примет вид:

$$\Gamma^0 = \{ \Gamma_1^0 = (9 \cdot 12); \Gamma_2^0 = (\bar{9} \cdot 12); \Gamma_3^0 = (9 \cdot \bar{12}); \Gamma_4^0 = (\bar{9} \cdot \bar{12}) \}. \quad (12)$$

С учетом полной группы несовместных состояний (10), произведено преобразование исходного оценочного СГ ДС $G_{s,t}^{ПЦ}$ (рис. 2а) в условные оценочные СГ ДС $G_{s,t_i}^{ПЦ}$, представленные на рис. 3, а

также исходного оценочного СГ ДС $G_{s,t}^{III}$ (рис. 2б) в условные оценочные СГ ДС G_{s,t_i}^{III} , представленные на рис. 4.

На представленных условных СГ ДС (рис. 3 и рис. 4) темные кружки означают соединение смежных вершин в общую точку по особым ребрам 9 и 12, когда эти ребра находятся в работоспособном состоянии; если эти ребра находятся в неработоспособном состоянии, то в соответствующих элементарных конструкциях (ПЦ и ПР) образуются разрывы, которые на указанных выше рисунках изображены штриховыми линиями.

Сформулированные и доказанные положения относительно справедливости применения комбинаторного метода для устранения взаимного пересечения ОЭП подтвердим следующим вычислительным экспериментом.

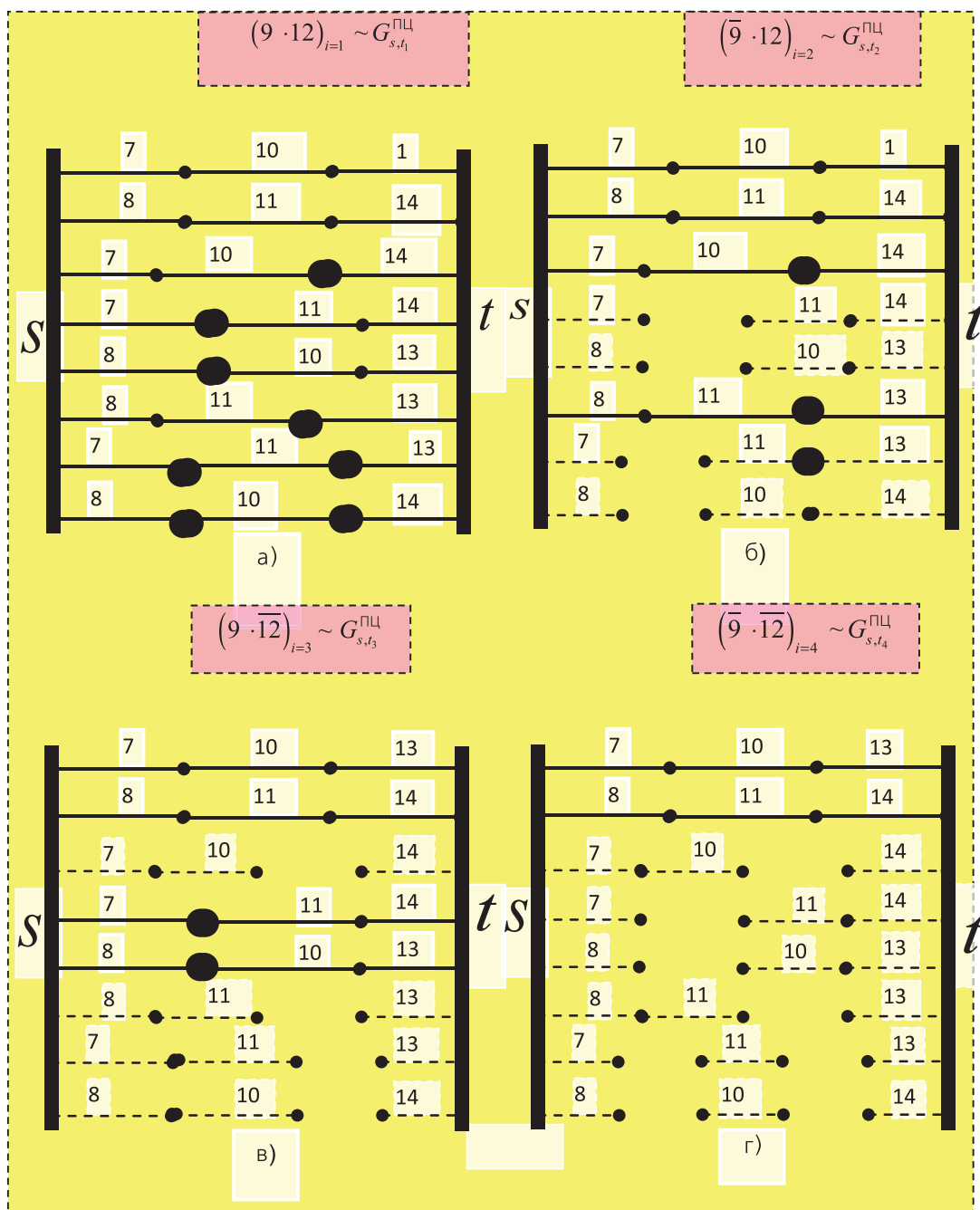


Рис. 3. Преобразование оценочного СГ ДС $G_{s,t}^{III}$ при принятии i -ой гипотезы

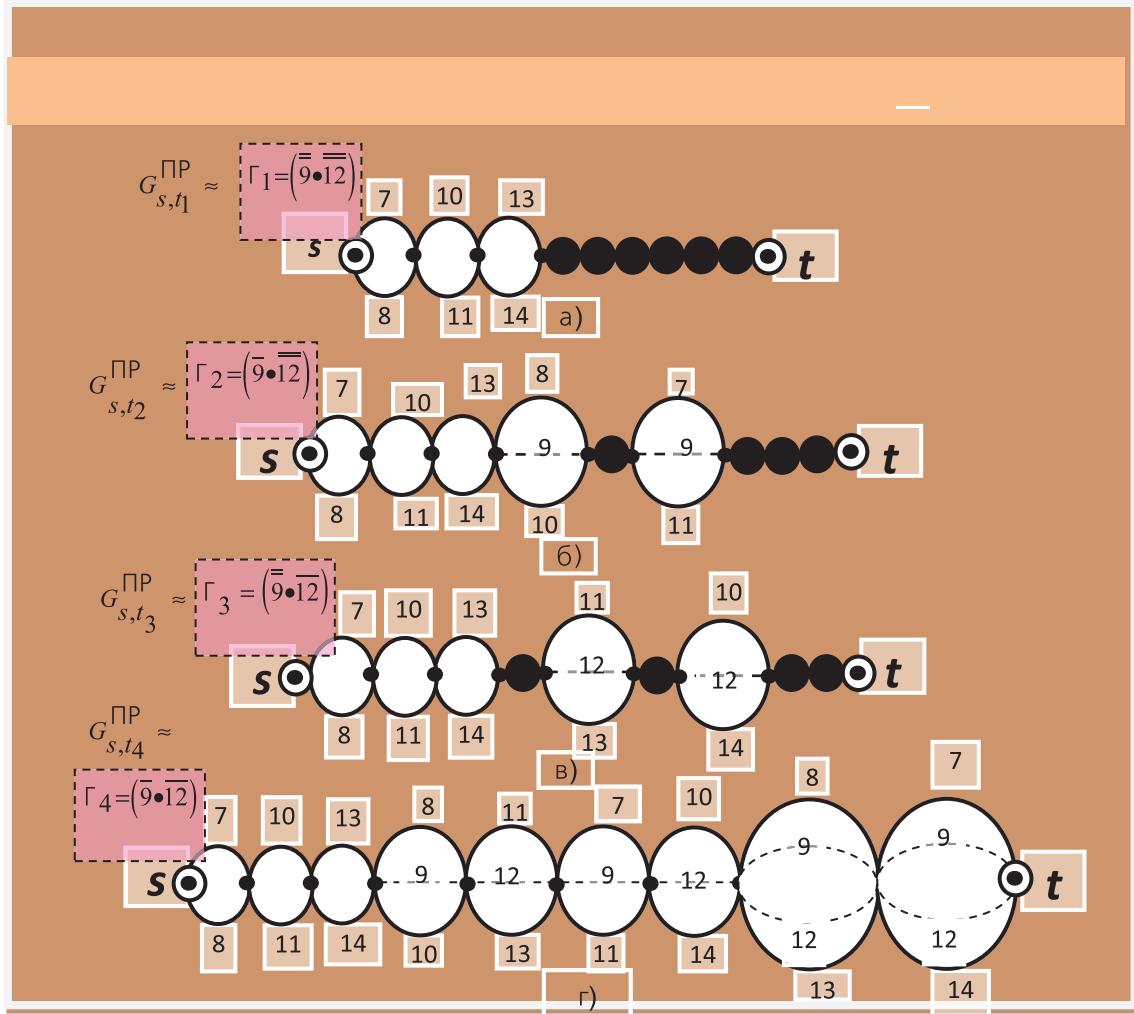


Рис. 4. Преобразование оценочного СГ ДС $G_{s,t}^{PP}$ при принятии i -ой гипотезы

Вычислим верхнюю $P_{s,t}^{BO}$ и нижнюю $P_{s,t}^{HO}$ оценки ВС СГ ДС (рис. 1) для следующих исходных данных (ИД) по надежности ребер $p_{\xi=7,14} = 0,5$.

Для принятых ИД, оценку (5), с учетом равенства (7) определим следующим образом:

$$P_{s,t}^{HO} = 0_{i=0} + 0,085902228_{i=1} + 0,14654541_{i=2} + 0,14654541_{i=3} + 0,19140625_{i=4} = 0,570399298 \quad (13)$$

Тогда, согласно (13) монотонную сходимость $P_{s,t}^{BO}$ к $P_{s,t}$ определим в следующем виде:

$$\begin{aligned} P_{s,t}^{BO} \rightarrow P_{s,t} &= 1_{i=0} \rightarrow \left(1 - 0,085902228_{i=0,1} = \underline{\underline{0,914097772}}\right)_{i=0,1} \rightarrow \left(1 - 0,232447638_{i=0,2} = \right. \\ &= \underline{\underline{0,767552365}}\left.)_{i=0,2} \rightarrow \left(1 - 0,378993048_{i=0,3} = \underline{\underline{0,621006952}}\right)_{i=0,3} \rightarrow \left(1 - 0,570399298_{i=0,4} = \right. \\ &= \underline{\underline{0,429600702}} = P_{s,t}^{BO}\left.)_{i=0,4} \end{aligned} \quad (14)$$

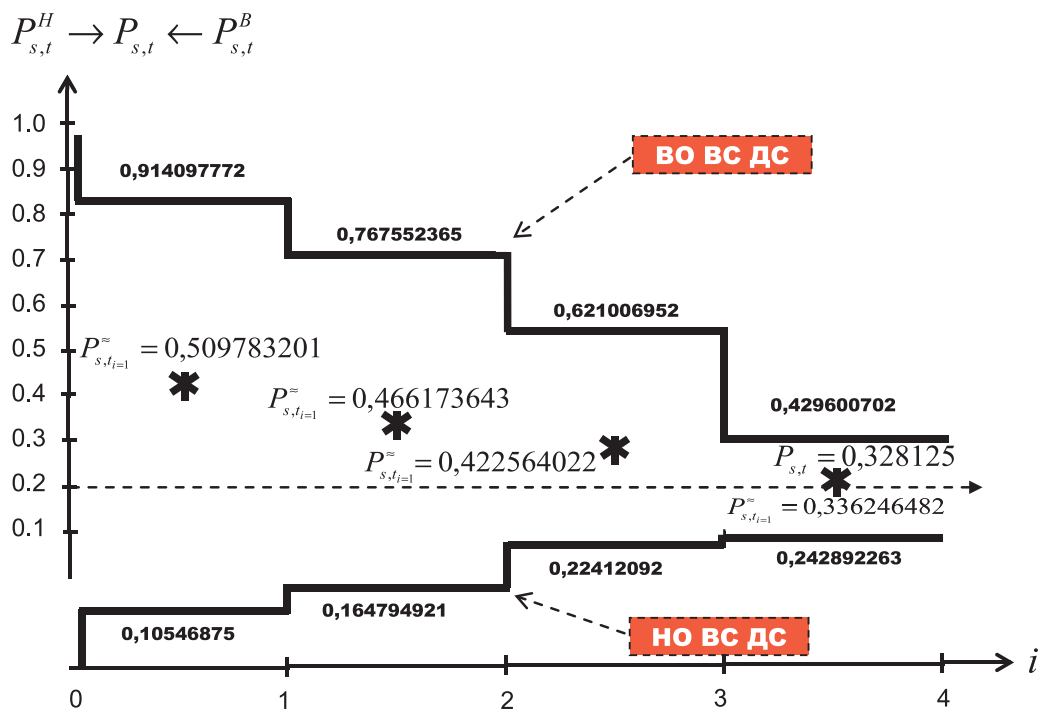


Рис. 5. Иллюстрация монотонной сходимости ОЭП к точному значению

Для принятых ИД $p_{\zeta=7,14} = 0,5 = q_{\zeta=7,14}$ НО ВС анализируемого СГ ДС (рис. 1) согласно (8) будет равна:

$$P_{s,t}^{HO} = 0_{i=0} + 0,10546875_{i=1} + 0,059326171_{i=2} + 0,059326172_{i=3} + 0,018771171_{i=4} =$$

$$= 0_{i=0} \rightarrow \underline{\underline{0,10546875}}_{i=1} \rightarrow \underline{\underline{0,164794921}}_{i=1,2} \rightarrow \underline{\underline{0,224121092}}_{i=1,3} \rightarrow \underline{\underline{0,242892263}}_{i=1,4}. \quad (15)$$

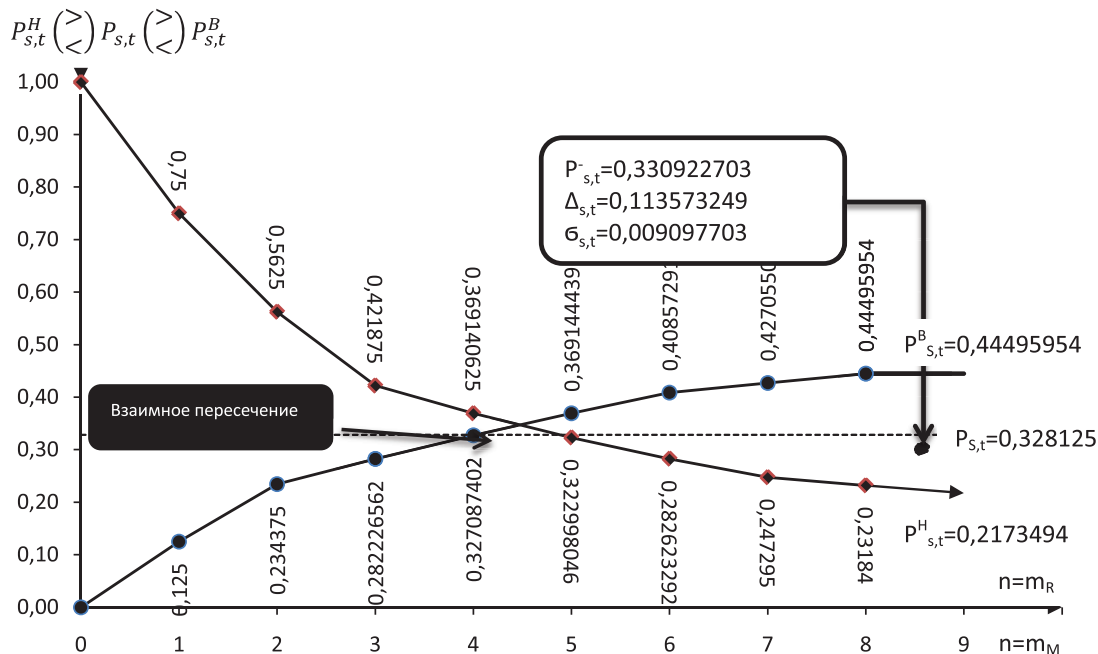


Рис. 6. Иллюстрация пересечения базовых ОЭП

На основе равенств (14) и (15) на рис. 5 построены графики монотонной сходимости ОЭП к точному значению вида $P_{s,t}^{HO} \rightarrow P_{s,t} \leftarrow P_{s,t}^{BO}$ для исходного СГ ДС, рис. 1. На рис. 5 «звездочкой» показана пошаговая сходимость погрешности вида $P_{s,t_i} \approx (P_{s,t_i}^{BO} + P_{s,t_i}^{HO}) / 2$ к точному значению $P_{s,t}$.

На рис. 6 представлена графическая интерпретация базовых ОЭП в динамике их пошагового изменения, применительно к анализу СГ ДС (рис.1) и ИД вида: $P_{\xi=\overline{7,14}} = 0,5 = q_{\xi=\overline{7,14}}$ [3].

Анализ, представленных в виде рис. 5 результатов выполненного численного эксперимента и их сравнение с базовыми ОЭП (рис. 6) показывает, что предложенный комбинаторный метод анализа обеспечивает ликвидацию взаимного пересечения и сокращение погрешностей ДСО ВС СГ ДС относительно базовых ОЭП.

Литература

1. Esary J., Proshan F. Coherent Structures of Non-Identifical Components // Technometrics. 1963.V.5. № 2. P.191-209.
2. Полесский В.П. Развязывание клаттеров, корреляционные неравенства и границы комбинаторной надежности // Проблемы передачи информации. 1997.Т.33. Вып. 3. С. 50-70.
3. Филин Б.П. О предельном развязывании клаттеров в оценках Полесского границ комбинаторной надежности случайных бинарных систем // Автоматика и телемеханика. 2005.№ 9.С. 149-189.
4. Филин Б.П. Методы анализа структурной надежности сетей связи. М.: Радио и связь, 1998.
5. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2000.
6. Кривулец В.Г. Об оценке оценок Эзари-Прошана в задачах анализа структурной надежности сетей связи // Труды 55-й Научной сессии, посвященной Дню радио./РНТОРЭС им. А.С. Попова. 2000.
7. Носов М.В. Предельные оценки надежности систем с сетевой структурой. / Надежность. 2010. № 2.
8. Носов М.В. Практическое приложение теории предельных оценок. // Надежность 2010. № 3.
9. Нетес В.А. Об оценке вероятности связности двухполюсных сетей / Электросвязь. 2001. № 11. С. 39-41.
10. Шубинский И.Б. Структурная надежность информационных систем. М: «Журнал Надежность», 2012. 216 с.
11. Шубинский И.Б. Функциональная надежность информационных систем. М: «Журнал Надежность», 2012. 295 с.
12. Мур Р., Шеннон К. Надежные схемы из ненадежных реле / Работы по теории информации и кибернетики. М.: ИЛ, 1963, С. 114-153.

**Nosov M.B.**

METHOD FOR ELIMINATION OF MUTUAL CROSSING OF ESARY-PROSHAN ESTIMATES IN TASKS OF ANALYSIS OF BIPOLAR NETWORKS CONNECTIVITY

The paper presents the method for elimination of mutual crossing and reduction of Esary-Proshan estimates errors.

Keywords: probability of connection, probability of discontinuity, bipolar network, random graph of bipolar network, simple path, simple cut, upper bound, lower bound, exact value, Esary-Proshan estimates, bilateral estimates, elementary designs.

1. Generalities and problem definition

Today the most known estimations of connectivity probability (CP) of bipolar networks (BN) are Esary-Proshan estimates (EPE) [1, 3, 7, 8, 9].

As estimated random graphs of bipolar networks (RG BN), EPE graphs offered in [3] use:

- For calculation of the upper bound of estimations – estimated RG BN, consisting of a full set of simple paths (SP) connected in parallel without the interdependence between circuits taken into account;
- For calculation of the lower bound of estimations – estimated RG BN, consisting of a full set of serially connected simple cuts (SC) without the interdependence between simple cuts taken into account.

However, the presence of dependences between SS or SC in corresponding estimated RG BN increases EPE errors in relation to the exact value of CP BN [2, 3].

In addition, EPE at incomplete use of a theoretically possible set of SP and SC in estimated RG BN mutually cross, that also being an essential disadvantage in EPE [3,6] (see fig. 6).

Owing to this, EPE retain “historical and methodical interest” but are not used for practical application [9].

Therefore, below we consider the method that allows us to eliminate mutual crossing and to receive monotonous convergence of EPE to the exact value of CP RG BN, and also to lower EPE errors.

Let us suppose that analyzed BN will be presented in the form of RG BN in which some message is transferred between vertices-poles S and t.

Let us believe that the mathematical model of RG BN is formally specified, if besides vertices-poles S and t, the restriction for the number of ϕ of transit vertices is also defined in connection paths between S and t as such that $0 \leq \phi \leq (m_v - 2)$, where $m_v = |V| = \left\{ v_{i=1, |V|} \right\}$ is the power of a vertex set RG BN.

For the accepted conditions, it is required to present a theoretical justification of the method providing monotonous (not overlapped) convergence of EPE to the exact value of CP RG BN, and also decrease of EPE errors.

2. The method's essence

In order to disclose the method's essence, we shall use some theoretical proposition in studies [10,11] and formulate the following theorem.

The theorem

Let the structure of analyzed RG BN consist of a vertex set $V = \{\vartheta_i\}$, $i = \overline{1, |m_V|}$, where $|m_V|$ is the power of a vertex set, and an edge set $L = \{l_\xi\}$, $\xi = \overline{1, |m_L|}$, where $|m_L|$ is the power of an edge set, in whose structure there is a subset of shared (bridge) edges $L^0 = \{l_\xi^0\}$, $\xi = \overline{1, |m_{L^0}|}$, $L^0 \in L$. Let us assume that vertices of RG BN are absolutely dependable. Dependability of a bridge edge l_ξ^0 is described by two states: operable state l_ξ^0 or down state $\bar{l}_\xi$, with corresponding probabilities. In view of this condition, we shall define the number of all possible states (hypotheses) of bridge edges as:

$$\Gamma^0 = 2^{m_{L^0}} = \{\Gamma_i^0\}, i = \overline{1, |m_{\Gamma^0}|}, \quad (1)$$

where $|m_{\Gamma^0}|$ is the power of a state set of shared edges.

Analyzed RG BN is characterized by SP set $M = \{\mu_n\}$, $n = \overline{1, |m_M|}$, and SC set $R = \{r_n\}$, $n = \overline{1, |m_R|}$, $|m_R|$ where $|m_M|$ is the power of SP set, and $|m_R|$ is the power of SC set, which accordingly form the structure of estimated RG BN under SP – $G_{s,t}^{III}$ and the structure of estimated RG BN under SC – $G_{s,t}^{PP}$.

Estimated RG BN $G_{s,t}^{III}$ and $G_{s,t}^{PP}$ when finding a subset of their bridge edges $L^0 = \{l_\xi^0\}$ in state Γ_i^0 will be transformed accordingly into conditional estimated RG BN $G_{s,t}^{III} / \Gamma_i^0$ and $G_{s,t}^{PP} / \Gamma_i^0$, i.e.

$$\begin{cases} G_{s,t}^{III} / \Gamma_i^0 = G_{s,t(i)}^{III} \\ G_{s,t}^{PP} / \Gamma_i^0 = G_{s,t(i)}^{PP} \end{cases} \quad (2)$$

In studies [3,4] it was shown that in order to calculate the upper bound of EPE, the following equality should be applied:

$$P_{s,t}^{BO} = I - P_{s,t}^{HO}, \quad (3)$$

where $P_{s,t}^{HO}$ is the lower bound of discontinuity probability of vertices s and t in RG BN.

For the specified conditions, it is required to prove the validity of application formulas of the following form for calculation of CP upper and lower bounds of analyzed RG BN:

$$P_{s,t}^{BO} = I - \left[P_{s,t}^{HO} = \sum_{i=1}^{m_{\Gamma^0}} P_{s,t(i)}^{HO} = \sum_{i=1}^{m_{\Gamma^0}} P(\Gamma_i^0) \overline{P(G_{s,t(i)}^{III} / \Gamma_i^0)} \right], \quad (T. 1)$$

$$P_{s,t}^{HO} = \sum_{i=1}^{m_{\Gamma^0}} P_{s,t(i)}^{HO} = \sum_{i=1}^{m_{\Gamma^0}} P(\Gamma_i^0) P(G_{s,t(i)}^{PP} / \Gamma_i^0), \quad (T. 2)$$

where $P(\Gamma_i^0)$ is the probability of the i -th state of a subset of bridge edges $L^0 = \{l_\xi^0\}$, $\xi = \overline{1, |m_{L^0}|}$;

$\overline{P(G_{s,t}^{III} / \Gamma_i^0)}$ is the conditional probability of discontinuity of vertices S and t of RG BN under SP, corresponding to hypothesis Γ_i^0 . For the sake of brevity of notation, we shall designate this probability as $P(G_{s,t_i}^{III})$, where $G_{s,t_i}^{III} = G_{s,t}^{III} / \Gamma_i^0$,

$P(G_{s,t}^{III} / \Gamma_i^0)$ is the conditional probability of connection of vertices S and t RG BN under SC, corresponding to hypothesis Γ_i^0 . This estimation shall be designated as $P(G_{s,t_i}^{III})$, where $G_{s,t_i}^{III} = G_{s,t}^{III} / \Gamma_i^0$;

$$P_{s,t_i}^{HO} = P(\Gamma_i^0) \overline{P(G_{s,t}^{III} / \Gamma_i^0)} \quad (T.3)$$

(T3) is the probability of discontinuity of vertices S and t of analyzed RG BN under SP provided that RG BN is in state Γ_i^0 .

The proof

As the set of hypotheses (states) $\Gamma_i^0 = \{\Gamma_i^0\}, i = \overline{1, m_{\Gamma^0}}$ of a subset of bridge edges $L^0 = \{l_\xi^0\}, \xi = \overline{1, m_{L^0}}$, form a full group of disjoint events, and conditional RG BN (2) can be formed only according to one of the hypotheses $\Gamma_i^0, i = \overline{1, m_{\Gamma}}$, then according to the contents of the formula for full probability [2], equality (T.1) and (T. 2) are determined correctly. The theorem has been proved.

The consequence

For $\xi=1, \Gamma^0=2^1=2: \Gamma_1^0=l_1, \Gamma_2^0=\bar{l}_1$.

Then:

$$P_{s,t}^{BO} = 1 - \left[P_{s,t}^{HO} = \sum_{i=1}^2 P_{s,t_i}^{HO} = \sum_{i=1}^2 P(\Gamma_i^0) \overline{P(G_{s,t_i}^{III} / \Gamma_i^0)} \right], \quad (4)$$

$$\text{where } P_{s,t_i}^{HO} = P(\Gamma_i^0) P(G_{s,t}^{III} / \Gamma_i^0), \quad (5)$$

$$P_{s,t}^{HO} = \sum_{i=1}^2 P_{s,t_i}^{HO} = \sum_{i=1}^2 P(\Gamma_i^0) P(G_{s,t_i}^{III} / \Gamma_i^0), \quad (6)$$

At $\xi=2, \Gamma^0=2^2=4: \Gamma_1^0=l_1 \cdot l_2; \Gamma_2^0=\bar{l}_1 \cdot l_2; \Gamma_3^0=l_1 \cdot \bar{l}_2; \Gamma_4^0=\bar{l}_1 \cdot \bar{l}_2$.

For this alternative:

$$P_{s,t}^{BO} = 1 - \left[P_{s,t}^{HO} = \sum_{i=1}^4 P_{s,t_i}^{HO} = \sum_{i=1}^4 P(\Gamma_i^0) \overline{P(G_{s,t_i}^{III} / \Gamma_i^0)} \right], \quad (7)$$

$$\text{where } P_{s,t}^{HO} = \sum_{i=1}^4 P_{s,t_i}^{HO} = \sum_{i=1}^4 P(\Gamma_i^0) P(G_{s,t_i}^{III} / \Gamma_i^0), \quad (8)$$

etc.

The probability of hypothesis Γ_i^0 we shall determine as follows:

$$P(\Gamma_i^0) = \prod_{\xi \in \beta_1} P(l_\xi^0) \prod_{\xi \in \beta_2} q(l_\xi^0), \quad (9)$$

where β_1 and β_2 are designations according to subsets of operable and failed bridge edges forming hypothesis Γ_i^0 ;

$P(l_\xi^0)$ is the probability of finding the shared edge l_ξ^0 in operable state, $q(l_\xi^0) = 1 - P(l_\xi^0)$.

Calculation of conditional probabilities $P(G_{s,t_i}^{III})$ and $P(G_{s,t_i}^{IV})$ is also feasible according to the structures of conditional estimated RG BN under SP – G_{s,t_i}^{III} and under SC – G_{s,t_i}^{IV} , obtained accordingly from estimated RG BN $G_{s,t}^{III}$ and $G_{s,t}^{IV}$ provided that the subset $L^0 = \{l_\xi^0\}$ of shared edges is in Γ_i state.

Let us show that the application of a combinatorial method eliminates mutual crossing of EPE. With this purpose we shall formulate and prove the following statement.

The statement

It is given: initial RG BN (fig. 1) and its estimated RG BN (fig. 2a and fig. 2b) for calculation of the upper estimate $P_{s,t}^{BO}$ and the lower estimate $P_{s,t}^{HO}$ of connection probability accordingly. If the offered combinatory method is applied to calculation of $P_{s,t}^{BO}$ and $P_{s,t}^{HO}$, then bilateral estimations of CP received at the i -th iterative steps do not overlap.

We need to prove:

$$P_{s,t}^{BO}(\Gamma_i^0) > P_{s,t}^{HO}(\Gamma_i^0), \quad (\text{U. 1})$$

for all values $0 < p(l_\xi) < 1$.

The proof

As all the possible hypotheses $\Gamma^0 = \{\Gamma_i^0\}$ used for definition of the upper and lower bounds of EPE are identical and make up a full group, then according to a Moore-Shannon decomposition formula the inequality $P_{s,t}^{BO}(\Gamma_i^0) > P_{s,t}^{HO}(\Gamma_i^0)$ is true for each i -th hypothesis for all values $0 < p(l_\xi) < 1$. The statement has been proved.

To illustrate the content of the offered method for analysis of bilateral EPE, we shall use two-bridge RG BN with continuous numbering of elements, fig. 1 [3].

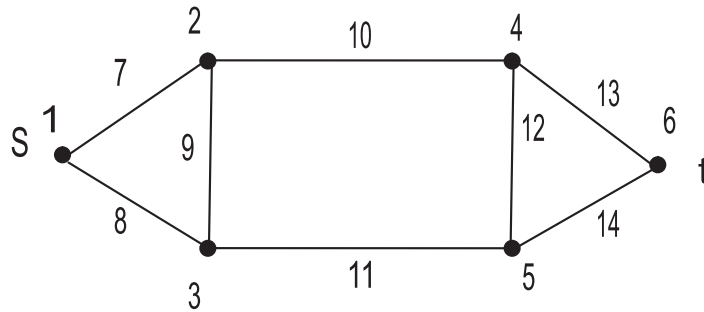


Fig. 1. Two-bridge RG BN with continuous numbering of elements

Structural elements in fig. 1 have only digital designations. This RG BN is characterized by a set of SP (fig. 2, a) of the following form:

$$M_{s,t} = \left\{ M_{n=1} = (7,10,13), M_{n=2} = (8,11,14), M_{n=3} = (7,10,12,14), M_{n=4} = (7,9,11,14), \right. \\ \left. M_{n=5} = (8,9,10,13), M_{n=6} = (8,11,12,13), M_{n=7} = (7,9,11,12,13), M_{n=8} = (8,9,10,12,14) \right\}, \quad (10)$$

determining the upper bound of EPE and also by a set of SC (fig. 2, b) having the following form:

$$R_{s,t} = \left\{ \begin{array}{l} r_{n=1} = (7,8), r_{n=2} = (10,11), r_{n=3} = (13,14), r_{n=4} = (8,9,10), r_{n=5} = (11,12,13), \\ r_{n=6} = (7,9,11), r_{n=7} = (10,12,14), r_{n=8} = (8,9,12,13), r_{n=9} = (7,9,12,14) \end{array} \right\}, \quad (11)$$

determining the lower bound of EPE.

Bridge edges 9 and 12 presented in fig. 2, a and 2, b are marked by thin double lines.

As the structure of initial RG BN (fig. 1) has two bridge edges (9 and 12), then the full group of disjoint states (hypotheses) of these edges will take the form:

$$\Gamma^0 = \{ \Gamma_1^0 = (9 \cdot 12); \Gamma_2^0 = (\bar{9} \cdot 12); \Gamma_3^0 = (9 \cdot \bar{12}); \Gamma_4^0 = (\bar{9} \cdot \bar{12}) \}. \quad (12)$$

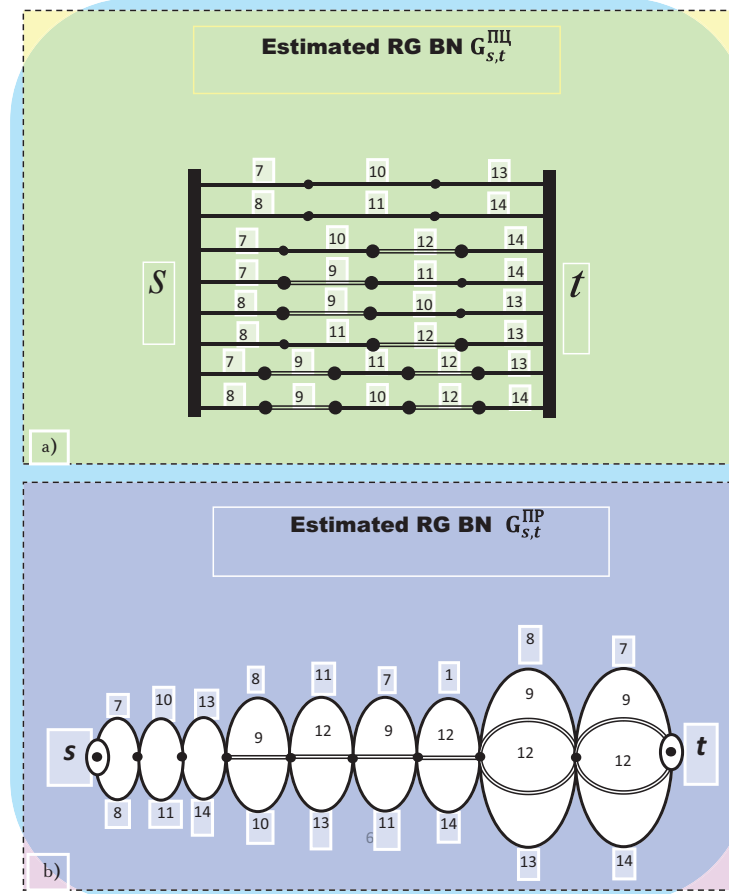


Fig. 2. Diagrams of estimated RG BN for EPE: a) under IIII; b) under IIP

In view of the full group of disjoint states (10), transformation of initial estimated RG BN $G_{s,t}^{IIII}$ (fig. 2, a) in conditional estimated RG BN G_{s,t_i}^{IIII} , presented in fig. 3 was carried out. And also, transformation of initial estimated RG BN $G_{s,t}^{IIP}$ (fig. 2, b) in conditional estimated RG BN G_{s,t_i}^{IIP} , presented in fig. 4 was made.

On presented conditional RG BN (fig. 3 and fig. 4) dark circles mean connection of adjacent vertices in the shared point over special edges 9 and 12 when these edges are in upstate. If these edges are in down state, then breaks are formed in corresponding elementary constructions (SP and SC) which in the mentioned above figures are represented by dashed lines.

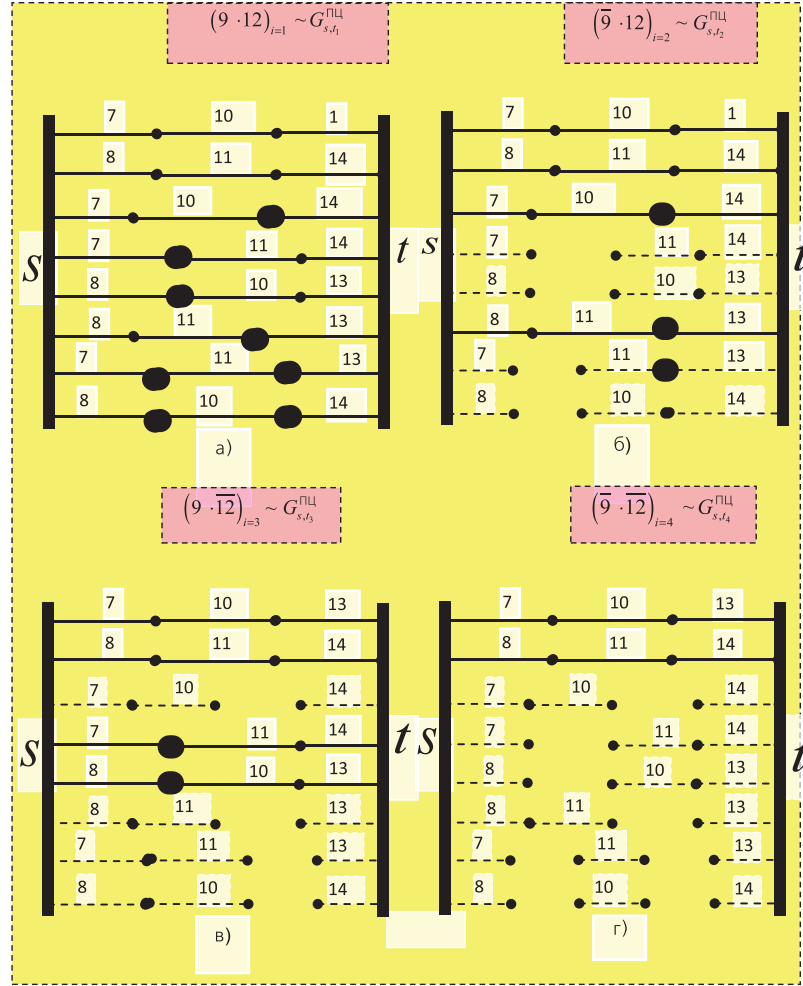


Fig. 3. Transformation of estimated RG BN $G_{s,t}^{III}$ at acceptance of the i -th hypotheses

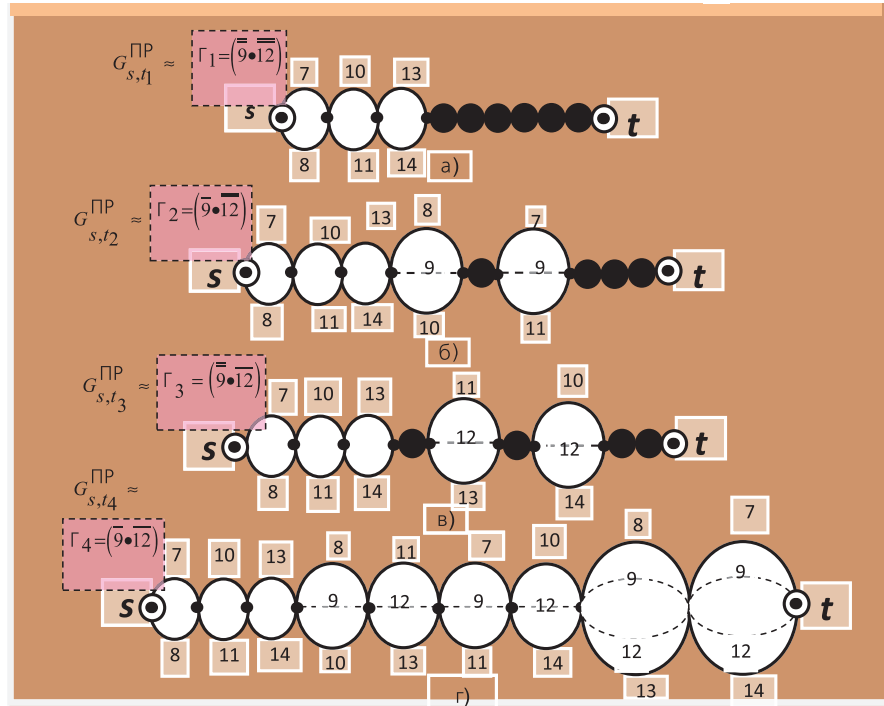


Fig. 4. Transformation of estimated RG BN $G_{s,t}^{III}$ at acceptance of the i -th hypotheses

The formulated and proved statements concerning validity of a combinatory method application for elimination of EPE mutual overlapping shall be confirmed by the following computing experiment.

Let us calculate upper $P_{s,t}^{BO}$ and lower $P_{s,t}^{HO}$ bounds of CP RG BN (fig. 1) for the following initial data (ID) on dependability of edges $p_{\xi=7,14} = 0,5$.

For accepted ID, estimation (5), in view of equality (7), shall be determined in the following form:

$$P_{s,t}^{HO} = 0_{i=0} + 0,085902228_{i=1} + 0,14654541_{i=2} + 0,14654541_{i=3} + 0,19140625_{i=4} = 0,570399298. \quad (13)$$

Then, according to (13), we shall determine monotonous convergence $P_{s,t}^{BO}$ to $P_{s,t}$ as follows:

$$\begin{aligned} P_{s,t}^{BO} \rightarrow P_{s,t} &= 1_{i=0} \rightarrow \left(1 - 0,085902228_{i=0,1} = \underline{\underline{0,914097772}}\right)_{i=0,1} \rightarrow \\ &\rightarrow \left(1 - 0,232447638_{i=0,2} = \underline{\underline{0,767552365}}\right)_{i=0,2} \rightarrow \left(1 - 0,378993048_{i=0,3} = \right. \\ &= \underline{\underline{0,621006952}}\left.)_{i=0,3} \rightarrow \left(1 - 0,570399298_{i=0,4} = \underline{\underline{0,429600702}} = P_{s,t}^{BO}\right)_{i=0,4}. \end{aligned} \quad (14)$$

For accepted ID $p_{\zeta=7,14} = 0,5 = q_{\zeta=7,14}$ the lower bound CP of analyzed RG BN (Fig. 1) according to (8) will be equal to:

$$\begin{aligned} P_{s,t}^{HO} &= 0_{i=0} + 0,10546875_{i=1} + 0,059326171_{i=2} + 0,059326172_{i=3} + 0,018771171_{i=4} = \\ &= 0_{i=0} \rightarrow \underline{\underline{0,10546875}}_{i=1} \rightarrow \underline{\underline{0,164794921}}_{i=1,2} \rightarrow \underline{\underline{0,224121092}}_{i=1,3} \rightarrow \underline{\underline{0,242892263}}_{i=1,4}. \end{aligned} \quad (15)$$

On the basis of equality (14) and (15), fig. 5 presents graphs of EPE monotonous convergence to the exact value $P_{s,t}^{HO} \rightarrow P_{s,t} \leftarrow P_{s,t}^{BO}$ for initial RG BN, fig. 1. In fig. 5 “asterisk” shows step-by-step convergence of the following error $P_{s,t_i} \approx (P_{s,t_i}^{BO} + P_{s,t_i}^{HO}) / 2$ to the exact value $P_{s,t}$.

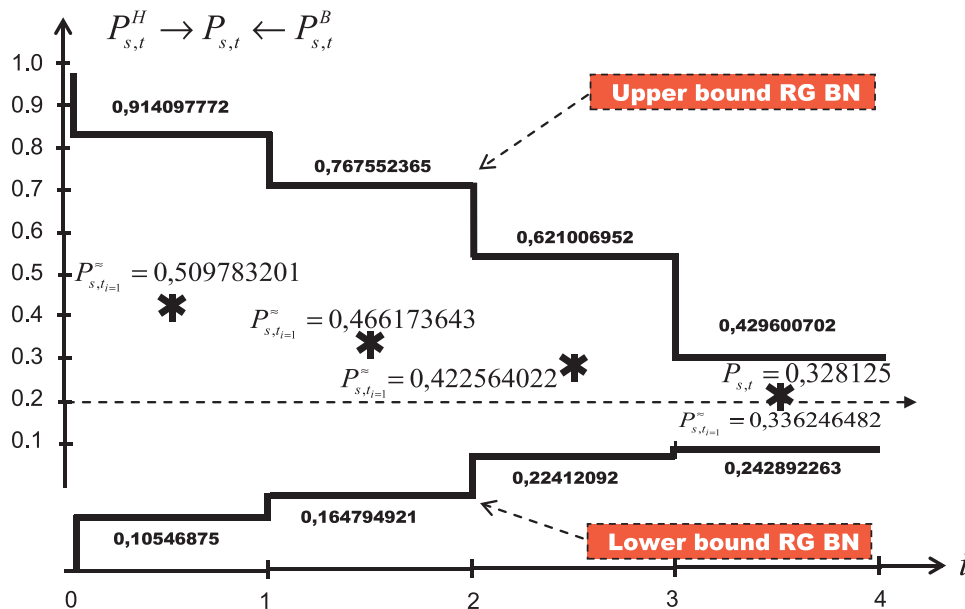


Fig. 5. Illustration of EPE monotonous convergence to the exact value

Fig. 6 presents graphic interpretation of basic EPE in dynamics of their step-by-step change, with regard to RG BN analysis (fig. 1) and ID of the following kind $P_{\xi=7,14} = 0,5 = q_{\xi=7,14}$ [3].

The analysis of the results of the executed numerical experiment presented in fig. 5 and their comparison with basic EPE (fig. 6) shows that the offered combinatory method of the analysis provides elimination of mutual crossing and reduction of CP RG BN errors in relation to basic EPE.

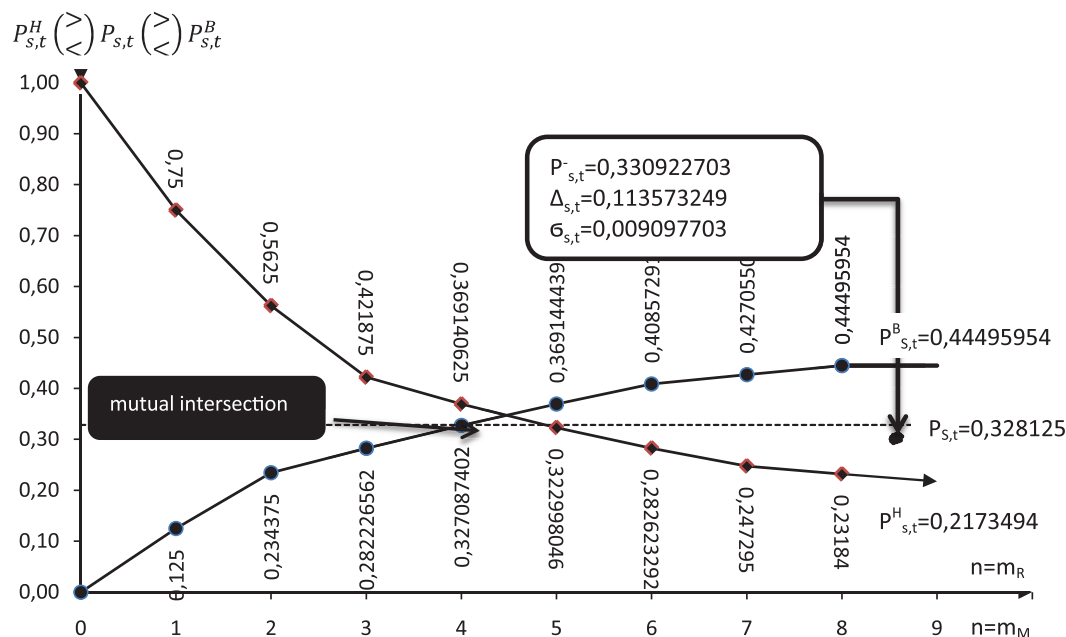


Fig. 6. Illustration of basic EPE crossing

References

1. **Esary J., Proschan F.** Coherent Structures of Non-Identical Components // Technometrics. 1963. V.5. № 2. P. 191-209.
2. **Polessky V.P.** Decoupling of clutters, correlated inequalities and boundaries of combinatory dependability // Problems of information transfer. 1997. V.33. Issue.3. pp. 50-70.
3. **Filin B.P.** About maximum decoupling of clutters in Polessky's estimations of combinatory dependability boundaries of random binary systems // Automatics and telemechanics. 2005. # 9. pp. 149-189.
4. **Filin B.P.** Methods of communication networks' structural dependability analysis. M.: Radio and communication, 1998.
5. **Ryabinin I.A.** Dependability and safety of structural – complex systems. St. Petersburg: Polytechnics, 2000.
6. **Krivulets V.G.** About assessment of Esary-Proschan estimates in problems of the analysis of communication networks structural dependability // Proceeding of the 55-th Scientific session devoted to Radio Day./ RNTORES. 2000.
7. **Nosov M.V.** Marginal valuation of dependability of systems with network structure. / Dependability. 2010. # 2.
8. **Nosov M.V.** Practical application of the theory of marginal ratings. // Dependability 2010. №3.
9. **Netes V.A.** About an estimation of connectivity probability of bipolar networks / Telecommunications. 2001. # 11, pp. 39-41.
10. **Shubinsky I.B.** Structural dependability of information systems. M: "Dependability Journal", 2012. 216 p.
11. **Shubinsky I.B.** Functional dependability of information systems. M: "Dependability Journal", 2012. 295 p.
12. **Moore R., Shannon K.** Reliable circuits out of unreliable relays / Works in the theory of information and cybernetics. M.: SILT, 1963, p. 114-153.



Пегушин С.Л., Шумихин А.Г.

ПРИМЕНЕНИЕ ТАКТИКИ ПОСЛЕДОВАТЕЛЬНЫХ КОНТРОЛЬНЫХ ИСПЫТАНИЙ НА НАДЕЖНОСТЬ ЭЛЕМЕНТОВ АСУ ТП И АВТОМАТИЧЕСКОЙ ПАЗ В УСЛОВИЯХ ЭКСПЛУАТАЦИИ ДЛЯ ЕЕ УЧЕТА ПРИ FMEA – АНАЛИЗЕ

В статье рассмотрена методика применения в условиях эксплуатации для технических средств АСУ ТП и автоматической противоаварийной защиты (ПАЗ) нефтеперерабатывающих производств, основанная на тактике последовательных контрольных испытаний на надёжность, и учета результатов испытаний при анализе отказов и их последствий в соответствии с методологией FMEA – анализа. Предполагается, что условия эксплуатации различных типов технических средств соответствуют режиму «нормального» функционирования системы и экспоненциальному (показательному) закону распределения времени безотказной работы. В нотации IDEF3 структурного моделирования приведено описание процесса испытаний, анализа причин отказов, разработки мероприятий по их предотвращению. Ведение единой базы данных по контрольным испытаниям на надежность осуществляется в PDM-системе.

Ключевые слова: нефтепереработка, автоматизированная система управления, надежность, причины и последствия отказов, анализ.

При эксплуатации комплекса средств АСУ ТП и автоматической ПАЗ возникает необходимость в контроле применяемых технических средств на соответствие показателей их надежности значениям, предусмотренным нормативной и конструкторско-проектной документации (НТД). Для организации такого контроля рассматривается применение в условиях эксплуатации тактики последовательных контрольных испытаний на надежность для экспоненциального закона распределения вероятности отказов [1].

Применение этой методики рассмотрено на примере датчиков давления печи П-2/3 установки селективной очистки масел 37-10 нефтеперерабатывающего производства для следующих исходных данных:

- общее количество датчиков давления $N=14$;
- наработка $t = 4392$ часа;
- риск потребителя $\alpha = 0.05$;
- риск поставщика $\beta = 0.05$;

– браковочное значение контролируемого показателя – времени безотказной работы $T_\beta=10000$ часов (принимается на основе технической документации на оборудование или по согласованию с заказчиком изделий);

– приемочное значение контролируемого показателя $T_\alpha=20000$ часов (принимается на основе технической документации на оборудование или по согласованию с заказчиком);

– отношение $(T_\alpha / T_\beta) = 2$.

В соответствии с методикой [1] определяются границы соответствия:

$$r^+ = a(t_\Sigma / T_\alpha - t_0 / T_\alpha),$$

и несоответствия

$$r^- = at_\Sigma / T_\alpha + r_0,$$

где a – тангенс угла наклона прямой; r – число отказов или число отказавших объектов; r_0 – точка пересечения линии несоответствия с осью ординат; t_Σ – ожидаемая суммарная наработка до принятия решения; t_0 – точка пересечения линии соответствия с осью абсцисс.

В соответствии с планом контроля средних показателей надежности по последовательному методу для экспоненциального распределения, приведенном в [1] для случая $T_\alpha / T_\beta = 2$ и $\alpha = \beta = 0.05$ находятся значения: $a = 1.44$; $r_0 = 4.25$; $t_0 / T_\alpha = 2.94$; $t_\Sigma / T_\alpha = 8.64$; $r_{yc} = 25$ (r_{yc} – предельное число отрицательных исходов при усеченном последовательном контроле).

Ожидаемая суммарная наработка до принятия решения о соответствии (несоответствии) определяется по формуле

$$t_\Sigma = Nt - \sum_{j=1}^r t_{ej}, \quad (1)$$

где t_{ej} – длительность восстановления работоспособного состояния после j -го из r отказов или длительность замены j -го из r отказавших образцов новым; t – наработка, измеряемая в часах.

За интервал наработки $t = 4392$ часа отказов датчиков давления в эксперименте зафиксировано не было и ожидаемая суммарная наработка, вычисленная по формуле (1), составила

$$t_\Sigma = Nt - \sum_{j=1}^r t_{ej} = 14 \cdot 4392 = 61488 \text{ и, соответственно, отношение } t_\Sigma / T_\alpha = 61488 / 20000 \text{ составило } 3.0744.$$

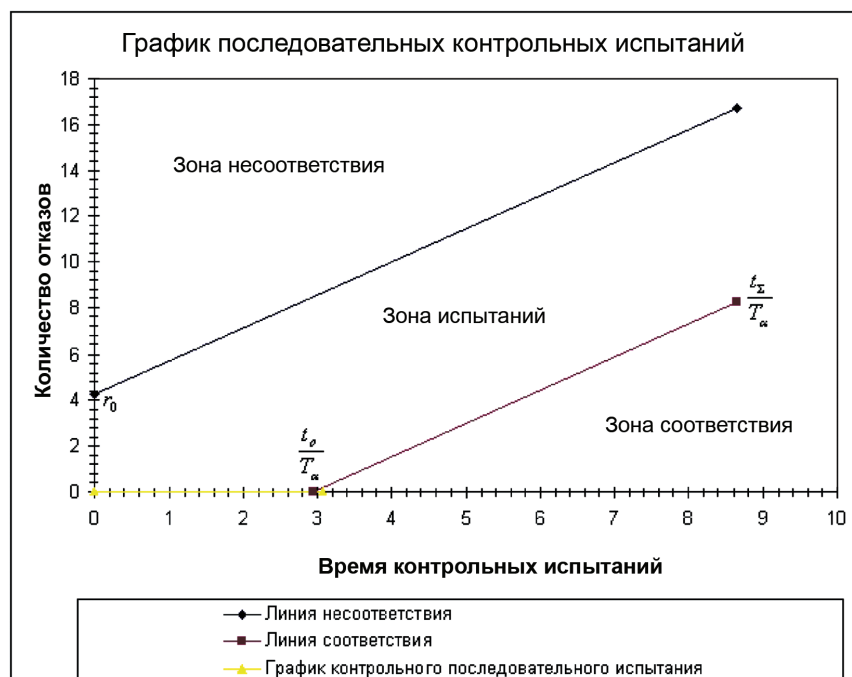


Рис. 1. График последовательных контрольных испытаний для датчиков давления

График контрольных последовательных испытаний для экспоненциального закона распределения, построенный в соответствии с методикой [1], представлен на рис. 1.

Представленный рисунок иллюстрирует, что датчики давления в рассматриваемом примере прошли контрольные испытания при эксплуатации и могут использоваться на нефтеперерабатывающем предприятии.

Информация по результатам контрольных наблюдений, накопленная в единой базе данных, позволяет использовать данные при выборе оборудования для вновь проектируемых и реконструируемых технологических установок нефтепереработки, снизить внеплановые остановки в результате отказа элементов комплекса технических средств за счет соответствующего технического обслуживания.

В случае, если оборудование не прошло контрольные испытания, необходимо проанализировать причины отказов и выработать мероприятия по их устранению. В качестве методологии для анализа причин отказов и их последствий возможно применение FMEA-методологии. Таблица FMEA-анализа имеет следующий вид:

Таблица 1. Пример таблицы FMEA

Вид оборудования	Вид потенциального отказа	Последствия отказа	Значимость отказа	Потенциальные причины отказа	Возникновение отказа	Меры по обнаружению отказа	Обнаружение отказа	Рекомендательные меры	Параметр риска потребителя
Отказ датчика температуры	Неисправность чувствительного элемента измерения	Отсутствие данных на мониторе оператора	4	Обрыв термопары, термометра сопротивления	2	Визуальный осмотр термопары, прозвонка термопары, измерение сопротивления	1	Изучение причины обрыва. Возможно, причины обрыва связаны с монтажными работами на технологическом объекте	8
Отказ датчика температуры	Неисправность HART преобразователя	Отсутствие данных на мониторе оператора	10	Отказ преобразователя	3	Визуальный осмотр, диагностика HART-коммуникатором или AMS	2	Наличие ЗИП	60

Значение коэффициента «Параметр риск потребителя» в таблице определяется как произведение коэффициентов «Значимость», «Возникновение отказа» и «Обнаружение». Коэффициенты для полей «Значимость», «Возникновение отказа», «Обнаружение» устанавливаются на основе экспертных оценок [2].

Описание процесса контрольных испытаний, анализа причин отказов и разработки мероприятий по их предотвращению схематично, в нотации IDEF3 структурного моделирования представлено на рис. 2.

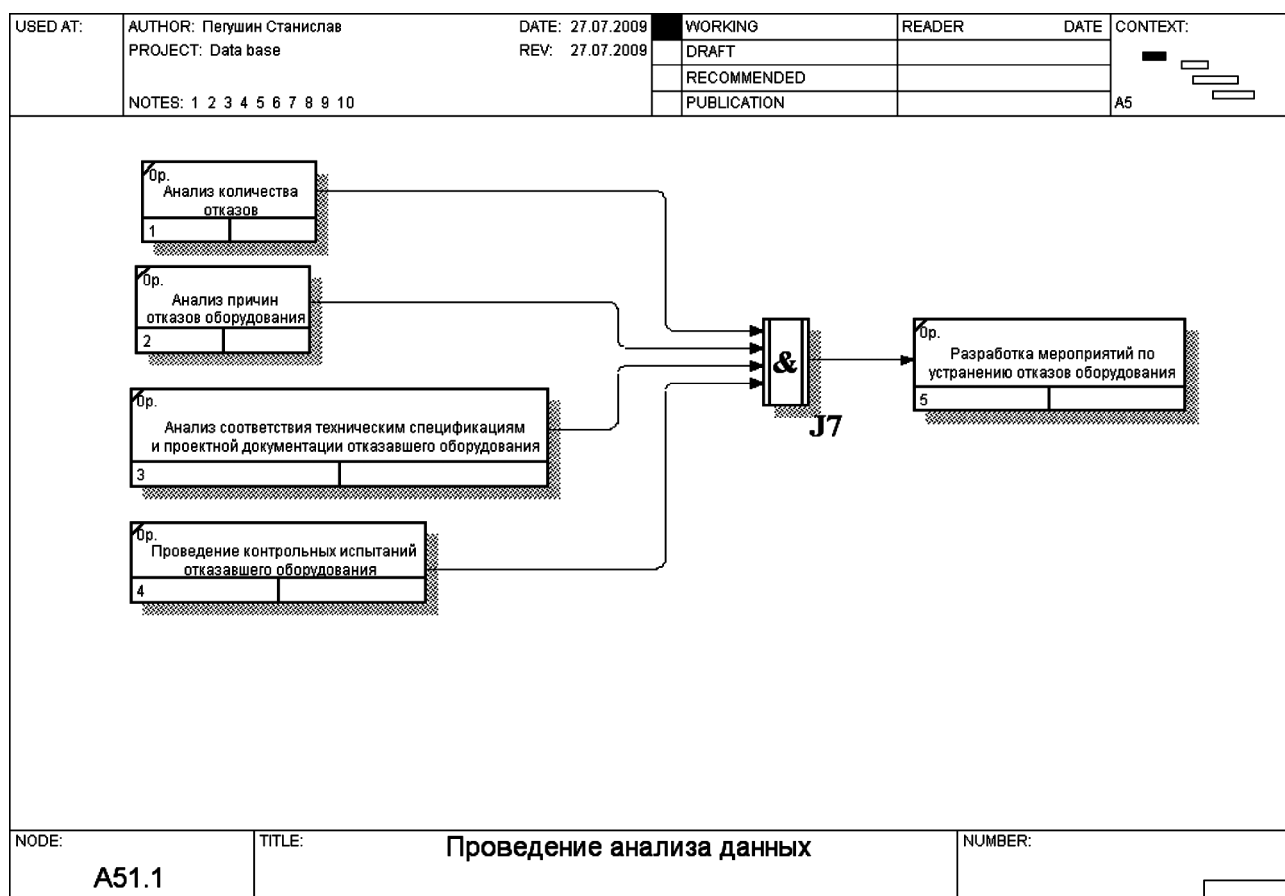


Рис. 2. Схема IDEF3 процесса контрольных последовательных испытаний

Результаты проведения контрольных испытаний хранятся в единой базе данных. Применение единой базы данных позволяет использовать большее количество выборок для проведения контрольных испытаний, что уменьшает вероятность совершить ошибку 1-го или 2-го рода при принятии решения о соответствии (несоответствии) по каждому типу оборудования.

Для создания и введения единой базы данных возможно использование PDM-системы, фрагмент «окна» которой представлен на рис. 3.

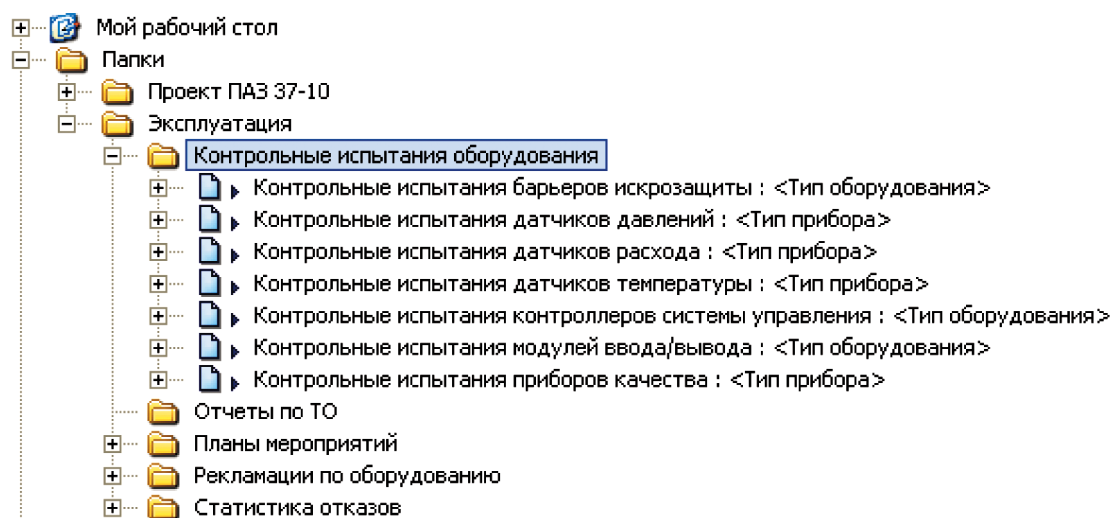


Рис. 3. Фрагмент контрольных испытаний в PDM-системе

Проведение контрольных испытаний позволяет в реальных условиях оценить надежность эксплуатируемого оборудования систем автоматической ПАЗ, разработать мероприятия по устранению выявленных неисправностей и внести соответствующие изменения в проектную и эксплуатационную документации, с целью совершенствования конфигурации систем и регламентов технического обслуживания.

Литература

1. ГОСТ 27.410-87. Надежность в технике. Методы контроля показателей надежности и планы контрольных испытаний на надежность.
2. ГОСТ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.
3. Приказ Ростехнадзора от 11.03.2013 N 96 «Об утверждении Федеральных норм и правил в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» (Зарегистрировано в Минюсте России 16.04.2013 N 28138).



Pegushin S.L., Shumikhin A.G.

APPLICATION OF THE TACTICS OF DEPENDABILITY CONSECUTIVE CHECK TESTS OF CAM ELEMENTS AND AUTOMATED SIS UNDER OPERATING CONDITIONS FOR USE OF RESULTS IN FMEA ANALYSIS

The paper considers the technique based on the tactics of consecutive check tests of dependability and applied for the equipment of computer-aided manufacturing (CAM) and automated safety instrumented systems (SIS) of oil refineries under operating conditions, with subsequent use of testing results in failure mode and effects analysis (FMEA). It is supposed that operation conditions for various types of equipment correspond to a mode of system "regular" functioning and to the exponential law of distribution of mean time to failure. The IDEF3 notation of structural modeling describes the testing process, analysis of failure causes, and development of measures to prevent them. A common database on dependability check tests is kept in PDM (Product Data Management) system.

Keywords: oil refining, automated control system, dependability, failure causes and effects, analysis.

The maintenance of CAM and automated SIS technological complexes brings necessity in control of engineering means as to compliance of their dependability parameters to the values stipulated in regulatory documents and specifications. To establish such control, application of the tactics of dependability consecutive check tests under operating conditions is considered for the exponential law of failure probability distribution [1].

Application of this technique is considered using the example of P-2/3 furnace pressure sensors of the 37-10 oil refining installation for selective oil cleaning for the following initial data:

- total of pressure sensors;
- lifetime $t = 4392$ h;
- consumer risk $\alpha = 0.05$;
- producer risk $\beta = 0.05$;
- rejection value of the controllable parameter – time to failure $T_\beta = 10000$ hours (accepted on the basis of specifications for equipment or as agreed with the customer of products);
- acceptance value of the controllable parameter $T_\alpha = 20000$ hours (accepted on the basis of specifications for equipment or as agreed with the customer);
- ratio $(T_\alpha / T_\beta) = 2$.

Boundaries of compliance are determined according to technique [1]:

$$r^+ = a(t_{\Sigma} / T_{\alpha} - t_0 / T_{\alpha}),$$

and boundaries of discrepancy are determined as follows

$$r^- = at_{\Sigma} / T_{\alpha} + r_0,$$

where α is the tangent of inclination of line; r is the number of failures or failed objects; r_0 is the point of discrepancy line crossing with ordinate axis; t_{Σ} is the expected total time to failure before decision-making; t_0 is the point of line compliance crossing with abscissa axis.

According to the plan of control of average dependability indices by a consecutive method for exponential distribution presented in [1] for the case $T_{\alpha} / T_{\beta} = 2$ and $\alpha = \beta = 0.05$, the values are determined as $a = 1.44$; $r_0 = 4.25$; $t_0 / T_{\alpha} = 2.94$; $t_{\Sigma} / T_{\alpha} = 8.64$; $r_{yc} = 25$ (r_{yc} is the limiting number of negative outcomes at the truncated consecutive control).

The expected total time to failure before decision-making about compliance (discrepancy) is determined under the following formula

$$t_{\Sigma} = Nt - \sum_{j=1}^r t_{ej}, \quad (1)$$

where t_{ej} is the recovery time of upstate after the j -th failure from r failures or duration of the j -th specimen replacement from r failed specimens by new ones; t is the time to failure measured in hours.

For the interval of time to failure $t = 4392$ hours, there have not been registered any failures of pressure sensors in the experiment, and the expected total time to failure calculated under formula (1), has made up $t_{\Sigma} = Nt - \sum_{j=1}^r t_{ej} = 14 \cdot 4392 = 61488$ and, accordingly, the ratio $t_{\Sigma} / T_{\alpha} = 61488 / 20000$ has made up 3.0744.

The diagram of consecutive check tests for the exponential law of distribution, constructed according to technique [1], is presented in fig. 1.

The presented figure illustrates that pressure sensors in the example under consideration have passed check tests at operation and can be used at an oil refining enterprise.

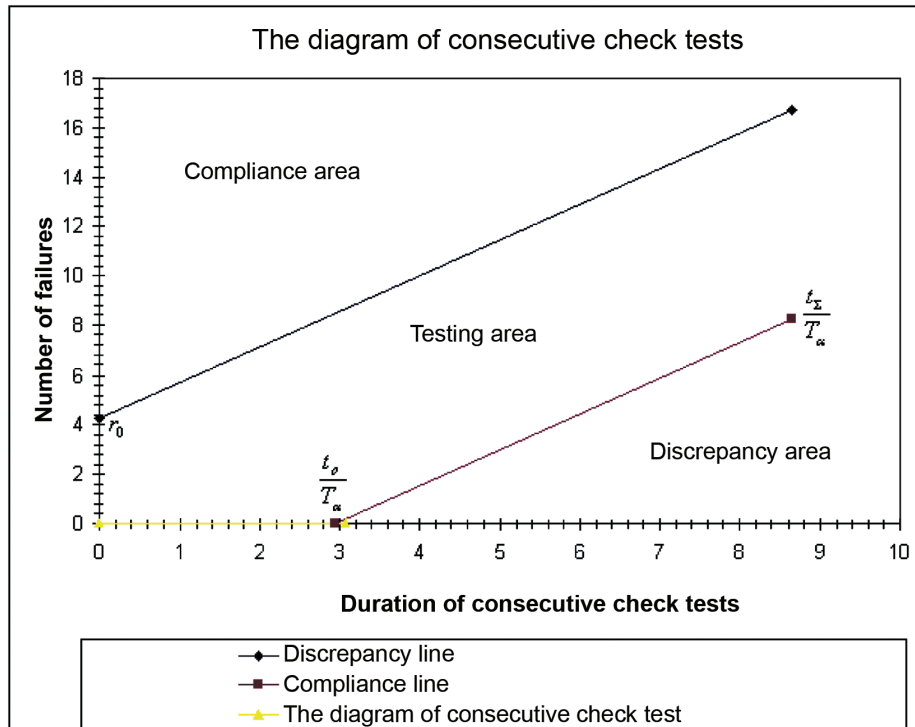


Fig. 1. The diagram of consecutive check tests for pressure sensors

The information about the results of control observations accumulated in the common database allows us to use the data to select equipment for newly designed and reconstructed technological installations of oil refining, to reduce off-schedule stops as a result of technological complex element failure due to respective maintenance.

In case the equipment has not passed check tests, it is necessary to analyze failure causes and to develop actions for their elimination. It is possible to use FMEA-methodology as a methodology for failure causes analysis and their effects. The table of the FMEA-analysis has the following form:

Table 1. Example of FMEA table

Equip- ment type	Potential failure mode	Failure effects	Failure signifi- cance	Potential failure cause	Failure occu- rence	Actions of fail- ure detection	Failure detec- tion	Recommended actions	Consumer risk pa- rameter
Tem- perature transduc- er failure	Failure of mea- surement compo- nent	Absence of data on operator monitor	4	Thermocou- ple break of resistance thermometer	2	Visual survey of the thermo- couple, thermo- couple ringup, measurement of resistance	1	Studying the causes of break- age. Probably, causes of break- age are connect- ed to installation works on techno- logical object	8
Tem- perature transduc- er failure	Malfunc- tion of HART converter	Absence of data on operator monitor	10	Conversion device fail- ure	3	Visual survey, diagnostics by HART- commu- nicator or AMS	2	Presence of spare parts	60

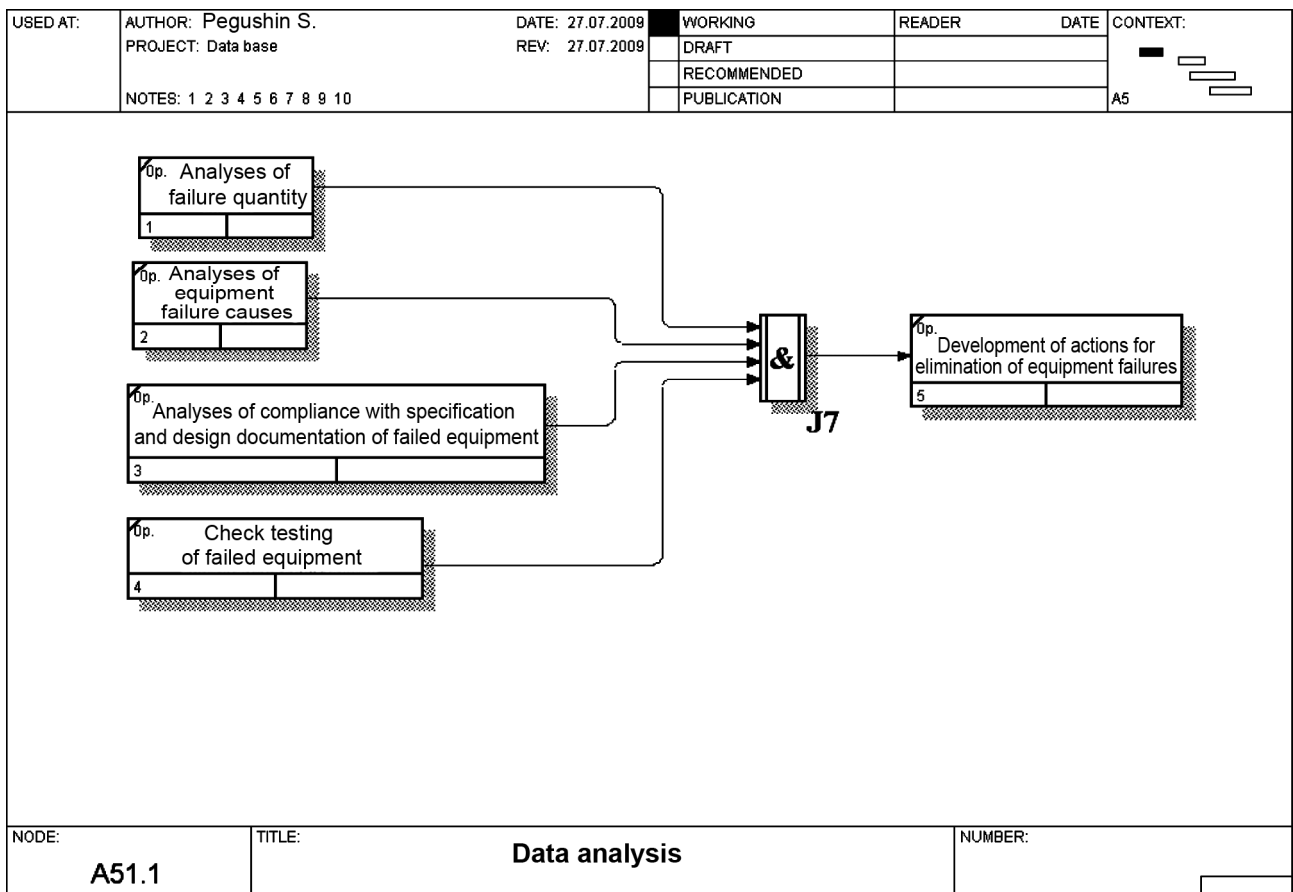


Fig. 2. IDEF3 scheme of consecutive check test process

The value of the factor “Consumer risk parameter” in the table is defined as product of factors «Importance», “Failure occurrence” and «Failure detection». Factors for the fields «Importance», “Failure occurrence” and «Failure detection» are established based on expert estimations [2].

The description of the check test process, the analysis of failure causes and development of actions on their prevention, schematically is presented in fig. 2 in the IDEF3 notation of structural modeling.

Results of check tests are stored in a common database. Application of a common database allows us to use a lot of samples for carrying out check tests, which reduces a probability to make a mistake of the 1-st or 2-nd kind at decision-making on compliance (discrepancy) for each type of equipment.

For creation and introduction of a common database it is possible to use PDM-system, whose «win-
dow» fragment is shown in fig. 3.

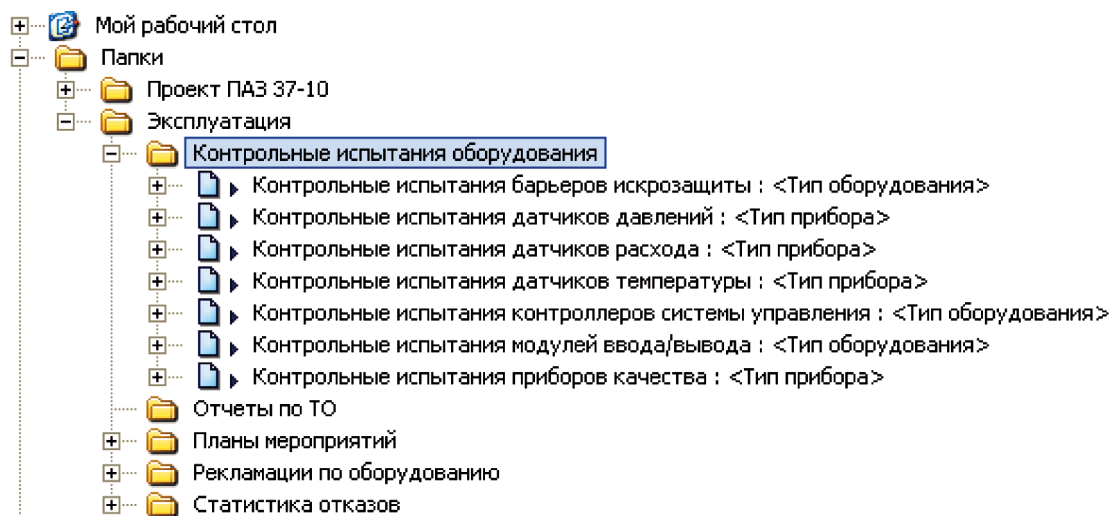


Fig. 3. A fragment of check tests in PDM-system

Carrying out control tests allows us to estimate in real conditions the dependability of operating equipment in automated SIS, to developing actions for elimination of revealed malfunctions and to bring appropriate alterations to designing and operational documentation with the purpose of perfection of a system configuration and maintenance regulations.

References

1. GOST 27.410-87. Dependability in technology. Methods of control of dependability indices and plans of dependability check tests.
2. GOST 27.310-95. Dependability in technology. Failure mode, effect and criticality analysis. Basic provisions
3. Rostekhnadsor Order of 11.03.2013 No.96 “About the adoption of Federal regulations and rules in the field of industrial safety “The general explosion safety rules for explosion and fire-hazardous chemical, petrochemical and oil refining manufactures” (It is registered in Ministry of Justice of Russia 16.04.2013 No.28138).

**Шубинский И.Б.**

МЕТОДЫ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ ПРОГРАММ

В статье рассматриваются основные аспекты построения надежного программного обеспечения. Обсуждаются методы и способы предупреждения ошибок на основе защитного и многоверсионного программирования, средства пассивного и активного обнаружения ошибок, принципы и методы исправления ошибок на основе динамической избыточности и рестарта. Большое внимание в статье уделяется решению задач построения программ устойчивых к ошибкам с помощью методов отступления, методов изоляции ошибок и построения избыточных алгоритмов не критичных к различного рода нарушениям информационного процесса.

Ключевые слова: программа, ошибка, надежность программ, предупреждение ошибок, обнаружение ошибок, исправление ошибок, устойчивость к ошибкам, защитное программирование, многоверсионное программирование, рестарт, динамическая избыточность, алгоритмическая избыточность, изоляция ошибок.

1. Введение

Функциональная надежность информационных систем в значительной мере зависит от надежности программных средств [1]. Все принципы и методы обеспечения функциональной надежности программ, в соответствии с их целью, можно разделить на четыре группы: **предупреждение ошибок, обнаружение ошибок, исправление ошибок и обеспечение устойчивости к ошибкам** (рис. 1). К первой группе относятся принципы и методы, позволяющие минимизировать или вообще исключить ошибки. Методы второй группы сосредоточивают внимание на функциях самого программного обеспечения, помогающих выявлять ошибки. К третьей группе относятся функции программного обеспечения, предназначенные для исправления ошибок или их последствий. Устойчивость к ошибкам (четвертая группа) – это мера способности системы программного обеспечения продолжать функционирование при наличии ошибок.

2. Предупреждение ошибок

К этой группе относятся принципы и методы, цель которых – не допустить появления ошибок в готовой программе. Должно быть очевидно, что предупреждение ошибок – оптимальный путь к достижению надежности программного обеспечения. Лучший способ обеспечить надежность



Рис. 1. Основные аспекты построения архитектуры надежного программного обеспечения

– прежде всего не допустить возникновения ошибок. С этой целью широко применяют способы так называемого **защитного (безопасного) программирования**, направленного на уменьшение вероятности ошибок в программах, а также **многоверсионное программирование**.

Под **защитным программированием** понимают ограничение неправильного использования программных объектов. Другими словами, выдвигается требование проектировать и программировать таким образом, чтобы не только гарантировать ожидаемое использование программы в строгом соответствии со спецификациями, но и сделать невозможным ее неправильное использование. Например, при проектировании системы, в которой взаимодействуют много модулей, мы можем потребовать, чтобы какие-то взаимодействия между ними разрешались лишь в определенных ситуациях. Таким образом, вызов модулем А модуля В может быть разрешен всегда, в определенных ситуациях или же никогда, несмотря на то, что модули А и В находятся в таких отношениях, что вызов возможен.

Защитное программирование – технология предупреждения потенциальных ошибок путем проверки в каждом модуле множества допустимых условий. Во время программирования может быть использовано много технических приемов, чтобы проверить аномалии в управлении или в данных. Ниже перечислены некоторые из методов безопасного программирования:

- анализируются граничные значения переменных;
- проверяются размеры, тип и диапазон параметров процедуры ввода данных;
- параметры “только для доступ к ним чтения” и “считывание-запись” должны быть разделены, и должен быть проверен доступ к ним;
- символьные константы не должны быть доступны для записи;
- входные переменные и промежуточные (вспомогательные) переменные с физическим значением должны быть проверены на предмет достоверности;

- воздействие выходных переменных должно быть проверено, предпочтительно непосредственным наблюдением связанных с ними изменений состояния системы и т.д.

Простейший метод защитного программирования заключается в использовании специальных ловушек ошибок, рассчитанных на ошибки типа неправильного использования модулей. Разработчика программы не интересует, что будет делать пользователь после того, как получит сообщение о неправильном использовании модуля, но при этом он обязан спроектировать модуль так, чтобы ошибки пользователя не вызывали необратимых изменений в модуле. Таким образом, пользователь, пойманный на неправильном употреблении модуля, принимает корректирующие действия и снова вызывает модуль, не оставляя никаких следов ошибочных вызовов. Иначе говоря, речь идет о таком программировании, когда программный продукт очень трудно или невозможно использовать за пределами области действия его спецификации.

Многоверсионное программирование (N-версионное программирование). Цель: обнаружить и замаскировать остаточные ошибки проекта программного обеспечения в течение выполнения программ, чтобы предотвратить критически опасные отказы системы, и продолжать работу с высокой надежностью. В многоверсионном программировании данная спецификация программы реализуется по-разному N раз. Те же самые значения входных данных задаются N версиям, и результаты, произведенные N версиями, сравниваются. Если результат считается достоверным, то он передается компьютеру в качестве выходных данных. N версии могут выполняться параллельно на отдельных компьютерах, альтернативно все версии могут выполняться на одном компьютере. Выходные результаты подвергаются внутреннему голосованию. Различные стратегии голосования могут быть использованы на N версиях в зависимости от требований применения. Для критически важных информационных систем необходимо полное согласие всех N версий. Для других информационных систем может быть использована стратегия голосования путем простого большинства. Для случаев, где не имеется коллективного согласия, могут быть использованы вероятностные подходы, чтобы максимизировать шанс выбора правильного значения, например, взяв среднее значение, временно заморозив выходные данные до возвращения согласия, и т.д.

При дуальном программировании (если разрабатываются две версии программы) в случае обнаружения расхождения в результатах, необходимо определить по дополнительным критериям, какой результат правильный и отбросить другой результат. При N-версионном программировании правильный результат определяется по мажоритарному признаку, т.е. выбирается тот результат, который наблюдается в большинстве вариантов программы.

Рассмотренные способы резервирования требуют в 2 или N раз больше времени для вычислений и увеличение объема труда программистов во столько же раз. В связи с этим представляет интерес модифицированное дуальное программирование, при котором наряду с достаточно точной, но сложной основной программой используется менее точная, но простая резервная программа. Если при одинаковых исходных данных результаты работы программ отличаются на величину большую, чем допустимая погрешность, делается предположение, что отказала основная программа, как менее надежная, и в качестве правильного результата принимается результат работы резервной программы.

Гарантировать отсутствие ошибок, однако, невозможно никогда. Другие три группы методов опираются на предположение, что ошибки все-таки будут.

3. Обнаружение ошибок

Если предполагать, что в программном обеспечении какие-то ошибки все же будут, то лучшая (после предупреждения ошибок) стратегия – включить средства обнаружения ошибок в само программное обеспечение.

Большинство методов направлено по возможности на незамедлительное обнаружение сбоев. Немедленное обнаружение имеет два преимущества: можно минимизировать влияние ошибки и последующие затруднения для человека, которому придется извлекать информацию о ней, находить ее и исправлять.

Меры по обнаружению ошибок можно разбить на две подгруппы: *пассивные* попытки обнаружить симптомы ошибки в процессе «обычной» работы программного обеспечения и *активные* попытки программной системы периодически обследовать свое состояние в поисках признаков ошибок.

Пассивное обнаружение. Меры по обнаружению ошибок могут быть приняты на нескольких структурных уровнях программной системы. Здесь мы будем рассматривать уровень подсистем, или компонентов, т.е. нас будут интересовать меры по обнаружению симптомов ошибок, предпринимаемые при переходе от одного компонента к другому, а также внутри компонента. Все это, конечно, применимо также к отдельным модулям внутри компонента.

Разрабатывая эти меры, мы будем опираться на следующее.

1. *Взаимное недоверие.* Каждый из компонентов должен предполагать, что все другие содержат ошибки. Когда он получает какие-нибудь данные от другого компонента или из источника вне системы, он должен предполагать, что данные могут быть неправильными, и пытаться найти в них ошибки.

2. *Немедленное обнаружение.* Ошибки необходимо обнаружить как можно раньше. Это не только ограничивает наносимый ими ущерб, но и значительно упрощает задачу отладки.

3. *Избыточность.* Все средства обнаружения ошибок основаны на некоторой форме избыточности (явной или неявной).

Когда разрабатываются меры по обнаружению ошибок, важно принять согласованную стратегию для всей системы. Действия, предпринимаемые после обнаружения ошибки в программном обеспечении, должны быть единообразными для всех компонентов системы. Это ставит вопрос о том, какие именно действия следует предпринять, когда ошибка обнаружена. Наилучшее решение – немедленно завершить выполнение программы или (в случае операционной системы) перевести центральный процессор в состояние ожидания. С точки зрения предоставления человеку, отлаживающему программу, например системному программисту, самых благоприятных условий для диагностики ошибок немедленное завершение представляется наилучшей стратегией. Конечно, во многих системах подобная стратегия бывает нецелесообразной (например, может оказаться, что приостанавливать работу системы нельзя). В таком случае используется метод *регистрации ошибок*. Описание симптомов ошибки и «моментальный снимок» состояния системы сохраняются во внешнем файле, после чего система может продолжать работу. Этот файл позднее будет изучен обслуживающим персоналом.

Всегда, когда это возможно, лучше приостановить выполнение программы, чем регистрировать ошибки (либо обеспечить как дополнительную возможность работу системы в любом из этих режимов). Различие между этими методами проиллюстрируем на способах выявления причин возникающего иногда скрежета вашего автомобиля. Если автомеханик находится на заднем сиденье, то он может обследовать состояние машины в тот момент, когда скрежет возникает. Если вы выбираете метод регистрации ошибок, задача диагностики станет сложнее.

Активное обнаружение ошибок. Не все ошибки можно выявить пассивными методами, поскольку эти методы обнаруживают ошибку лишь тогда, когда ее симптомы подвергаются соответствующей проверке. Можно делать и дополнительные проверки, если спроектировать специальные программные средства для активного поиска признаков ошибок в системе. Такие средства называются *средствами активного обнаружения ошибок*.

Активные средства обнаружения ошибок обычно объединяются в *диагностический монитор*: параллельный процесс, который периодически анализирует состояние системы, с целью обнару-

жить ошибку. Большие программные системы, управляющие ресурсами, часто содержат ошибки, приводящие к потере ресурсов на длительное время. Например, управление памятью операционной системы сдает блоки памяти «в аренду» программам пользователей и другим частям операционной системы. Ошибка в этих самых «других частях» системы может иногда вести к неправильной работе блока управления памятью, занимающегося возвратом сданной ранее в аренду памяти, что вызывает медленное вырождение системы.

Диагностический монитор можно реализовать как периодически выполняемую задачу (например, она планируется на каждый час) либо как задачу с низким приоритетом, которая планируется для выполнения в то время, когда система переходит в состояние ожидания. Как и прежде, выполняемые монитором конкретные проверки зависят от специфики системы, но некоторые идеи будут понятны из примеров. Монитор может обследовать основную память, чтобы обнаружить блоки памяти, не выделенные ни одной из выполняемых задач и не включенные в системный список свободной памяти. Он может проверять также необычные ситуации: например, процесс не планировался для выполнения в течение некоторого разумного интервала времени. Монитор может осуществлять поиск «затерявшихся» внутри системы сообщений или операций ввода-вывода, которые необычно долгое время остаются незавершенными, участков памяти на диске, которые не помечены как выделенные и не включены в список свободной памяти, а также различного рода странностей в файлах данных.

Иногда желательно, чтобы в чрезвычайных обстоятельствах монитор выполнял диагностические тесты системы. Он может вызывать определенные системные функции, сравнивая их результат с заранее определенным и проверяя, насколько разумно время выполнения. Монитор может также периодически предъявлять системе «пустые» или «легкие» задания, чтобы убедиться, что система функционирует хотя бы самым примитивным образом.

4. Исправление ошибок

Следующий шаг – методы исправления ошибок. После того как ошибка обнаружена, либо она сама, либо ее последствия должны быть исправлены программным обеспечением. Исправление ошибок самой системой – плодотворный метод проектирования надежных систем аппаратного обеспечения. Некоторые устройства способны обнаружить неисправные компоненты и перейти к использованию идентичных запасных. Аналогичные методы неприменимы к программному обеспечению вследствие глубоких внутренних различий между сбоями аппаратуры и ошибками в программах. Если некоторый программный модуль содержит ошибку, идентичные «запасные» модули также будут содержать ту же ошибку.

Другой подход к исправлению связан с попытками восстановить разрушения, вызванные ошибками, например искажения записей в базе данных или управляющих таблицах системы. Польза от методов борьбы с искажениями ограничена, поскольку предполагается, что разработчик заранее предугадает несколько возможных типов искажений и предусмотрит программно реализуемые функции для их устранения. Это похоже на парадокс, поскольку, если знать заранее какие ошибки возникнут, можно было бы принять дополнительные меры по их предупреждению. Если методы ликвидации последствий сбоев не могут быть обобщены для работы со многими типами искажений, лучше всего направлять силы и средства на предупреждение ошибок. Вместо того, чтобы, разрабатывая операционную систему, оснащать ее средствами обнаружения и восстановления цепочки искаженных таблиц или управляющих блоков, следовало бы лучше спроектировать систему так, чтобы только один модуль имел доступ к этой цепочке, а затем настойчиво пытаться убедиться в правильности этого модуля.

5. Устойчивость к ошибкам

Основное допущение программирования, *устойчивого к программным ошибкам*, заключается в том, что как бы хорошо ни была спроектирована и реализована программа, в ней обязательно будет содержаться несколько остаточных ошибок. А раз так, то модули программы, которые могут дать сбой, должны иметь “резервный запас”. С этой целью модуль проектируется в виде *блоков восстановления*. Каждый блок восстановления содержит пропускной тест и один или несколько вариантов реализации. Основной вариант иницируется при вызове блока восстановления, и когда его выполнение завершается, происходит проверка значения пропускного теста. Если он дает «истину», то считается, что выполнение блока восстановления успешно завершено. Если же тест дает «ложь», то иницируется другой вариант, за которым следует определение значения пропускного теста и т.д., и так до успешного выполнения блока восстановления. Если же ни один вариант не прошел пропускного теста, то блок восстановления рассматривается как ошибочный и начинается исполнение другого варианта вызываемого модуля. Применяется также и другой технический прием: написаны, часто независимо, несколько различных сегментов программы, каждый из которых предназначен для выполнения одной функции. Программа строится из этих сегментов. Первый сегмент, называемый *первичным*, выполняется первым. За ним следует приемочное испытание результата вычислений первого сегмента. Если испытание прошло успешно, тогда результат принимается и передается к последующим частям системы. Если испытание было неудачным, любые побочные эффекты первого сегмента сбрасываются, и выполняется второй сегмент, называемый *первым альтернативным*. За ним также следует приемочное испытание, результаты которого рассматриваются как в первом случае. Если необходимо, могут быть реализованы другие альтернативные приемы.

Приведенный способ парирования остаточных ошибок в программе путем проектирования модуля в виде блока восстановления требует порой неоправданных усилий, связанных с проектированием нескольких блоков восстановления, каждый из которых содержит пропускной тест и один или несколько вариантов реализации. В целях практического обеспечения функционирования программной системы при наличии в ней ошибок разработана группа методов, которая разбивается на четыре подгруппы: *динамическая избыточность, методы отступления, методы изоляции ошибок и построение алгоритмов нечувствительных (или не критичных) к различного рода нарушениям информационного процесса (использование алгоритмической избыточности)*.

1. Истоки концепции *динамической избыточности* лежат в проектировании аппаратного обеспечения. Один из подходов к динамической избыточности – *мажоритарное резервирование* (метод голосования). Данные обрабатываются независимо несколькими идентичными устройствами, и результаты сравниваются. Если большинство устройств выработало одинаковый результат, этот результат и считается правильным. И опять, вследствие особой природы ошибок в программном обеспечении ошибка, имеющаяся в копии программного модуля, будет также присутствовать во всех других его копиях, поэтому идея голосования здесь, видимо, неприемлема. Предлагаемый иногда подход к решению этой проблемы состоит в том, чтобы иметь несколько неидентичных копий модуля. Это значит, что все копии выполняют одну и ту же функцию, но либо реализуют различные алгоритмы, либо созданы разными разработчиками. Этот подход бесперспективен по следующим причинам. Часто трудно получить существенно разные версии модуля, выполняющие одинаковые функции. Кроме того, возникает необходимость в дополнительном программном обеспечении для организации выполнения этих версий параллельно или последовательно и сравнения результатов. Это дополнительное программное обеспечение повышает уровень сложности системы, что, конечно, противоречит основной идее предупреждения ошибок – стремиться в первую очередь минимизировать сложность.

Второй подход к динамической избыточности – выполнять эти запасные копии только тогда, когда результаты, полученные с помощью основной копии, признаны неправильными. Если это происходит, система автоматически вызывает запасную копию. Если и ее результаты неправильны, вызывается другая запасная копия и т.д.

2. Вторая подгруппа методов обеспечения устойчивости к ошибкам называется *методами отступления* или сокращенного обслуживания. Эти методы приемлемы обычно лишь тогда, когда для системы программного обеспечения существенно важно корректно закончить работу. Например, если ошибка оказывается в системе, управляющей технологическими процессами, и в результате эта система выходит из строя, то может быть загружен и выполнен особый фрагмент программы, призванный подстраховать систему и обеспечить безаварийное завершение всех управляемых системой процессов. Аналогичные средства часто необходимы в операционных системах. Если операционная система обнаруживает, что вот-вот выйдет из строя, она может загрузить аварийный фрагмент, ответственный за оповещение пользователей у терминалов о предстоящем сбое и за сохранение всех критических для системы данных.

3. Третья подгруппа – *методы изоляции ошибок*. Основная их идея – не дать последствиям ошибки выйти за пределы как можно меньшей части системы программного обеспечения, так, чтобы, если ошибка возникнет, не вся система оказалась неработоспособной; отключаются лишь отдельные функции в системе либо некоторые ее пользователи. Например, во многих операционных системах изолируются ошибки отдельных пользователей, так что сбой влияет лишь на некоторое подмножество пользователей, а система в целом продолжает функционировать. В телефонных переключательных системах для восстановления после ошибки, чтобы не рисковать выходом из строя всей системы, просто разрывают телефонную связь. Другие методы изоляции ошибок связаны с защитой каждой из программ в системе от ошибок других программ. Ошибка в прикладной программе, выполняемой под управлением операционной системы, должна оказывать влияние только на эту программу. Она не должна сказываться на операционной системе или других программах, функционирующих в этой системе.

В информационной системе изоляция программ является ключевым фактором, гарантирующим, что ошибки в программе одного пользователя не приведут к ошибкам в программах других пользователей или к полному выводу системы из строя. Основные правила изоляции ошибок в программах состоят в следующем:

1) Прикладная программа не должна иметь возможности непосредственно ссылаться на другую прикладную программу или данные в другой программе и изменять их.

2) Прикладная программа не должна иметь возможности непосредственно ссылаться на программы или данные операционной системы и изменять их. Связь между двумя программами (или программой и операционной системой) может быть разрешена только при условии использования четко определенных сопряжений и только в случае, когда обе программы дают согласие на эту связь.

3) Прикладные программы и их данные должны быть защищены от операционной системы до такой степени, чтобы ошибки в операционной системе не могли привести к случайному изменению прикладных программ или их данных.

4) Операционная система должна защищать все прикладные программы и данные от случайного их изменения операторами системы или обслуживающим персоналом.

5) Прикладные программы не должны иметь возможности ни остановить систему, ни вынудить ее изменить другую прикладную программу или ее данные.

6) Когда прикладная программа обращается к операционной системе, должна проверяться достоверность всех параметров. Прикладная программа не должна иметь возможности изменить эти параметры между моментами проверки и реального их использования операционной системой.

7) Никакие системные данные, непосредственно доступные прикладным программам, не должны влиять на функционирование операционной системы. Ошибка в прикладной программе, вследствие которой содержимое этой памяти может быть случайно изменено, приводит, в конце концов, к сбою системы.

8) Прикладные программы не должны иметь возможности в обход операционной системы прямо использовать управляемые ею аппаратные ресурсы. Прикладные программы не должны прямо вызывать компоненты операционной системы, предназначенные для использования только ее подсистемами.

9) Компоненты операционной системы должны быть изолированы друг от друга так, чтобы ошибка в одной из них не привела к изменению других компонентов или их данных.

10) Если операционная система обнаруживает ошибку в себе самой, она должна попытаться ограничить влияние этой ошибки одной прикладной программой и в крайнем случае прекратить выполнение только этой программы.

11) Операционная система должна давать прикладным программам возможность по требованию исправлять обнаруженные в них ошибки, а не безоговорочно прекращать их выполнение.

Реализация многих из этих принципов влияет на архитектуру лежащего в основе системы аппаратного обеспечения. Хотя в формулировке многих из них употребляются слова «операционная система», они применимы к любой программе (будь то операционная система, монитор телеобработки или подсистема управления файлами), которая занята обслуживанием других программ.

4. Четвертая подгруппа – *введение алгоритмической избыточности*.

6. Заключение

В статье рассмотрены эффективные методы и способы построения архитектуры функционально надежных программных средств. Использован европейский опыт разработки программ для связанных с безопасностью систем [2], а также рекомендации стандарта [3]. Обеспечение надежности программных средств не ограничивается этапами разработки их спецификации и качественной архитектуры. Для решения ключевой задачи построения надежной информационной системы необходимо спроектировать надежное программное обеспечение, реализовать его, интегрировать с аппаратными средствами, обеспечить надежность программных средств в процессе аттестации, эксплуатации и сопровождения. Эти этапы построения надежной программы являются предметом дальнейшего обсуждения.

Литература

1. Шубинский И.Б. Функциональная надежность информационных систем (Методы анализа). М.: ООО «Журнал «Надежность», 2012, 296с.
2. BS EN 50128:2011. Программное обеспечение для систем управления и защиты на железных дорогах.
3. ГОСТ Р/МЭК 61508–3–2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Требования к программному обеспечению.



Shubinsky I.B.

METHODS OF SOFTWARE FUNCTIONAL DEPENDABILITY ASSURANCE

The paper considers the basic aspects of the construction of reliable software. It discusses methods and ways of error prevention based on protective and multiversion programming, tools of passive and active detection of errors, principles and methods of error correction based on dynamic redundancy and restart. Some emphasis is made on solving the tasks of construction of error-tolerant programs with the help of digression methods, techniques of error isolation and construction of redundant algorithms not critical to various types of information process violations.

Keywords: *a program, an error, software dependability, error prevention, error detection, error correction, error-tolerant software, antialiasing, multiversion programming, restart, dynamic redundancy, algorithmic redundancy, isolation of errors.*

1. Introduction

The functional dependability of information systems substantially depends on software dependability [1]. All principles and methods of software functional dependability assurance in accordance with their purpose can be divided into four groups: **error prevention, error detection, error correction and error tolerance assurance** (fig. 1). Principles and methods allowing to minimize or completely exclude errors belong to the first group. Methods of the second group concentrate on the functions of software itself that help to reveal errors. The third group includes the functions of software intended for correction of errors or their consequences. Error tolerance (the fourth group) is a degree of software system ability to continue functioning in case of errors.

2. Error prevention

This group includes principles and methods, whose purpose is to prevent from occurrence of errors in the ready-made software. It should be obvious that the error prevention is an optimal way to achieve software dependability. The best way to provide dependability is in the first place to prevent from occurrence of errors. To that end, developers widely apply methods of the so-called **antialiasing (safe programming)** designed to reduce the probability of errors in programs, and also **multiversion programming**.

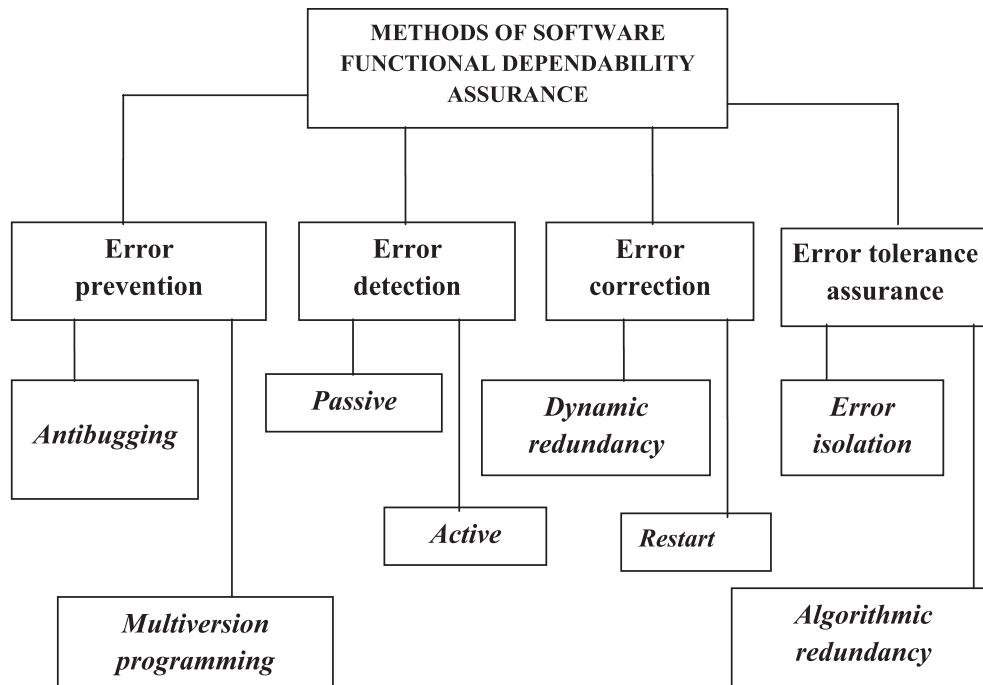


Fig. 1. The basic aspects of construction of the architecture of reliable software

Antibugging is understood as a restriction of misuse of program objects. In other words, the requirement is put forward to designing and programming in such a way that would insure the expected use of the program in strict conformity with specifications, as well as to make its misuse impossible. For example, when designing a system in which many modules interact, we can demand that some interactions between them should be allowed only in certain situations. Thus, module A can request module B always, in certain situations or never in spite of the fact that modules A and B are in such relations that the request is possible.

Antibugging is a technology of potential errors' prevention by checking a set of allowable conditions in each module. During programming many techniques can be used to check up anomalies in control or in data. Some of antibugging methods are listed below:

- boundary values of variables are analyzed;
- the sizes, type and range of parameters of data input procedure are checked;
- parameters "access only to read" and "read-write" should be divided, and access to them should be checked up;
- symbolic constants should not be accessible for writing;
- input variables and intermediate (auxiliary) variables with physical value should be checked up for authenticity;
- influence of output variables should be checked up, preferably by direct observation of changes of a system state connected to them, etc.

The elementary method of antibugging consists in use of special traps for errors intended for errors such as misuse of modules. The developer of the program does not concern about what the user will do after receiving the message on misuse of the module, but he is obliged to design the module so that user errors will not cause irreversible changes in the module. Thus, the user caught on misuse of the module makes adjusting actions and again activates the module, not leaving any traces of erroneous calls. In other words, it implies such programming when it is not so easy or impossible to use the software product outside the scope of its specification.

Multiversion programming (N-version programming). The purpose of this method is to find out and mask residual errors of software design during execution of programs, to prevent critically hazardous

system failures, and to continue operation with high dependability. In N-version programming the given specification of the program is realized differently for N time. The same values of input data are given to N-versions, and then the results made by N-versions are compared. If the result is considered credible, it is transferred to computer as output data. N-versions can be carried out in parallel on separate computers or all versions can alternatively be executed on one computer. Output results are exposed to internal voting. Various strategies of voting can be used on N-versions depending on requirements of application. For critical information systems, the full consent of all N-versions is necessary. For other information systems, the strategy of voting by a simple majority can be used. For cases where there is no collective consent, probabilistic approaches can be used to maximize the chance of choosing a correct value, for example, by taking an average value, temporarily freezing output data before the consent returns, etc.

For dual programming (if two versions of the program are developed), in case of detection of divergence in results, it is necessary to define by additional criteria what result is correct and to reject any other result. For N-version programming, the correct result is defined according to a majority criterion, i.e. we select the result which is observed in the majority of program versions.

The considered ways of redundancy demand twice or N as much time for calculations and increase in labor volume of programmers by as much time. In this reference, of interest is modified dual programming where a sufficiently exact, but complex basic program is accompanied by a less exact, but simple backup program. If for identical initial data the results of programs' execution differ by the value which is higher than the allowable error, the assumption is taken that the basic program has failed as a less dependable one, and the result of backup program execution is accepted as the correct result.

However, it is never possible to guarantee the absence of errors. Other three groups of methods rely on the assumption that errors will nevertheless take place.

3. Error detection

If we assume that any mistakes will nevertheless take place in software, the best strategy (after error prevention) is to include tools for error detection in software itself.

The majority of methods are designed whenever possible for immediate detection of failures. The immediate detection has two advantages: it is possible to minimize error influence and the subsequent difficulties for the person who should extract information about it, to find and to correct it.

Measures related to error detection can be divided in two subgroups: *passive* attempts to find out error symptoms in the process of "usual" execution of software and *active* attempts of program system to periodically survey its own condition in search for an error flag.

Passive detection

Measures related to error detection can be accepted at several structural levels of a program system. Here we shall consider a level of subsystems, or components, i.e. we shall be interested in measures on error symptoms' detection undertaken at transition from one symptom to another, and also symptoms inside a component. Certainly, all this applies also to individual modules inside a component.

Developing these measures, we shall rely on the following.

1. *Mutual suspicion*. Each of the components should assume that all others contain errors. When it obtains any data from another component or from a source outside of the system, it should assume that the data can be wrong, and try to find errors in them.

2. *Immediate detection*. It is necessary to detect errors as soon as possible. It limits damage inflicted by them as well as considerably simplifies the problem of debugging.

3. *Redundancy*. All means of error detection are based on some form of redundancy (explicit or implicit).

When measures on error detection are developed, it is necessary to accept the coordinated strategy for the whole system. The actions undertaken after error detection in software should be uniform for all system components. It brings an attention to the question as to what actions should be taken, when an error is not detected. The best decision is immediately to end the program execution or (in case of an operating system) to put a central processor in wait state. From the point of view of granting the most favorable conditions in error diagnostics for a person debugging the program, for example, a system programmer, the immediate end offers the best strategy. Certainly, in many systems a similar strategy appears unreasonable (for example, it can appear that it is impossible to suspend system operation). In this case a method of *error registration* is used. The description of error symptoms and “snapshot” of system state is saved in an external file, and then the system can continue operation. This file will be investigated by maintenance staff later.

Always, when it is possible, it is better to suspend program execution than to register errors (or to provide system operation in any of these modes as an additional opportunity). The difference between these methods will be illustrated by ways of revealing causes for a grinding sound sometimes arising in your car. If the car mechanic is on a back seat, he can survey a car’s state at that moment when a grinding sound arises. If you choose a method of error registration, the problem of diagnostics becomes more complex.

Active detection of errors

Not all errors can be revealed by passive detection methods as these methods detect an error only when its symptoms are exposed to appropriate checkup. It is possible to make even additional checkup if to design special software for active search for error attributes in a system. Such means refer to as *tools for active detection of errors*.

Tools for active detection of errors are usually combined in *the diagnostic monitor*: parallel process, which periodically analyzes a system’s state with the purpose to detect an error. The large-scale program systems managing resources frequently contain errors that lead to resource loss for long time. For example, running of an operating system’s memory hands over blocks of memory “in rent” to programs of users and other parts of the operating system. An error in these very “other parts” of the system can sometimes lead to erroneous operation of the memory control block as the memory engaged in return of memory handed over earlier in rent, which causes slow degeneration of the system.

The diagnostic monitor can be realized as a periodically executed task (for example, it is planned for each hour) or as a task with a low priority, which is planned for execution when the system switches over to wait state. As before, concrete checks carried out by the monitor depend on system specificity, but some ideas will be understandable from examples. The monitor can examine the basic memory to detect memory blocks, not dedicated to any of tasks carried out and not included in a system’s list of free memory. It can check also unusual situations: for example, a process was not planned for performance during some reasonable interval of time. The monitor can carry out search for “mislaidd” messages inside the system or operations of input-output which remain uncompleted for unusually long time. The monitor can also search for sites of memory on a disk which are not marked as allocated and are not included in the list of free memory, and also a various sort of strangeness in data files.

Sometimes it is desirable that under emergency the monitor should execute trouble-shooting testing of a system. It can activate certain system functions, comparing their results with beforehand determined ones and checking them as far as the execution time is reasonable. The monitor can also periodically submit “empty” or “easy” tasks to the system to make sure that the system functions at least in some primitive mode.

4. Error correction

The following step consists in methods of error correction; when the error is detected, either it or its consequences should be corrected by the software. Error correction by the system is a fruitful method of dependable hardware. Some devices are capable to detect faulty components and switch over to use identical backup components. Similar methods are inapplicable to software due to deep internal distinctions between equipment failures and errors in programs. If some program module contains an error, identical “backup” modules will also contain the same error.

Another approach to error correction is connected to attempts to recover the destructions caused by errors, for example, distortions of records in databases or control tables of a system. The advantages of methods used for struggle against distortions are limited, as it is supposed that the developer beforehand will foresee some possible types of distortions and will provide software functions for their elimination. It is similar to paradox as, if to foreknow, what errors will arise, it would be possible to take additional measures for their prevention. If methods of failure consequence elimination cannot be generalized to work with many types of distortions, it will be the best way to direct efforts and means for error prevention. Instead of equipping an operating system under development with its tools of detection and restoration of a chain of distorted tables or control blocks, when developing an operating system, it is better to design a system in such a way that only one module will have access to this chain, and then persistently try to receive evidence of this module correctness.

5. Error tolerance

The basic assumption of *software error-tolerant* programming consists in the fact that it does not matter how good the program has been designed and realized, it will still contain some residual errors. And if that's the case, then modules of the program which can fail, should have “a buffer stock”. With this purpose the module is designed in the form of *recovery blocks*. Each recovery block contains a pass-through test and one or several alternatives of realization. The basic alternative is initiated by activation of the recovery block and when its execution comes to the end, the checkup of a pass-through test value is carried out. If it makes “true”, it is considered that the execution of a recovery block is successfully completed. If the test makes “false”, then another alternative is initiated and after that the definition of a pass-through test value is carried out again, etc. and so on till the successful execution of a recovery block. If any alternative has not passed the pass-through test, the recovery block is considered as erroneous and the execution of another alternative of the activated module begins. Other technique is applied as well: various segments of the program are written, frequently independently, each of which is intended for execution of one function. The program is made up of these segments. The first segment named primary is executed first. It is followed by a pass-through test of the calculation result of the first segment. If the test has passed successfully, then the result is accepted and transferred to the subsequent parts of the system. If the test has been unsuccessful, any side effects of the first segment are reset, and the second segment named as the first alternative is executed. It is also followed by a pass-through test whose results are considered as in the first case. If it is necessary, other alternative techniques can be realized.

The introduced method of parrying software residual errors by designing the module in the form of a recovery block sometimes requires the unjustified efforts connected to designing of several recovery blocks, each of which contains the pass-through test and one or several alternatives of realization. For the purpose of practical support of program system functioning at presence of errors, the group of methods which is divided into four subgroups has been developed: *dynamic redundancy*, *back-off methods*, *methods*

of error isolation and construction of algorithms immune (or not critical) to various sorts of information process violations (use of algorithmic redundancy).

1. The **dynamic redundancy** concept roots in designing of hardware. One of the approaches to dynamic redundancy is the *majority backup* (a method of voting). The data are processed independently by several identical devices, and obtained results are compared. If the majority of devices have produced an identical result, then this result is considered as correct. And again, as a result of special nature of errors in software, the error presented in a copy of the program module will be present also in all its other copies; therefore, in this case the idea of voting probably is unacceptable. The approach sometimes offered for the solution of this problem consists in having some not identical copies of the module. It means that all copies execute the same function, but either they realize various algorithms or are developed by different authors. This approach is unpromising for the following reasons. It is frequently difficult to receive essentially different versions of the module which executes identical functions. Besides, there is a necessity in additional software for the execution of these module versions in parallel or serially and comparisons of obtained results. This additional software improves the level of system complexity that certainly contradicts to the basic idea of error prevention – first of all to aspire to minimize software complexity.

The second approach to dynamic redundancy consists in execution of these backup copies only when the results received with the help of the basic copy are recognized wrong. If it occurs, the system automatically activates a backup copy. If its results are also wrong, another backup copy is activated etc.

2. The second subgroup of error tolerance assurance methods refers to as **back-off methods** or methods of reduced service. These methods are acceptable usually only when the most important thing for software system is to end an operation correctly. For example, if an error turns out in the system controlling technological processes and as a result this system fails, then a special fragment of the program designed to secure the system and to provide accident-free end of all processes controlled by the system can be loaded and executed. Similar tools are frequently necessary in operating systems. If an operating system detects that it is just about to fail, it can load the emergency fragment responsible for notification of users at terminals about a forthcoming failure and for saving of all system critical data.

3. The third subgroup consists of error isolation methods. Their basic idea is to prevent error consequences from going outside the boundaries of the smallest possible system software part, so that if an error arises then not the whole system will fail; some system functions or some of its users are shut down. For example, in many operational systems errors of some individual users are isolated, so failure influences only some subset of users, and the system as a whole continues to function. In telephone switching systems for recovery after an error in order not to risk the whole system failure, telephone connection is simply cut. Other methods of error isolation are related to protection of each of system programs from errors of other programs. An error in the applied program which is executed under operating system control, should affect only this program. It should not affect an operating system or other programs functioning in this system.

Isolation of programs in an information system is the key factor ensuring that errors in a single user program will not lead to errors in programs of other users or to a complete system failure. Key rules of error isolation in programs consist in the following:

1. The applied program should not have any opportunity to refer directly to another applied program or data in other programs and to change them.

2. The applied program should not have any opportunity to refer directly to programs or a operating system and to change them. Communication between two programs (or the program and the operating system) can be allowed only under the condition of usage of precisely defined interfaces and only in case when both programs agree to this communication.

3. Applied programs and their data should be protected from the operating system to a point that errors in the operating system could not lead to casual change of applied programs or their data.

4. The operating system should protect all applied programs and data from their casual change by system operators or maintenance staff.

5. Applied programs should not have any opportunity either to stop a system, or to compel it to change another applied program or its data.

6. When the applied program addresses the operating system, the acceptability of all parameters should be checked, the applied program should not have any opportunity to change these parameters between the moments of check and their real use by the operating system.

7. None of system data directly accessible to applied programs should influence the functioning of an operating system. An error in the applied program owing to which the contents of this memory can accidentally be changed, leads eventually to system failure.

8. Applied programs should not have any opportunity to bypass an operating system to directly use hardware resources controlled by it. Applied programs should not call directly the components of an operating system intended for use only by its subsystems.

9. Components of an operating system should be isolated from each other so that an error in one of them should not lead to changes of other components or their data.

10. If an operating system detects an error in itself, it should try to limit influence of this error by one applied program and as a last resort to stop execution of only this program.

11. An operating system should give applied programs an opportunity to correct errors detected in them on demand, instead of unconditionally stopping the execution of applied programs.

Realization of many of these principles influences the architecture of system underlying hardware. Though we use the term “operating system” when defining many of them, they are applicable to any program (whether it is an operating system, teleprocessing monitor or file management subsystem) which is engaged with service of other programs.

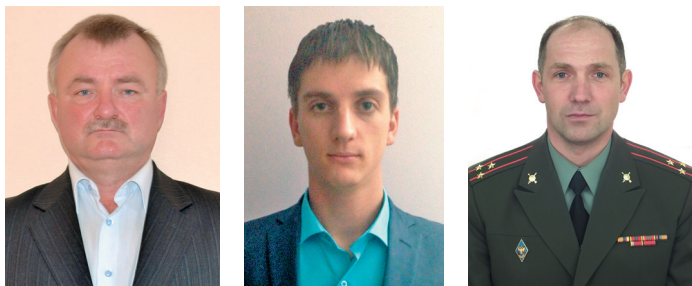
4. The fourth subgroup is *introduction of algorithmic redundancy*.

6. The conclusion

The paper considers effective methods and ways for construction of the architecture of functionally dependable software. The European experience in development of programs for safety related systems [2] is used, and recommendations of standard [3] are also applied. Ensuring software dependability is not limited by development stages of their specification and qualitative architecture. To solve the key task of reliable information system construction, it is necessary to design the dependable software, to implement, to integrate it with hardware, to provide dependability of software during certification, operation and maintenance. These stages of construction of dependable program are the subject of further discussion.

References

1. **Shubinsky I.B.** Functional dependability of information systems (Methods of analysis). M.: Dependability Journal Ltd., 2012, 296p.
2. BS EN 50128:2011. The software for control and protection systems on railways.
3. GOST R/IEC 61508-3-2012. Functional safety of electrical/electronic/programmable electronic safety-related systems. Requirements for software.



Терсков В.А., Шеенок Д.А., Карцан И.Н.

ГЕНЕТИЧЕСКИЙ АЛГОРИТМ ДЛЯ ОПТИМИЗАЦИИ АРХИТЕКТУРЫ БОРТОВОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Описывается модель архитектуры бортового программного обеспечения, позволяющая оценить надежность проектируемой программной системы и трудозатраты на ее реализацию. Описываются параметры и операторы генетического алгоритма, позволяющего найти оптимальные характеристики архитектуры бортового программного обеспечения.

Ключевые слова: генетический алгоритм, бортовое программное обеспечение, программная избыточность, надежность программного обеспечения.

Бортовое программное обеспечение (БПО) автоматизированных систем управления спутниковыми системами связи выполняется на различных типах ЭВМ, характеристики которых определяются назначением систем [1]. Эти факторы влияют на рациональный уровень автоматизации проектирования, на трудоемкость и длительность создания программного обеспечения и т.д. Однако принципы и методы проектирования ПО при этом меняются относительно мало.

БПО, использующееся в АСУ спутниковыми системами связи, обладает всеми свойствами сложных систем [2]. Оно содержит большое количество модулей, тесно взаимодействующих в процессе решения общей целевой задачи.

БПО имеет единую цель функционирования – обработку информации и принятие решений для управления объектами, вплоть до формирования соответствующих управляющих воздействий [3].

Для обеспечения взаимодействия модулей в едином комплексе широко используются иерархические структуры с несколькими уровнями группирования и подчиненности модулей. Каждый модуль имеет свою целевую задачу и специфический частный критерий качества, как правило, не совпадающий с критерием эффективности всего комплекса программ.

При выборе того или иного варианта построения архитектуры БПО руководствуются критериями надёжности и затрат на реализацию системы с заданной надёжностью. Очевидно, что положения этих критериев противоречат друг другу, так как система с большей надёжностью требует затрат больших ресурсов.

Показателем надёжности системы в исходной модели архитектуры программной системы является значение коэффициента готовности системы, прогнозируемого на стадии проектирования. Надёжность всей системы может быть достигнута введением программной избыточности в от-

дельные компоненты её архитектуры. Основным ресурсом при разработке БПО являются трудозатраты специалистов реализующих систему. Для расчета этих показателей в модели необходим учет дополнительных параметров.

В компонент программной архитектуры, функционирование которого особо критично по надёжности, может быть введена программная избыточность методом N -версионного программирования или блока восстановления. Очевидно, что надёжность компонентов с программной избыточностью прямо пропорциональна глубине избыточности (или количеству различных его версий) [4] и надёжностью среды исполнения версий (алгоритма голосования или приемочного теста).

Надёжность мультиверсионного компонента i на архитектурном уровне j , построенного из K версий методом мультиверсионного программирования для любого K равна [5]:

$$R_{ij} = p_{ij}^v \left(1 - \prod_{k=1}^K (1 - p_{ij}^k) \right),$$

где p_{ij}^v – вероятность безотказной работы алгоритма голосования, p_{ij}^k – вероятность безотказной работы версии $k \in Z_{ij}$.

Надёжность мультиверсионного компонента i на архитектурном уровне j , построенного из K версий методом блока восстановления для любого K равна [5]:

$$R_{ij} = \sum_{k=1}^K \left(p_{ij}^k p_{ij}^{AT} \right) \prod_{l=1}^{k-1} \left((1 - p_{ij}^l) p_{ij}^{AT} + p_{ij}^l (1 - p_{ij}^{AT}) \right),$$

где p_{ij}^{AT} – вероятность безотказной работы приемочного теста для компонента i , $i=1, \dots, N$ на уровне j , $j=1, \dots, M$; p_{ij}^k – вероятность безотказной работы версии $k \in Z_{ij}$.

Вероятность сбоя компонента i на уровне j равна:

$$PF_{ij} = 1 - R_{ij}.$$

Трудоёмкость разработки системы равна сумме трудоёмкостей всех компонентов архитектуры системы. При расчете трудоёмкости разработки компонентов с программной избыточностью должны учитываться затраты на реализацию среды исполнения версий модуля (NVX_{ij}) и затраты на реализацию каждой версии i -го компонента на уровне j (T_{ij}^k) [6]. Трудоёмкость разработки всей системы T_s рассчитывается следующим образом:

$$T_s = \sum_{j=1}^M \sum_{i=1}^{N_j} \left(B_{ij} T_{ij} + (NVP_{ij} + RB_{ij}) \left(NVX_{ij} + \sum_{k \in Z_{ij}} T_{ij}^k \right) \right),$$

где NVX_{ij} – трудоёмкость разработки среды исполнения версий (приемочного теста для RB или алгоритма голосования для NVP) (N -version execute environment); B_{ij} – бинарная переменная, принимающая значение 1 (тогда $NVP_{ij}=0$, $RB_{ij}=0$), если в программном компоненте не используется программная избыточность, иначе равна 0;

NVP_{ij} – бинарная переменная, принимающая значение 1 (тогда $B_{ij}=0$, $RB_{ij}=0$), если в программном компоненте введена программная избыточность методом NVP , иначе равна 0;

RB_{ij} – бинарная переменная, принимающая значение 1 (тогда $B_{ij}=0$, $NVP_{ij}=0$), если в программном компоненте введена программная избыточность методом RB , иначе равна 0.

В случае если производится моделирование уже существующей системы, которую планируется модернизировать, то для тех архитектурных компонентов, которые уже существуют в системе, затраты равны $T_{ij}=0$.

Программный компонент, участвующий в критически важных циклах управления, должен выполнить вычисления за такое время, чтобы время всего цикла управления не превышало критическое значение. Если компонент не успевает выдать управляющее воздействие другому компоненту, то происходит сбой.

Среднее время выполнения программного компонента i на уровне j вычисляется как сумма времени работы компонента без сбоев и среднего времени простоя компонента:

$$RT_{ij} = TU_{ij} \cdot Ntu_{ij} \cdot \left(1 - \left(PF_{ij} + \sum_{ab \in E_{ij}} (PL_{ij}^{ab} \cdot PF_{ab} \cdot PU_{ab}) \right) \right) + \\ + (TA_{ij} \cdot Nta_{ij} + TC_{ij} \cdot Ntc_{ij} + TE_{ij} \cdot Nte_{ij}) \cdot \left(PF_{ij} + \sum_{ab \in E_{ij}} (PL_{ij}^{ab} \cdot PF_{ab} \cdot PU_{ab}) \right),$$

где PL_{ij}^{ab} – условная вероятность того, что в компоненте i на уровне j возникнет сбой, если сбой возникнет в компоненте a на уровне b , $a \in \{1, \dots, N_b\}$, $b \in \{1, \dots, M\}$, $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$; PU_{ab} – вероятность того, что компонент a на уровне b будет использоваться;

PF_{ab} – вероятность того, что в компоненте a на уровне b возникнет сбой;

Nta_{ij} – число сбойных компонентов на более низких архитектурных уровнях во время доступа к компоненту i на уровне j ;

Ntc_{ij} – число сбойных компонентов на всех архитектурных уровнях, анализируемых в одно и тоже время с компонентом i на уровне j ;

Nte_{ij} – число сбойных компонентов на всех уровнях архитектуры, в которых происходит устранение сбоев во время устранения сбоя в компоненте i на уровне j ;

Ntu_{ij} – число компонентов на всех уровнях архитектуры, используемых в одно и тоже время с компонентом i на уровне j .

Далее представлены обозначения параметров модели архитектуры БПО [7]:

M – количество архитектурных уровней в программной архитектуре;

N_j – количество компонентов на уровне j , $j \in \{1, \dots, M\}$;

D_{ij} – множество индексов компонентов, зависящих от компонента i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$;

E_{ij} – множество индексов компонентов, от которых зависит компонент i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$;

F_{ij} – событие сбоя, возникшего в компоненте i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$;

PU_{ij} – вероятность, того что компонент i на уровне j будет использоваться;

PF_{ij} – вероятность, того, что в компоненте i на уровне j возникнет сбой;

R_{ij} – вероятность того, что в компоненте i на уровне j сбой не появится;

PL_{nm}^{ij} – условная вероятность того, что в компоненте m на уровне n возникнет сбой, если возникнет сбой в компоненте i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, $n \in \{1, \dots, N_m\}$, $m \in \{1, \dots, M\}$;

TA_{ij} – относительное время доступа к компоненту i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, определяемое отношением среднего времени доступа к компоненту i на уровне j к числу сбойных компонентов на более низких уровнях архитектуры во время доступа к компоненту; параметр TA_{ij} имеет смысл использовать, если компонент работает на удаленных или изолированных системах;

Nta_{ij} – число сбойных компонентов на более низких уровнях архитектуры во время доступа к компоненту i на уровне j ;

TC_{ij} – относительное время анализа сбоя в компоненте i на уровне j , определяемое отношением среднего времени анализа сбоя в компоненте i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, к числу сбойных компонентов на всех уровнях архитектуры, анализируемых в одно и тоже время; к анализу относится время на воспроизведение ошибки и её локализацию;

Ntc_{ij} – число сбойных компонентов на всех уровнях архитектуры, анализируемых в одно и тоже время с компонентом i на уровне j ;

TE_{ij} – относительное время устранения сбоя в компоненте i на уровне j , определяемое отношением среднего времени восстановления в компоненте i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, к числу сбойных компонентов на всех уровнях архитектуры, в которых происходит устранение сбоев в одно и тоже время;

Nte_{ij} – число сбойных компонентов на всех уровнях архитектуры, в которых происходит устранение сбоев во время устранения сбоя в компоненте i на уровне j ;

TU_{ij} – относительное время использования компонента i на уровне j , определяемое отношением среднего времени использования компонента i на уровне j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, к числу компонентов на всех уровнях архитектуры, используемых в одно и тоже время;

Ntu_{ij} – число компонентов на всех уровнях архитектуры, используемых в одно и тоже время с компонентом i на уровне j ;

K_{ij} – глубина программной избыточности компонента i , на уровне j ;

Z_{ij} – множество версий компонента i , на уровне j ;

RT_{ij} – среднее время выполнения модуля i на уровне j ;

T_{ij} – трудоемкость разработки компонента i на уровне j ;

T^k_{ij} – трудоемкость разработки версии k компонента i на уровне j , $k \in Z_{ij}$, в чел-часах;

NVX_{ij} – трудоемкость разработки среды исполнения версий (приемочного теста для *RB* (*recovery block*, блок восстановления) или алгоритма голосования для *NVP* (*N-version programming*, *N*-версионное программирование));

B_{ij} – бинарная переменная, принимающая значение 1 (тогда $NVP_{ij}=0$, $RB_{ij}=0$), если в программном компоненте не используется программная избыточность, иначе равна 0;

NVP_{ij} – бинарная переменная, принимающая значение 1 (тогда $B_{ij}=0$, $RB_{ij}=0$), если в программном компоненте введена программная избыточность методом *NVP*, иначе равна 0;

RB_{ij} – бинарная переменная, принимающая значение 1 (тогда $B_{ij}=0$, $NVP_{ij}=0$), если в программном компоненте введена программная избыточность методом *RB*, иначе равна 0;

TR – среднее время простоя системы, которое определяется как среднее время, в течение которого программное обеспечение не может выполнять свои функции;

$MTTF$ – среднее время возникновения сбоя в системе, которое определяется как среднее время, в течение которого сбоев в программном обеспечении не возникает;

S – коэффициент готовности программной системы;

T_s – общая трудоемкость реализации программной системы.

Среднее время сбоя в программной системе равно [8]:

$$\begin{aligned}
 MTTF = & \sum_{j=1}^M \sum_{i=1}^{N_j} \{PU_{ij} \times (1 - PF_{ij}) \times [TU_{ij} + \\
 & \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left((1 - PL_{nm}^{ij}) \times \left(TU_{nm} + \sum_{l \in D_{nm}} ((1 - PL_{lm}^{nm}) \times TU_{lm}) \right) \right) + \\
 & + \sum_{k \in D_{ij}} \left((1 - PL_{kj}^{ij}) \times \left(TU_{kj} + \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left((1 - PL_{nm}^{kj}) \times \left(TU_{nm} + \sum_{l \in D_{nm}} ((1 - PL_{lm}^{nm}) \times TU_{lm}) \right) \right) \right) \right) \}.
 \end{aligned}$$

Среднее время простоя программной системы равно [8]:

$$\begin{aligned}
 TR = & \sum_{j=1}^M \sum_{i=1}^{M_j} \{PU_{ij} \times PF_{ij} \times [(TA_{ij} + TC_{ij} + TE_{ij}) + \\
 & + \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left(PL_{nm}^{ij} \times \left((TA_{nm} + TC_{nm} + TE_{nm}) + \sum_{l \in D_{nm}} (PL_{lm}^{nm} \times (TA_{lm} + TC_{lm} + TE_{lm})) \right) \right) \times \\
 & \times \sum_{k \in D_{ij}} [PL_{kj}^{ij} \times [(TA_{kj} + TC_{kj} + TE_{kj}) + \\
 & + \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left(PL_{nm}^{kj} \times \left((TA_{nm} + TC_{nm} + TE_{nm}) + \sum_{l \in D_{nm}} (PL_{lm}^{nm} \times (TA_{lm} + TC_{lm} + TE_{lm})) \right) \right) \right] \} \}.
 \end{aligned}$$

Коэффициент готовности программной системы равен:

$$S = \frac{MTTF}{MTTF + TR}.$$

Трудозатраты на разработку системы равны:

$$T_s = \sum_{j=1}^M \sum_{i=1}^{N_j} \left(B_{ij} T_{ij} + (NVP_{ij} + RB_{ij}) \cdot \left(NVX_{ij} + \sum_{k \in Z_{ij}} T_{ij}^k \right) \right).$$

Для компонентов, в которых возможно введение программной избыточности, могут быть изменены следующие характеристики [9].

Метод реализации программной избыточности: мультиверсионное программирование ($NVP_{ij}=1$, $RB_{ij}=0$) или блок восстановления ($NVP_{ij}=0$, $RB_{ij}=1$). Если выбран метод NVP , то устанавливается значение гена равно 0, если RB , то равно 1.

Номер варианта (альтернативы) Var_{v1} – «вероятность сбоя/трудозатраты». Возможные варианты задаются аналитиком для каждого компонента ($1 \leq Var_{v1} \leq V_{ij}$). V_{ij} – количество альтернативных вариантов разработки для каждого компонента.

Номер варианта $Var_{v2} \dots Var_{v10}$ – вероятности сбоя для каждой версии компонента, аналогично пункту 2 ($0 \leq Var_{v2..10} \leq V_{ij}$, 0 – версии нет). Предельное количество версий программного компонента, если будет применена избыточность, заранее задается аналитиком и не может быть больше 10 версий, т.к. большее количество вносит в компонент дополнительную сложность и стоимость, неоправданную увеличением надёжности.

Если гены $Var_{v2} \dots Var_{v10}$ принимают значение 0, то считается, что программная избыточность не вводится в данном компоненте ($B_{ij}=1$).

Для компонентов, в которых не предусматривается введение программной избыточности, изменяется только вариант Var вероятности сбоя компонента и соответствующей трудоемкости для достижения этой вероятности сбоя ($1 \leq Var \leq \text{Кол-во вариантов для данного компонента}$).

Таким образом, фенотип особи (решения) формируется из переменных характеристик программных компонентов [10]. В таблице 1 представлен общий вид фенотипа с примером аллелей.

Таблица 1. Фенотип особи

Группа компонентов, с возможностью программной избыточности								Группа компонентов, без возможности программной избыточности			
Компонент 1				..	Компонент N				Компонент 1	..	Компонент M
NVP/RB	Var _{v1}		Var _{v4}		NVP/RB	Var _{v1}		Var _{v5}	Var		Var
1	3	..	0		0	1	..	0	2		3

Скрещивание выбранных особей происходит с заранее заданной вероятностью. Если родители не скрещиваются, то происходит их клонирование.

Скрещивание происходит посредством разрыва хромосомы родителей в заданном количестве точек, при этом потомки получают различные признаки обоих родителей.

В природе существует огромное количество признаков и свойств живых организмов, которые определяются двумя и более парами генов, и наоборот, один ген часто контролирует многие признаки. Кроме того, действие гена может быть изменено соседством других генов и условиями внешней среды. Еще в одной из работ 1928 г. Ю.А. Филипченко, было доказано, что наряду с «основным» геном, определяющим признак, существует ряд генов-модификаторов этого признака. Подобный тип наследования встречается часто. Таким образом, фенотип, как правило, представляет собой результат сложного взаимодействия генов [11].

Таким образом, введем понятие «связанные гены». Связанные гены – это гены, взаимная комбинация которых осуществляет влияние на определенный признак особи.

Надёжность и трудозатраты для компонентов с возможной программной избыточностью определяются взаимодействующими генами версий и метода избыточности. Разрывы хромосомы могут происходить как между генами одного программного компонента, так и между генами разных компонентов. Причем вероятность выбора точки разрыва хромосомы между генами одного программного компонента (связанными генами) заранее задана. При равномерном скрещивании разрыв может происходить либо во всех точках или только между несвязанными генами.

Мутация особей популяции происходит с заданной вероятностью. Кроме вероятности применения мутации к каждой особи, используется вероятность применения мутации к каждому её гену, величину которой обычно задают от 1 до 10%. При мутации бинарных генов метода избыточности происходит инвертирование значения.

Аллели генов альтернатив «вероятность сбоя/трудоемкость» характеризуются шкалой порядка, таким образом, что каждый следующий вариант, лучше по надёжности, но хуже по трудозатратам. Таким образом, заранее заданные альтернативные варианты для конкретного программного компонента оптимальны по Парето. Мутация таких генов может происходить двумя способами:

1. Выбор любой альтернативы «вероятность сбоя/трудоемкость» равновероятен.
2. Выбор любого варианта «вероятность сбоя/трудоемкость» происходит вероятностью распределенной по закону нормального распределения вероятностей для дискретной случайной величины [12]. При этом выбор текущего значения варианта невозможен. При мутации генов версий программных компонентов, для которых возможно значение 0 (отсутствие версии), такое значение добавляется как дополнительное возможное значение. В таблице 3 приведены вероятности выбора вариантов при мутации гена версии программного компонента, текущее значение которого равно 4, а общее количество заданных вариантов равно 7.

Таблица 3. Распределение вероятностей выбора варианта

Отсутствие версии	Вар. 1	Вар. 2	Вар. 3	Вар. 4 (текущий)	Вар. 5	Вар. 6	Вар. 7
0.015625	0.09375	0.234375	0.3125	0	0.234375	0.09375	0.015625

Генетический алгоритм основан на идеях метода с независимой селекцией Шаффера при многокритериальной оптимизации *VEGA* (*Vector Evaluated Genetic Algorithm*) [13].

Селекция происходит с вероятностью, пропорциональной значению критерия. Вероятность индивида быть отобранным по критерию S рассчитывается по формуле [14]:

$$p_i = \frac{f_i}{\sum_{j=1}^N f_j} = \frac{f_i}{\bar{f} \cdot N},$$

где f_i – пригодность индивида i ; $\bar{f} = \frac{1}{N} \sum_{j=1}^N f_j$ – средняя пригодность популяции; N – размер популяции; $\sum_{j=1}^N p_j = 1$.

Вероятность индивида быть отобранным по минимизируемому критерию T_s рассчитывается по формуле [15]:

$$p_i = \frac{-f_i + C}{N \cdot C - \sum_{j=1}^N f_j},$$

где f_i – пригодность индивида i ; C – константа, определяющая минимальную пригодность популяции; $C : p_i \geq 0, \forall i$; N – размер популяции; $\sum_{j=1}^N p_j = 1$.

В рассматриваемом алгоритме константа C равна максимальной пригодности особи в популяции. Таким образом, минимальная вероятность быть отобранным индивидом по критерию T_s равна 0.

При определении пригодности особи значения S и T_s рассчитываются по алгоритму, изображенном на рис. 1.

Каждая особь с рассчитанными критериями записывается в массив. Перед тем как рассчитывать критерии для следующей особи происходит поиск аналогичной уже рассчитанной ранее особи [10]. Это действие целесообразно и позволяет экономить время работы алгоритма, т.к. расчет критериев значительно дольше поиска идентичной особи в массиве решений.

Для решения многокритериальной задачи условной оптимизации необходимо использовать подход, основанный на сведении условной задачи к безусловной. Поиск Парето-оптимальных решений осуществляется по схеме метода *VEGA*. Решения задачи с ограничениями должны не только принадлежать множеству Парето, но и находиться в допустимой области. Поэтому к предложенному алгоритму дополнительно вводится процедура, позволяющая стягивать решения в допустимую область [14].

Чтобы стало возможным решение задачи условной оптимизации, каждое ограничение рассматривается как отдельная целевая функция, и поэтому изначально условная задача с несколькими целевыми функциями сводится к безусловной многокритериальной задаче оптимизации. Преобразование исходной задачи условной многокритериальной оптимизации имеет следующий вид [14]:

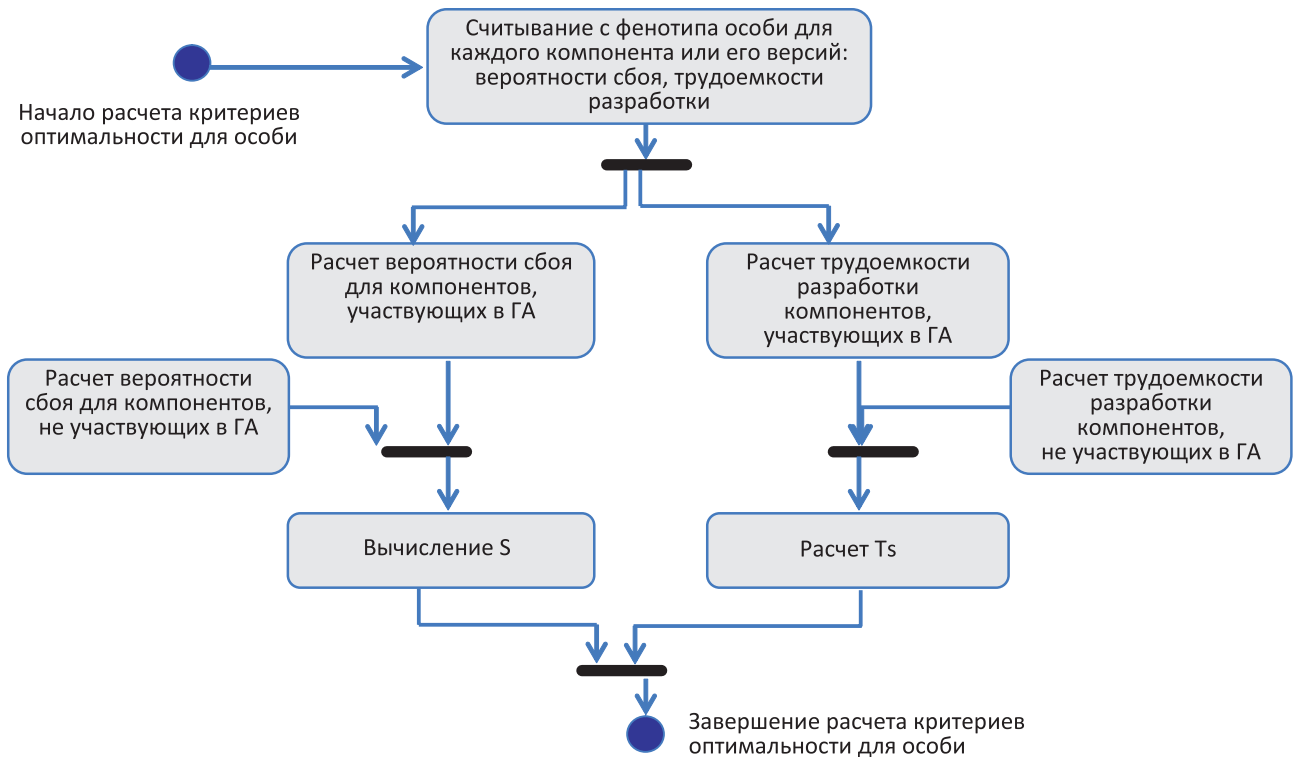


Рис. 1. Алгоритм расчета критериев оптимальности

Целевые функции исходной задачи – $F(X) \rightarrow opt$, ограничения исходной задачи – $G(X) \leq B$.

Целевые функции преобразованной задачи – $F(X) \rightarrow opt$, ограничения преобразованной задачи – $|G(X) - B| \rightarrow opt$.

В первую очередь несколько итераций алгоритма решается исходная условная задача, но без учета ограничений. Затем, чтобы получить большее число решений, принадлежащих допустимой области, поиск продолжается уже без учета целевых функций исходной задачи, а только по ограничениям. Таким образом, поиск решений производится только по функциям-ограничениям, что приводит большую часть популяции в допустимую область, но с потерей качества решений по критериям оптимизации [14].

Генетический алгоритм многокритериальной условной оптимизации программной архитектуры [16] также основан на идеях метода *VEGA* (*Vector Evaluated Genetic Algorithm*) с независимой селекцией Шаффера при многокритериальной оптимизации.

Отличие алгоритма от ГА безусловной оптимизации состоит в том, что в нем каждое ограничение рассматривается как дополнительный критерий оптимизации. Часть поколений алгоритм работает без учета дополнительных критериев оптимизации, а затем оставшуюся часть поколений алгоритм работает по двум критериям нарушения ограничения на S , T_s , и критериям нарушения ограничения RT_{ij} .

Входные параметры ГА следующие:

- размер популяции (N);
- вероятность скрещивания ($prob_cross$);
- вид скрещивания (1,2,3-точечное, равномерное);
- вероятность разрыва связанных генов ($prob_cross_inter$);
- вероятность мутации особи ($prob_mutate$);
- вероятность мутации гена ($prob_mutate_gen$);
- критерии останова (максимальное время работы $time_ga$, количество популяций без улучшения решения (стагнация) $stagnancy$, количество популяций pop_count);

- процент популяций на обработку ограничений *percent_bound*;
- количество ограничений на время выполнения компонентов *B*.

Алгоритм реализуется следующей последовательностью действий:

1. Генерация родительской популяции *P* размером *N* случайных особей.
2. Расчет критериев для всех особей популяции *P*.
3. Пропорциональная селекция *N/2* особей из *P* по критерию *S* в промежуточную популяцию *P'*.
4. Пропорциональная селекция *N/2* особей по критерию *T_s* в промежуточную популяцию *P'*.
5. Скрещивание с вероятностью *prob_cross* *N/2* случайно выбранных пар особей из промежуточной популяции *P'*. Формирование основной популяции *P* из *N* выбранных особей.
6. Выполнение оператора мутации с вероятностью *prob_mutate* на каждой особи основной популяции *P* и каждому гену особи с вероятностью *prob_mutate_gen*.
7. Расчет значений критериев оптимизации для всех особей популяции *P*.
8. Выбор из популяции *P* недоминируемых решений. Если в найденных ранее решениях есть решения, которые их доминируют, то *stagnancy* = *stagnancy*+1.
9. Если сработал хотя бы один критерий останова, то остановка алгоритма.
10. Если номер популяции меньше, либо равен *percent_bound*pop_count*, то переход на шаг 3.
11. Пропорциональная селекция *N/(2+Q)* особей из *P* по критерию нарушения ограничения на *S* в промежуточную популяцию *P'*.
12. Пропорциональная селекция *N/(2+Q)* особей по критерию нарушения ограничения на *T_s* в промежуточную популяцию *P'*.
13. Пропорциональная селекция *N/(2+Q)* особей по каждому критерию нарушения ограничения на время выполнения компонента *RT_{ij}* в промежуточную популяцию *P'*.
14. Скрещивание с вероятностью *prob_cross* *N/(2+Q)* случайно выбранных пар особей из промежуточной популяции *P'*. Формирование основной популяции *P* из *N* выбранных особей.
15. Выполнение оператора мутации с вероятностью *prob_mutate* на каждой особи основной популяции *P* и каждому гену особи с вероятностью *prob_mutate_gen*.
16. Расчет критериев по ограничениям для всех особей популяции *P*.
17. Выбор из популяции *P* лучших решений по критериям ограничений. Если в найденных ранее решениях есть лучше, то *stagnancy* = *stagnancy*+1.
18. Если сработал хотя бы один критерий останова, то остановка алгоритма, иначе переход на шаг 11.

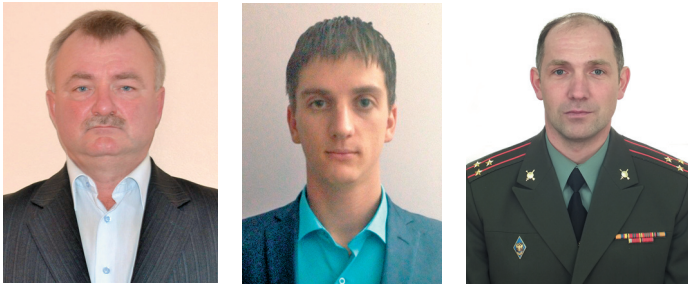
Недоминируемые решения, полученные на каждой итерации, отбираются в множество Парето. Решения множества Парето не могут быть предпочтены друг другу, поэтому после его формирования задача может считаться математически решенной [17].

Разработанный генетический алгоритм был протестирован на специально подготовленных задачах, а также был использован при разработке программного обеспечения корпоративных систем управления, и БПО. С помощью разработанного ГА все задачи были решены, а также найдены эффективные архитектурные решения.

Литература

1. Kovalev I. Optimal Time Cyclograms of Spacecrafts Control Systems / I. Kovalev, O. Davydenko // Advances in Modeling and Analysis. Vol.48. № 2–3. 1996. AMSE PRESS. P. 19–23.
2. Царев Р.Ю. Программно-аппаратное обеспечение отказо- и катастрофоустойчивых систем управления и обработки информации: монография / А.В. Аниконов, М.Ю. Слободин, Р.Ю. Царев. – М.: Макс-пресс, 2006. – 244 с.

3. **Царев Р.Ю.** Оптимизационно-имитационный подход к синтезу автоматизированных систем управления / **И.В. Ковалев, М.В. Тюпкин, Р.Ю. Царев, Ю.Д.Цветков** // Программные продукты и системы. – 2007. – № 3. – С. 73–74.
4. **Царев Р.Ю.** Система многоатрибутивного формирования мультиверсионных программных средств отказоустойчивых систем управления: Дис. Канд. Техн. Наук: Красноярск, 2003. – 143 с.
5. **Новый А.В.** Система анализа архитектурной надежности программного обеспечения.: Дис. Канд. Техн. Наук: Красноярск, 2011 – 131 с.
6. **Шеенок Д.А., Кукарцев В.В.** Оценка затрат на модернизацию программного обеспечения критических по надежности систем // Вестник СибГАУ. Вып. 5(45). – 2012. – С. 62-65.
7. **Шеенок Д.А.** Модификация модели программной архитектуры для многокритериальной условной оптимизации // Перспективы развития информационных технологий: Материалы XI международной научно-практической конференции. – 2013. – С.76-81.
8. **Русаков М.А.** Многоэтапный анализ архитектурной надежности в сложных информационно-управляющих системах: Дис. Канд. Техн. Наук: Красноярск, 2005 – 168 с.
9. **Шеенок Д.А., Кукарцев В.В.** Оптимизация программной архитектуры логистических информационных систем // Логистические системы в глобальной экономике: материалы Междунар. науч.-практ. конф. (14-15 марта 2013 г., Красноярск). Ч. 1. – 2013. – С.138-145.
10. **Шеенок Д.А.** Генетический алгоритм поиска оптимальной архитектуры программного обеспечения // Актуальные вопросы современной науки: Материалы IV международной научной конференции 14-15 декабря 2012 г. – 2012. – С.62-68.
11. **Инге-Вечтомов С.Г.** Генетика с основами селекции: Учеб. Для биолог. Спец. Ун-тов. – М.: Высш. Шк., 1989. – 591 с.
12. **Спицын В.Г., Цой Ю.Р.** Представление знаний в информационных системах: учебное пособие. – Томск: Изд-во ТПУ, 2006. – 146 с.
13. **Сергиенко Р.Б.** Козволюционный алгоритм для задач условной и многокритериальной оптимизации / **Р.Б. Сергиенко, Е.С. Семенкин** // Программные продукты и системы. – №4. – 2010. – С. 24-28.
14. **Гуменникова А.В.** Адаптивные поисковые алгоритмы для решения сложных задач многокритериальной оптимизации: Дис. Канд. Техн. Наук: Красноярск, 2006 – 129 .
15. **Сопов Е.А.** Эволюционные алгоритмы моделирования и оптимизации сложных систем: Дис. Канд. Техн. Наук: Красноярск, 2004 – 129 с.
16. **Шеенок Д.А.** Инструментальное средство проектирования оптимальной архитектуры отказоустойчивых программных систем // Программная инженерия. №6. – 2013. – С. 20-26.
17. **Сергиенко Р.Б.** Автоматизированное формирование нечетких классификаторов самонастраивающимися козволюционными алгоритмами: Дис. Канд. Техн. Наук: Красноярск, 2010 – 192 с.



Terskov V.A., Sheenok D.A., Kartsan I.N.

GENETIC ALGORITHM FOR OPTIMIZATION OF ONBOARD SOFTWARE ARCHITECTURE

The paper describes the model of onboard software architecture that allows us to assess the dependability of a designed program system and labour efforts spent on its realization. The paper defines parameters and operators of the genetic algorithm that makes it possible to find optimal characteristics of onboard software architecture.

Keywords: *genetic algorithm, onboard software, program redundancy, software dependability.*

Onboard software (OSW) in automated control systems to control satellite communication systems is implemented on various types of computers whose characteristics are defined by the purpose of systems [1]. These factors influence a rational level of designing automation, labor input and duration of software development, etc. However, principles and methods of SW designing vary relatively little.

OSW used in automatic control systems to control satellite communication systems possesses all properties of complex systems [2]. It contains a large quantity of modules closely interacting during common target task solution.

OSW has the common objective of functioning – information processing and decision-making to control objects, right up to generation of corresponding control actions [3].

Hierarchical structures with several levels of grouping and subordination of modules are widely used for ensuring interaction of modules in an integrated complex. Each module has the target task and specific individual criterion of quality, as a rule, not corresponding to the efficiency criterion of the whole system of programs.

It is believed that choosing this or that alternative of construction of onboard software architecture (OSW), one should be guided by dependability criteria and costs for realization of a system with specified dependability. It is obvious that statements of these criteria disagree with each other as a system with a greater dependability demands larger resources.

The dependability index of a system in the initial model of program system architecture is the value of system availability predicted at the design stage. The dependability of the whole system can be achieved by introducing program redundancy in separate components of its architecture. The basic resource in OSW development is labor expenditures of experts implementing the system. To calculate these indices in a model, it is necessary to take into account additional parameters.

In a component of program architecture, whose functioning is especially critical for dependability, program redundancy can be introduced by the method of N-version programming or by recovery block. It is obvious that dependability of components with program redundancy is directly proportional to the depth of redundancy (or to the number of its various versions) [4] and dependability of the environment of versions' execution (algorithm of voting or acceptance test).

Dependability of multiversion component i at the architectural level j constructed of K versions by the method of multiversion programming for any K is equal to [5]:

$$R_{ij} = p_{ij}^v \left(1 - \prod_{k=1}^K (1 - p_{ij}^k) \right),$$

where p_{ij}^v is the probability of non-failure operation of a voting algorithm, p_{ij}^k is the probability of non-failure operation of the version $k \in Z_{ij}$.

Dependability of the multiversion component i at the architectural level j constructed of K versions by recovery block method for any K is equal to [5]:

$$R_{ij} = \sum_{k=1}^K \left(p_{ij}^k p_{ij}^{AT} \right) \prod_{l=1}^{k-1} \left((1 - p_{ij}^l) p_{ij}^{AT} + p_{ij}^l (1 - p_{ij}^{AT}) \right),$$

where p_{ij}^{AT} is the probability of non-failure operation of the acceptance test for a component i , $i=1.., N$ at the level j , $j=1.., M$; p_{ij}^k is the probability of non-failure operation of the version $k \in Z_{ij}$.

The probability of failure of the component i at the level j is equal to:

$$PF_{ij} = 1 - R_{ij}.$$

Labor input of system engineering is equal to the sum of labor inputs of all components of system architecture. During calculation of labor input of components' development with program redundancy, the costs for implementation of versions' execution environment of the module (NVX_{ij}) and the costs for implementation of each version of the i -th component at the level j (T_{ij}^k) [6] should be taken into account. Labor input of the whole system development of T_s is calculated as follows:

$$T_s = \sum_{j=1}^M \sum_{i=1}^{N_j} \left(B_{ij} T_{ij} + (NVP_{ij} + RB_{ij}) \left(NVX_{ij} + \sum_{k \in Z_{ij}} T_{ij}^k \right) \right).$$

where NVX_{ij} is the labor input of versions execution environment development (the acceptance test for RB or voting algorithm for NVP) (*N-version execute environment*); B_{ij} is the binary variable accepting the value 1 (then $NVP_{ij}=0$, $RB_{ij}=0$) if the program component does not use program redundancy, otherwise it is equal to 0;

NVP_{ij} is the binary variable accepting the value 1 (then $B_{ij}=0$, $RB_{ij}=0$) if program redundancy is introduced in the program component by NVP method, otherwise it is equal to 0;

RB_{ij} is the binary variable accepting the value 1 (then $B_{ij}=0$, $NVP_{ij}=0$) if program redundancy is introduced in the program component by RB method, otherwise it is equal to 0.

In case if we model an already existing system, which is planned to be updated, then for those architectural components which already exist in system, costs are equal to 0 ($T_{ij}=0$).

The program component participating in critical control cycles should execute calculations in such time that the time of the whole control cycle should not exceed the critical value. If the component is not in time to give out control action to the other component, then a failure occurs.

The average time of the execution of the program component i at the level j is calculated as the sum of the component operating time without failures and the average idle time of the component:

$$RT_{ij} = TU_{ij} \cdot Ntu_{ij} \cdot \left(1 - \left(PF_{ij} + \sum_{ab \in E_{ij}} (PL_{ij}^{ab} \cdot PF_{ab} \cdot PU_{ab}) \right) \right) + \\ + (TA_{ij} \cdot Nta_{ij} + TC_{ij} \cdot Ntc_{ij} + TE_{ij} \cdot Nte_{ij}) \cdot \left(PF_{ij} + \sum_{ab \in E_{ij}} (PL_{ij}^{ab} \cdot PF_{ab} \cdot PU_{ab}) \right),$$

where PL_{ij}^{ab} is the conditional probability of a failure occurring in the component i at the level j if a failure occurs in the component a at the level b , $a \in \{1, \dots, N_b\}$, $b \in \{1, \dots, M\}$, $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$;

PU_{ab} is the probability that the component a at the level b will be used;

PF_{ab} is the probability of a failure occurring in the component a at the level b ;

Nta_{ij} is the number of faulty components at lower architectural levels during access to the component i at the level j ;

Ntc_{ij} is the number of faulty components at all architectural levels analyzed at the same time with the component i at the level j ;

Nte_{ij} is the number of faulty components at all levels of architecture in which there is an elimination of failures during the elimination of a failure in the component i at the level j ;

Ntu_{ij} is the number of components at all levels of architecture used at the same time with the component i at the level j .

Below the designations of parameters of OSW architecture model [7] are presented:

M – the number of architectural levels in program architecture;

N_j – the number of components at the level j , $j \in \{1, \dots, M\}$;

D_{ij} – a set of indexes of components dependent on the component i at the level j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$;

E_{ij} – a set of indexes of components on which the component i at the level j depends, $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$;

F_{ij} – a failure event occurred in the component i at the level j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$;

PU_{ij} – the probability that the component i at the level j will be used;

PF_{ij} – the probability of a failure occurring in the component i at the level j ;

R_{ij} – the probability of a failure not occurring in the component i at the level j ;

PL_{nm}^{ij} – the conditional probability that a failure will occur in the component m at the level n if there is a failure in the component i at the level j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, $n \in \{1, \dots, N_m\}$, $m \in \{1, \dots, M\}$;

TA_{ij} – relative access time to the component i at the level j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, determined by the ratio of the average access time to the component i at the level j to the number of faulty components at lower levels of architecture during access to the component; parameter TA_{ij} can be used, if the component operates on the remote or isolated systems;

Nta_{ij} – the number of faulty components at lower levels of architecture during access to the component i at the level j ;

TC_{ij} – the relative time of failure analysis in the component i at the level j , determined by the ratio of the failure analysis average time in the component i at the level j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, to the number

of faulty components at all levels of architecture analyzed simultaneously (time for error reproduction and its localization relates to the analysis time);

Nta_{ij} – the number of faulty components at all levels of architecture analyzed simultaneously with the component i at the level j ;

TE_{ij} – the relative time of failure removal in the component i at the level j , determined by the ratio of restoration average time in the component i at the level j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, to the number of faulty components at all levels of architecture in which removal of failures occurs at the same time;

Nte_{ij} – the number of faulty components at all architecture levels in which removal of failures occurs during removal of failure in the component i at the level j ;

TU_{ij} – the relative time of use of the component i at the level j , determined by the ratio of average use time of the component i at the level j , $i \in \{1, \dots, N_j\}$, $j \in \{1, \dots, M\}$, to the number of components at all levels of architecture used simultaneously;

Ntu_{ij} – the number of components at all levels of architecture used simultaneously with the component i at the level j ;

K_{ij} – the program redundancy depth of the component i at the level j ;

Z_{ij} – the plurality of versions of the component i at the level j ;

RT_{ij} – the average time of execution of the module i at the level j ;

T_{ij} – the labor input of the development component i at the level j ;

T^k_{ij} – the labor input of the development version k of the component i at the level j , $k \in Z_{ij}$, in man-hours;

NVX_{ij} – the labor input of development of versions' execution environment (the acceptance test for *RB* (recovery block) or voting algorithm for *NVP* (*N-version programming*));

B_{ij} – the binary variable accepting value 1 (in this case $NVP_{ij}=0$, $RB_{ij}=0$) if the program component does not use program redundancy, otherwise it is equal to 0;

NVP_{ij} – the binary variable accepting value 1 (in this case $B_{ij}=0$, $RB_{ij}=0$) if program redundancy is introduced in the program component by *NVP* method, otherwise it is equal to 0;

RB_{ij} – the binary variable accepting value 1 (in this case $B_{ij}=0$, $NVP_{ij}=0$) if program redundancy is introduced in the program component by *RB* method, otherwise it is equal to 0;

TR – the average idle time of a system which is defined as the average time during which the software cannot carry out its functions;

$MTTF$ – the mean time to failure in system which is defined as the average time during which failures in the software do not arise;

S – the availability factor of a program system;

T_s – the general labor input of program system realization.

Mean time to failure in a program system is determined as follows [8]:

$$\begin{aligned}
 MTTF = & \sum_{j=1}^M \sum_{i=1}^{N_j} \{PU_{ij} \times (1 - PF_{ij}) \times [TU_{ij} + \\
 & \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left((1 - PL_{nm}^{ij}) \times \left(TU_{nm} + \sum_{l \in D_{nm}} ((1 - PL_{lm}^{nm}) \times TU_{lm}) \right) \right) \} + \\
 & + \sum_{k \in D_{ij}} \left((1 - PL_{kj}^{ij}) \times \left(TU_{kj} + \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left((1 - PL_{nm}^{kj}) \times \left(TU_{nm} + \sum_{l \in D_{nm}} ((1 - PL_{lm}^{nm}) \times TU_{lm}) \right) \right) \right) \right) \}
 \end{aligned}$$

Average idle time of a program system is equal to [8]:

$$\begin{aligned}
 TR = & \sum_{j=1}^M \sum_{i=1}^{M_j} \{PU_{ij} \times PF_{ij} \times [(TA_{ij} + TC_{ij} + TE_{ij}) + \\
 & + \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left(PL_{nm}^{ij} \times \left((TA_{nm} + TC_{nm} + TE_{nm}) + \sum_{l \in D_{nm}} (PL_{lm}^{nm} \times (TA_{lm} + TC_{lm} + TE_{lm})) \right) \right) \times \\
 & \times \sum_{k \in D_{ij}} [PL_{kj}^{ij} \times [(TA_{kj} + TC_{kj} + TE_{kj}) + \\
 & + \sum_{(m=1) \& (m \neq j)}^M \sum_{n=1}^{N_m} \left(PL_{nm}^{kj} \times \left((TA_{nm} + TC_{nm} + TE_{nm}) + \sum_{l \in D_{nm}} (PL_{lm}^{nm} \times (TA_{lm} + TC_{lm} + TE_{lm})) \right) \right) \right] \}.
 \end{aligned}$$

The availability factor readiness of a program system is determined as follows:

$$S = \frac{MTTF}{MTTF + TR}.$$

Man-hours for system engineering are equal to:

$$T_s = \sum_{j=1}^M \sum_{i=1}^{N_j} \left(B_{ij} T_{ij} + (NVP_{ij} + RB_{ij}) \cdot \left(NVX_{ij} + \sum_{k \in Z_{ij}} T_{ij}^k \right) \right).$$

For components in which introduction of program redundancy is possible, the following characteristics [9] can be changed:

1. A method of program redundancy implementation: multi-version programming ($NVP_{ij}=1$, $RB_{ij}=0$) or recovery block ($NVP_{ij}=0$, $RB_{ij}=1$). If the NVP method is chosen, then the gene value is established as 0, if the RB method is chosen, then the gene value is established as 1.

2. The variant (alternative) number Var_{v1} is “failure probability / man-hours”. Possible versions are set by the analyst for each component ($1 \leq Var_{v1} \leq V_{ij}$). V_{ij} is the number of alternative versions of development for each component.

3. The variant number $Var_{v2} \dots Var_{v10}$ is the probabilities of failure for each version of a component, similar to the above point 2 ($0 \leq Var_{v2 \dots 10} \leq V_{ij}$, 0 – there is no version). The limiting number of program component versions if redundancy will be applied, is set beforehand by the analyst and there cannot be more than 10 versions since a larger quantity brings additional complexity and cost in a component, unjustified by increase in dependability.

If genes $Var_{v2} \dots Var_{v10}$ take on the value 0, it is considered that program redundancy is not introduced in the given component ($B_{ij}=1$).

For components in which introduction of program redundancy is not provided, only the version Var of the component failure probability and corresponding labor input for achievement of this failure probability changes ($1 \leq Var \leq$ the number of versions for the given component).

Thus, the phenotype of an individual (decision) is formed from variable characteristics of program components [10]. Table 1 presents the general type of a phenotype with an example of alleles.

Table 1. Phenotype of an individual

Group of components with the possibility of program redundancy								Group of components with no possibility of program redundancy			
Component 1				..	Component N				Component 1	..	Component M
NVP/ RB	Var _{v1}	..	Var _{v4}		NVP/ RB	Var _{v1}	..	Var _{v5}	Var		Var
1	3		0		0	1		0	2		3

Crossing of the chosen individuals occurs with the predetermined probability. If parents are not crossed, their cloning takes place.

Crossing occurs by break of parents' chromosome in the set number of points, and descendants receive various attributes of both parents.

In nature there is a huge quantity of attributes and properties of live organisms which are defined by two and more pairs of genes and, on the contrary, one gene frequently supervises many attributes. Besides, action of a gene can be changed by the neighborhood of other genes and environment conditions. In one of studies as early as in 1928 J.A. Filipchenko proved that alongside with the "basic" gene determining an attribute there is a number of genes-modifiers of this attribute. The similar type of inheritance is met frequently. Thus, the phenotype, as a rule, represents the result of complex interaction of genes [11].

Thus, let us introduce the concept "related genes". The related genes are genes whose mutual combination influences a certain attribute of an individual.

Dependability and man-hours for components with possible program redundancy are defined by interacting genes of versions and redundancy method. Breaks of a chromosome can occur both between genes of one program component, and between genes of different components. And the probability of choosing a chromosome break point between genes of one program component (related genes) is predetermined. At uniform cross breeding break can occur either in all points or only between unrelated genes.

The mutation of individuals of a population occurs with the specified probability. In addition to the probability of mutation application to each individual, the probability of mutation application to its each gene is used with the size usually set from 1 up to 10 % [42]. At mutation of binary genes of redundancy method a value invert conversion takes place.

Alleles of genes of alternatives "failure probability / labor input" are characterized by a rank scale in such a manner that each following version is better in relation to dependability, but it is worse in relation to man-hours. Thus, predetermined alternative versions for a specific program component are Pareto optimal. The mutation of such genes can occur in two ways:

1. The choice of any alternative "failure probability / labor input" is equiprobable.
2. The choice of any version "failure probability / labor input" occurs with the probability distributed under the law of normal distribution of probabilities for a discrete random variable [12]. And the choice of the version current value is impossible. At the mutation of genes of versions of program components, for which the value 0 is possible (absence of any version), such value is added as an additional possible value. Table 3 presents probabilities of versions' choice at mutation of a gene of the program component version, whose current value is equal to 4, and the total number of specified versions is equal to 7.

Table 3. Probability distribution of a version choice

Absence of the version	Var. 1	Var. 2	Var. 3	Var. 4 (current)	Var. 5	Var. 6	Var. 7
0.015625	0.09375	0.234375	0.3125	0	0.234375	0.09375	0.015625

The genetic algorithm is based on ideas of a method with independent Shaffer's selection for multi-criterion optimization *VEGA* (*Vector Evaluated Genetic Algorithm*) [13].

Selection occurs with the probability proportional to criterion value. The probability of an individual to be selected under criterion S is calculated by the formula [14]:

$$p_i = \frac{f_i}{\sum_{j=1}^N f_j} = \frac{f_i}{\bar{f} \cdot N},$$

where f_i is the suitability of the individual i ; $\bar{f} = \frac{1}{N} \sum_{j=1}^N f_j$ is the average suitability of the population; N is the size of the population; $\sum_{j=1}^N p_j = 1$.

The probability of an individual to be selected under minimized criterion T_s is calculated by the following formula [15]:

$$p_i = \frac{-f_i + C}{N \cdot C - \sum_{j=1}^N f_j},$$

where f_i is the suitability of the individual i ; C is the constant determining the minimal suitability of the $C: p_i \geq 0, \forall i$ population; N is the size of the population; $\sum_{j=1}^N p_j = 1$.

In the considered algorithm the constant C is equal to the maximal suitability of an individual in population. Thus, the minimal probability of an individual to be the selected under criterion T_s is equal to 0.

When defining the suitability of an individual, the values S and T_s are calculated under the algorithm represented in fig. 1.

Each individual with calculated criteria is recorded into data array. Search of similar calculated earlier individual is carried out before criteria calculation for the following individual [10]. This action is reasonable and allows saving an operating time of algorithm since calculation of criteria is much longer than search of an identical individual in data array of decisions.

For the solution of the multi-criterion task of conditional optimization, it is necessary to use the approach based on conditional task reduction to the unconditional one. Search of Pareto optimal solutions is carried out under the design of *VEGA* method. Task solving with restrictions should belong to a Pareto set, as well as it should be in a legitimate range. Therefore, in addition to the offered algorithm, we should introduce an additional procedure that allows us to bring solutions into a legitimate range [14].

To make it possible to solve a conditional optimization task, each restriction should be considered as a separate criterion function and consequently, an initially conditional task with several criterion functions is reduced to the unconditional task of optimization. The transformation of an initial task of conditional multi-criterion optimization has the following form [14]:

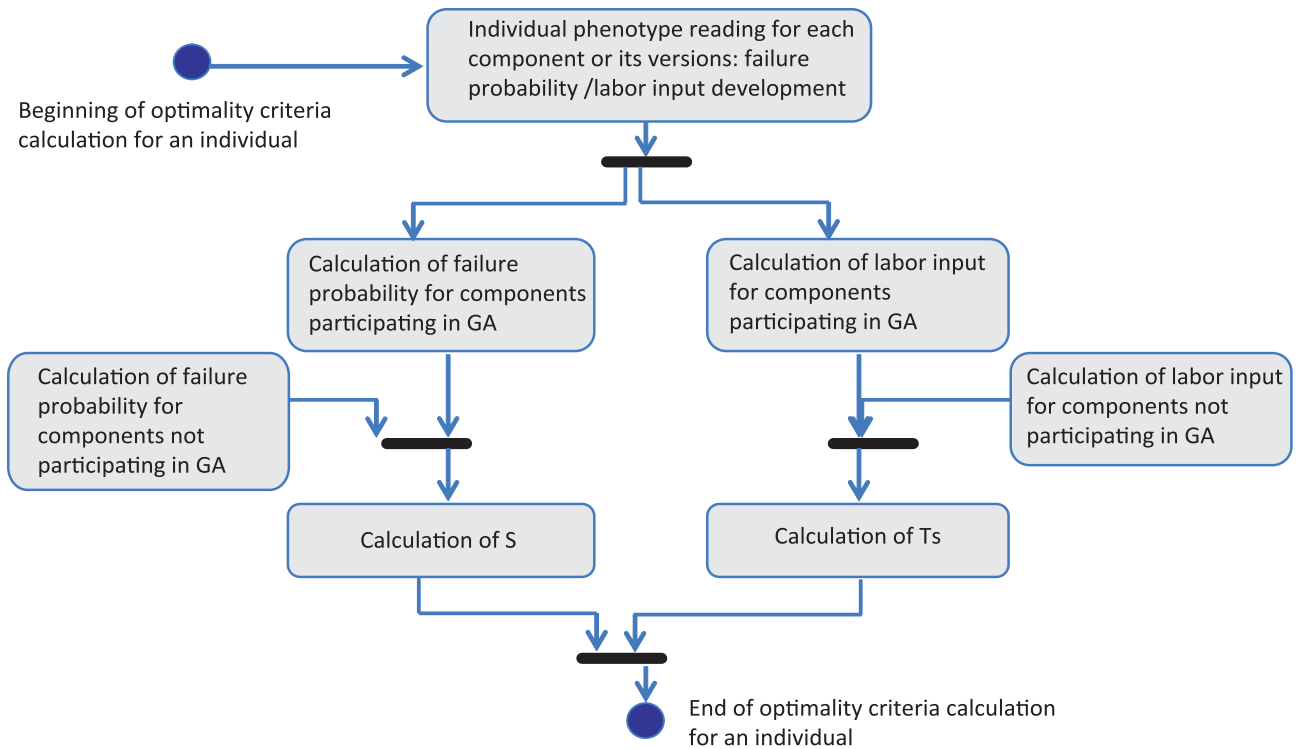


Fig. 1. Algorithm of optimality criteria calculation

Criterion functions of an initial task are $F(X) \rightarrow opt$, restrictions of the initial task are $G(X) \leq B$.

Criterion functions of the transformed task are $F(X) \rightarrow opt$, restrictions of the transformed task are $|G(X) - B| \rightarrow opt$.

For the first several iterations of the algorithm, the initial conditional task is solved, but without taking into account restrictions. Next, to receive a greater number of solutions belonging to the legitimate range, search proceeds this time without taking into account criterion functions of the initial task, but restrictions only. Thus, search of solutions is made only as to functions – restrictions, which brings the most part of the population into a legitimate range, but with loss of solutions' quality under criteria of optimization [14].

The genetic algorithm for multi-criterion conditional optimization of program architecture [16] is also based on ideas of *VEGA* method (*Vector Evaluated Genetic Algorithm*) with independent Shaffer's selection at multi-criterion optimization.

The difference of *VEGA* algorithm from *GA* (genetic algorithm) of unconditional optimization consists in the fact that each restriction in it is considered as additional criterion of optimization. With the part of generations, the algorithm works without taking into account additional criteria of optimization, and then with the rest of generations the algorithm works as to two criteria of restriction violation on S , T_s , and criteria of restriction violation RT_{ij} .

Input parameters of *GA* are the following:

- population size (N);
- probability of crossing ($prob_cross$);
- type of crossing (1,2,3-point, uniform);
- probability of related genes break ($prob_cross_inter$);
- probability of individual mutation ($prob_mutate$);
- probability of gene mutation ($prob_mutate_gen$);
- halt criteria (the maximal operating time $time_ga$, the number of populations without solution improvement $stagnancy$, the number of populations pop_count);

- percent of populations for processing of restrictions *percent_bound*;
- number of restrictions for the period of components' execution *B*.

The algorithm is implemented by the following sequence of actions:

1. Generation of parental population *P* with size *N* of casual individuals.
2. Calculation of criteria for all individuals of population *P*.
3. Proportional selection $N/2$ of individuals from *P* under criterion *S* in intermediate population *P'*.
4. Proportional selection $N/2$ of individuals by criterion T_s in intermediate population *P'*.
5. Crossing with probability *prob_cross* $N/2$ of casually chosen pairs of individuals from intermediate population *P'*. Generation of basic population *P* from *N* chosen individuals.
6. Execution of the mutation operator with the probability *prob_mutate* on each individual of basic population *P* and on each gene of an individual with the probability *rob_mutate_gen*.
7. Calculation of optimization criteria values for all individuals of population *P*.
8. Selection from population *P* of undominated solutions. If there are solutions in the decisions found earlier which dominate them, then *stagnancy* = *stagnancy* + 1.
9. If even one criterion of halt works, then the algorithm stops.
10. If the number of population is less, or equal to *percent_bound* * *pop_count*, then move to step 3.
11. Proportional selection of $N / (2+Q)$ of individuals from *P* under criterion of restriction violation on *S* in intermediate population *P'*.
12. Proportional selection of $N / (2+Q)$ of individuals under criterion of restriction violation on T_s in intermediate population *P'*.
13. Proportional selection $N / (2+Q)$ of individuals under each criterion of restriction violation for the period of RT_{ij} component implementation in intermediate population *P'*.
14. Crossing with probability *prob_cross* $N / (2+Q)$ of casually chosen pairs of individuals from intermediate population *P'*. Generation of basic population *P* from *N* chosen individuals.
15. Execution of the mutation operator with the probability *prob_mutate* on each individual of basic population *P* and each gene of an individual with the probability *prob_mutate_gen*.
16. Calculation of criteria under restrictions for all individuals of population *P*.
17. Selection from population *P* of the best decisions under criteria of restrictions. If there are better solutions in the decisions found earlier, then *stagnancy* = *stagnancy* + 1.
18. If even one criterion of halt works, then the algorithm stops, otherwise move to step 11.

Undominated decisions obtained for each iteration are selected in a Pareto set. Decisions of a Pareto set cannot be preferred to each other, therefore after its generation the task can be considered mathematically solved [17].

The developed genetic algorithm has been tested on specially prepared tasks and has also been used in development of the software for corporate control systems and OSW. With the help of the developed GA, all tasks have been effectively solved, efficient architectural decisions have been found.

References

1. **Kovalev I.** Optimal Time Cyclograms of Spacecrafts Control Systems / **I. Kovalev, O. Davydenko** // Advances in Modeling and Analysis. Vol.48. # 2-3.1996. AMSE PRESS. P. 19-23.
2. **Tsarev R.Yu.** Firmware of fail-safe and catastrophe-safe control and of the information processing systems: the study / **A.V.Anikonov, M.Yu..Slobodin, R.Yu.Tsarev.** – M.: Makc-press, 2006. – 244 p.
3. **Tsarev R.Yu.** Optimization and simulation approach to synthesis of the automated control systems / **I.V.Kovalev, M.V.Tjupkin, R.Yu.Tsarev, Yu.D.Tsvetkov** // Software products and systems. – 2007. – # 3. – pp. 73-74.

4. **Tsarev R.Yu.** System of multi-attributive formation of multi-version software in fail-safe control systems: PhD Thesis: Krasnoyarsk, 2003. – 143 p.
5. **Novoy A.B.** System for the analysis of software architectural dependability: PhD Thesis: Krasnoyarsk, 2011 – 131 p.
6. **Sheenok D.A., Kukartsev V.V.** Costs estimate for upgrading software of dependability critical systems // SibSAU Bulletin. Issue 5 (45). – 2012. – pp. 62-65.
7. **Sheenok D.A.** Updating of program architecture model for multi-criterion conditional optimization // Prospects of development of information technologies: Matter of XI international scientific – practical conference. – 2013. – pp 76-81.
8. **Rusakov M.A.** Multistage analysis of architectural dependability in complex information – management systems: PhD Thesis: Krasnoyarsk, 2005 – 168 p.
9. **Sheenok D.A., Kukartsev V.V.** Program architecture optimization of logistical information systems // Logistical systems in global economy: Matters of international scientific-practical conference. (March, 14-15, 2013, Krasnoyarsk). Part 1. – 2013. – pp 138-145.
10. **Sheenok D.A.** Genetic algorithm of software optimum architecture search // Urgent issues of modern science: Matter of IV international scientific conference on December, 14-15, 2012 – pp. 62-68.
11. **Inge-Vechtomov S.G.** Genetics with fundamentals of selection: Textbook for the biological special subject in universities. – M.: Higher school, 1989. – 591 p.
12. **Spitsyn V.G., Tsoy Yu. R.** Representation of knowledge in information systems: tutorial manual. – Tomsk: Publishing house TPU, 2006. – 146 p.
13. **Sergienko R.B.** Coevolution algorithm for tasks of conditional and multi-criterion optimization / **R.B.Sergienko, E.S.Semenkin** // Software products and systems. – # 4. – 2010. – pp. 24-28.
14. **Gumennikova A. V.** Adaptive search algorithms for the solution of complex tasks of multi-criterion optimization: PhD Thesis: Krasnoyarsk, 2006 – 129.
15. **Sopov E. A.** Evolutionary algorithms of complex systems modeling and optimization: PhD Thesis: Krasnoyarsk, 2004 – 129 p.
16. **Sheenok D.A.** Tool for designing of optimum architecture of fail-safe program systems // Program engineering. # 6. – 2013. – P. 20-26.
17. **Sergienko R.B.** Automated generation of fuzzy qualifiers by self-adapting coevolution algorithms: PhD Thesis: Krasnoyarsk, 2010 – 192 p.



Семенов С.С., Полтавский А.В., Маклаков В.В.

ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЙ ПРИ СОЗДАНИИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ И ЗАДАЧА ВЫБОРА АЛЬТЕРНАТИВ

Создание высококонкурентной продукции связано с принятием обоснованных и правильных решений, что может быть обеспечено применением системного подхода к созданию новой продукции и современных методов из области теории принятия решений. Одним из важнейших понятий системного анализа является понятие «принятие решений». В данной статье рассмотрены основные стадии жизненного цикла сложной технической системы (СТС), математическая постановка задачи принятия решений при создании СТС и условия по выбору методов решения задачи при анализе альтернативных решений. Показано значение процесса принятия решения на различных стадиях, при этом на основе современных представлений подробно описана процедура принятия решений, которая включает семь этапов – от целей решения проблемы и до ее реализации.

Ключевые слова: сложная техническая система, многоуровневые сложные технические системы, системный анализ, жизненный цикл, стадия жизненного цикла, процесс принятия решений, лицо принимающее решение, альтернативный вариант (альтернатива), показатели и критерии эффективности.

Введение

Теория принятия решений дает рецепт выбора линии поведения человека в различных ситуациях. По мере развития общества и информационных технологий усложняются условия, в которых оказывается человек.

Рациональная теория принятия решений призвана дать ответы на два вопроса:

- 1) Какие сведения существенные для данного выбора;
- 2) Как сопоставить их друг с другом, чтобы прийти к правильному заключению.

Основное свойство рационального решения – это оптимальность, т.е. при прочих равных условиях выбранный вариант должен иметь самую высокую оценку.

Этот простой принцип стремления к максимизации выигрыша и минимизации потерь представляется наиболее разумным в простых ситуациях [1]. В случае, когда мы имеем дело с техническими объектами (техническими системами), наши неправильные действия могут привести к невыполнению их основного назначения, потерям финансового и временного характера. В условиях

научно-технического прогресса, становления нового технологического уклада, основанного на новых и, прежде всего, информационных технологиях, выбор правильного и научно-обоснованного решения приобретает первостепенное значение.

Как в нашей стране, так и за рубежом разработана целая система мер по управлению и обеспечению выпуска качественной продукции. Возникла даже новая наука – квалиметрия, под которой понимают науку об измерении качества различных объектов [2, 3]. Данная наука основана на современных методах и моделях оценки качества и технического уровня (ТУ) создаваемой продукции и успешно развивается, о чем свидетельствует множество опубликованных статей в периодических изданиях и выпуск учебных пособий и монографий [4-8].

Применительно к продукции специального назначения в 1990-е годы был предложен метод оценки ТУ образцов вооружения и военной техники (ВВТ) с привлечением математических методов теории принятия решений и экспертных оценок [9], который затем получил применение и прошёл апробацию при оценке конкретных образцов ВВТ [10-12]. Данный метод, реализованный на компьютерных технологиях, вызвал широкое обсуждение среди ученых и специалистов оборонно-промышленного комплекса в силу простоты, доступности, надежности и оперативности получения результатов [13].

В данной статье рассмотрены особенности и уточнены основные понятия системного анализа, концепция к постановке задачи принятия решений и выбору альтернатив при создании сложных технических систем, а также основные этапы процесса принятия решений.

1. Особенности современных технических систем

В настоящее время технические системы, как правило, являются сложными, поэтому следует говорить о СТС, определение которым можно дать следующим образом: система – это внутренне организованная, на основе того или иного принципа, целостность, в которой все элементы настолько тесно связаны друг с другом, что выступают по отношению к окружающим условиям и другим системам как нечто единое [14]. Пока не существует формального и строгого определения понятия сложной или большой системы. Отметим основные свойства системы, которыми должен удовлетворять объект как СТС [15, 16]. Это признаки целостности и модульности объекта, наличие более или менее устойчивых связей (отношений) между элементами системы, при этом с системных позиций определяющими являются не любые связи, а только лишь существенные связи (отношения), которые определяют интегративные свойства систем, наличие интегративных свойств (качеств), присущих системе в целом, но не присущих ее элементам в отдельности, и организация (организованность) развивающихся систем, которая проявляется в структурных особенностях системы, сложности, способности сохранения системы и ее развития.

Системный анализ рекомендует начинать процесс принятия решений с выявления и четкого формулирования конечных целей, рассматривать проблему как единую систему и выявлять все последствия и взаимосвязи каждого частного решения, согласовывать цели подсистем с общей целью системы, выявлять и анализировать возможные пути достижения цели и выбирать из них наиболее эффективные.

Принимать решения приходится на всех стадиях жизненного цикла СТС. Согласно национальному российскому стандарту «Информационная технология. Системная инженерия. Процессы жизненного цикла систем ISO/IEC 15288:2002» различают семь стадий жизненного цикла (табл. 1) [17]: стадия замысла; стадия разработки; стадия производства; стадия применения; стадия управления в поддержке применения; стадия прекращения применения и списания.

Таблица 1. Этапы жизненного цикла СТС, цель и варианты решений на этапах в соответствии с ГОСТ ИСО 15288-2002

Этапы жизненного цикла	Цель	Варианты решений
1. Замысел	– Определение потребности заказчиков – Исследование концепции – Формирование предложений по жизнеспособным решениям	– Исполнение следующего этапа – Продолжение стадии – Переход к предыдущему этапу
2. Разработка	– Уточнение требований к системе – Создание проекта решения – Построение системы – Проведение верификации и валидации системы	– Задержка в исполнении проекта – Остановка проекта
3. Производство	– Производство системы – Инспектирование и тестирование	
4. Эксплуатация	– Использование системы для удовлетворения нужд заказчиков	
5. Сопровождение	– Обеспечение поддерживаемых системных возможностей	
6. Снятие с эксплуатации	– Хранение, архивирование или списание системы	
7. Утилизация		

Примечание к табл. 1

Верификация (*verification*) – подтверждение на основе представления объективных свидетельств того, что установленные требования были выполнены. Верификация в контексте жизненного цикла системы является совокупностью действий по сравнению полученного результата жизненного цикла системы с требуемыми характеристиками для этого результата. Результатами жизненного цикла могут являться (но не ограничиваются только ими) установленные требования, описание проекта и непосредственно система.

Валидация (*validation*) – подтверждение на основе представления объективных свидетельств того, что требования, предназначенные для конкретного использования или применения, выполнены. Валидация в контексте жизненного цикла системы является совокупностью действий, гарантирующих и обеспечивающих уверенность в том, что система способна выполнять заданные функции в соответствии с установленными целями и назначением в конкретных условиях функционирования.

Стадии могут применяться для построения структур, при помощи которых процессы жизненного цикла используются для моделирования непосредственно жизненного цикла. Масштабы и точность применения процессов в рамках описанных стадий и с учетом их продолжительности зависят от изменяющихся технических и деловых потребностей СТС (проекта), определяющих и использующих жизненный цикл. Пример информационной поддержки (ИП) СТС применительно к образцам ВВТ показан на рис. 1 [18].

2. Концепция к постановке задачи принятия решений и выбору альтернатив

Стратегия выбора может быть основана на предлагаемых комплексах методов, созданных моделей и алгоритмов, в которых задача принятия решений одна из самых распространенных в любой предметной области. При создании объектов СТС лицо, принимающее решение (ЛПР) сталкива-



Рис. 1. Реализация ИП-технологий на этапах жизненного цикла СТС:

ЕИП – единое информационное пространство, ИПИ – информационная поддержка изделий, ВТ – военная техника. Процесс решения задач принятия решений на этапах стратегического прогнозирования, планирования, распределения ресурсов и формирования (синтеза) альтернативных решений и пр. Решение таких задач сводится к выбору одного или нескольких лучших альтернативных вариантов из заданного набора множеств [19]. Для того чтобы сделать такой выбор, необходимо четко определить цель, задачи и критерии (совокупность показателей качества), по которым будет проводиться та или иная оценка для некоторого набора альтернативных вариантов.

Существует множество различных подходов к постановке задачи для выбора обоснованных решений при выборе объектов СТС [20]. Мы приведем один из альтернативных подходов применительно к критериально-экстремизационному выбору.

Пусть x – некоторое решение, возможные варианты которого определены на допустимом множестве X . Качество принимаемого решения ЛПР оценивается n скалярными критериями R_j , $j = 1, 2, \dots, n$, оценки по которым образуют вектор эффективности $r = r_1, \dots, r_n$. Этот вектор связан с альтернативой x функциональным отображением $F: X \rightarrow R$, которое может быть задано аналитически, статистически или эвристически. Необходимо найти такое множество из лучших вариантов Y , удовлетворяющий требованиям (желаниям) следующего вида:

$$Y_x = \{ \forall y \in X : \exists X \in X : r(x) \succ r(y) \}.$$

При данной постановке предполагается, что критериальная оценка $r(x)$ для варианта x зависит только от этого варианта и совершенно не зависит от того, какие другие возможные варианты включены в множество X .

Технология постановки задачи управления в принятии решения при разработке СТС состоит из трех этапов: задача анализа и теоретические исследования к постановке задачи, разработка концепции и построение комплекса методов и математических моделей, непосредственно организацию самого процесса испытаний и возможности их внедрения. Содержание этапов представлено в табл. 2.

Выбор того или иного метода (или комплекса методов) для решения задачи зависит от количества и качества доступной информации. Такие данные, необходимые для осуществления концепции

Таблица 2. Технология постановки задачи управления и принятия решений при создании СТС

Этапы	Содержание этапов
Этап № 1. Теоретические исследования	Описание системы и построение моделей СТС Анализ моделей СТС Задача синтеза управления (оптимизация) СТС Исследование устойчивости решений
Этап № 2. Построение моделей	Идентификация моделей Имитационные эксперименты
Этап № 3. Внедрение	Анализ эффективности проекта и внедрение

научно-обоснованного выбора, которую можно разделить на четыре категории: информация об альтернативных вариантах, информация о критериях выбора, информация о предпочтениях, информация множества решаемых задач.

Следует уточнить, что показатель эффективности оценивает количественную степень достижения цели, а критерий эффективности является некоторым правилом, с помощью которого по данному показателю эффективности выбирается наиболее предпочтительный вариант СТС.

При выборе альтернатив важным этапом является процесс принятия решений. Этот процесс является сложным, состоящим из ряда этапов и недостаточно освещен в литературе по принятию решений.

3. Процедура принятия решений при разработке СТС

Рассмотрим непосредственно сам процесс принятия решений при формировании технического решения. В соответствии ГОСТ ИСО 15288-2002 ранее введено такое понятие как «процессы проекта», которые включают:

- процесс планирования проекта;
- процесс оценки проекта;
- процесс контроля проекта;
- процесс принятия решений;
- процесс управления рисками;
- процесс управления конфигурацией;
- процесс управления информацией.

Процессы проекта используются для установления и выполнения планов, оценки фактических достижений и продвижений проекта в соответствии с планами и для контроля выполнения проекта вплоть до его завершения. Отдельные процессы проекта могут осуществляться в любой момент жизненного цикла и на любом уровне иерархии проектов как в соответствии с проектными планами, так и с учетом непредвиденных обстоятельств. Уровень точности и формализации, с которой осуществляются процессы проекта, зависит от сложности самого проекта и проектных рисков.

Планирование исследования операции, оценка и контроль являются ключевыми процессами практически для всех видов управления.

Цель процесса управления оценкой проекта заключается в определении статуса проекта. В ходе этого процесса периодически или при возникновении важных событий проводится оценка развития проекта и достижений относительно требований, планов и целей бизнеса. В случае обнаружения существенных отклонений информация о результатах оценки сообщается заинтересованным сторонам для осуществления адекватных управляющих воздействий.

В результате успешного осуществления процесса оценки проекта:

- становятся доступными показатели или результаты оценки рабочих характеристик проекта;
- оценивается адекватность ролей, обязанностей и полномочий участников проекта;
- оценивается адекватность ресурсов и услуг, необходимых для реализации проекта;
- анализируются отклонения от планируемых значений показателей рабочих характеристик проекта;
- заинтересованные стороны информируются о статусе проекта.

В системном анализе обычно считают, что выбор – это уже принятие решений. Однако из представленных элементов процесса проекта мы видим, что между элементами «оценка проектов» и «принятие решений» включен и элемент «процесс контроля проекта».

Цель процесса контроля проекта заключается в организации исполнения плана проекта и обеспечении гарантий реализации проекта в соответствии с планами и графиками в пределах бюджета проекта и гарантий удовлетворения технических целей.

В результате управления процессом принятия решений:

- определяются и совершаются корректирующие действия, если результаты проекта не соответствуют запланированным заданиям;
- инициируется перепланирование проекта, если цели проекта или ограничения изменились, или допущения, сделанные при планировании, оказались неверными;
- санкционируются действия по переходу от одного запланированного этапа или события к следующему (при условии успешной реализации предыдущего этапа или события);
- достигаются цели проекта.

В соответствии с ГОСТ ИСО 15288- 2002 цель процесса принятия решений заключается в выборе из существующих альтернатив наиболее предпочтительного направления проектных действий. Этот процесс является реакцией на возникающие в процессе жизненного цикла системы запросы о принятии решений, направленных на достижение заданных, желаемых или оптимальных результатов вне зависимости от характера или источников таких запросов. Альтернативные действия анализируются, и выбирается направление действий. Решения и их обоснование документируются для поддержки принятия решений в будущем.

В результате успешного осуществления процесса принятия решений:

- определяется стратегия принятия решений;
- определяются альтернативные направления действий;
- выбирается наиболее предпочтительное направление действий;
- принятое решение, его обоснование и допущения документируются и доводятся до сведения заинтересованных сторон.

Процесс принятия решения – это процесс, в результате которого поставленная проблема получает разрешение. Теории принятия решений посвящено достаточно много работ. В общем виде процесс принятия решения с технологической точки зрения хорошо изложен в методической разработке Новосибирского государственного технического университета, который можно представить в виде этапов решений [21]:

- Этап 1. Целевыявление.
- Этап 2. Формирование целей.
- Этап 3. Выработка решений.
- Этап 4. Выбор решений.
- Этап 5. Оценка решений.
- Этап 6. Принятие решения.
- Этап 7. Реализация решения.

Этап 1 является важным и определяющим, так как дает ответы на вопросы: какую проблему и в каких условиях нужно решать; когда ее нужно решать; какими силами и средствами она будет решаться.

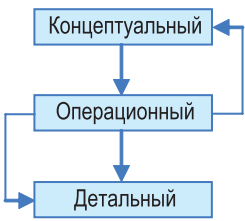
На втором этапе формулируются цели системы. Чем точнее будут сформулированы цели системы, тем легче выбрать средства их достижения. Методологической основой этапа формирования целей является системный анализ с использованием экспертных методов.

На третьем этапе вырабатываются альтернативные варианты решений, осуществляется поиск различных путей достижения поставленных целей. Формами генерирования альтернатив могут быть мозговой штурм, разработка сценариев и деловые игры.

Выбор решений из множества альтернативных производится ЛПР на четвертом этапе на основе сформированного критерия, по которому судят о степени достижения намеченной цели. Критерием полезности альтернативного решения может быть любой ее признак или множество признаков, измеренные на качественном либо количественном уровне. Для описания цели часто вводятся несколько критериев таким образом, чтобы они более полно характеризовали цель. Критерии для выбора решений определяются методами экспертного анализа и аппаратом математической статистики.

На пятом этапе на основе модели оценки альтернативных решений, учитывающей сложившуюся ситуацию, цели, множество ограничений, варианты решений производится оценка решений через систему предпочтений ЛПР для выбора наилучшего решения. Данная задача может решаться в условиях неопределенности, порожденной влиянием внешней среды на оценку альтернативных решений, которая может быть учтена с помощью известных приемов из теории вероятностей. При отсутствии неопределенности (в случае определенности) многие задачи принятия решений решают известными методами оптимизации.

Таблица 3. Иерархия уровней принятия решений

Уровни принятия решений	Объект исследования	Цель исследования	Модель	Показатели и критерии эффективности
	Система	Анализ концепций проведения операции. Определение перечня подцелей и задач, подсистем, условий их функционирования. Формирование «облика» системы.	Аналитическая	Степень достижения цели операции. Критерий пригодности. Критерий адаптивности.
	Подсистема	Анализ способов выполнения задач подсистемами. Определение обобщенного облика подсистем и средств, общие требования к качеству их элементов.	Имитационная	Степень выполнения задач подсистемами. Критерий пригодности. Критерий оптимальности.
	Элемент	Детальный анализ качества элементов.	Статистическая	Детальный анализ качества элементов.

Примечание. Для достижения поставленной цели необходима целенаправленная деятельность – операция. Операция есть система целенаправленных действий, объединенных общим замыслом и единой целью. Понятие операции включает три определяющих момента [22]: 1) управляющая деятельность человека (ЛПР), организующего операцию на основе выбора рационального использования активных средств для достижения цели операции; 2) активные средства (технические системы, ресурсы), находящиеся в распоряжении управляющего органа и используемые в операции в соответствии с выбранным способом (стратегии управления); 3) другие средства (системы), непосредственно взаимодействующие с активными средствами.

Самым важным является шестой этап, на котором необходимо выбрать решение для его последующей реализации по определенному алгоритму, выбирающему одно единственное решение, лучшее по некоторому критерию или принципу оптимальности.

При принятии решений по многим частным критериям (векторных задач оптимизации) возникают дополнительные трудности определения лучшего с точки зрения ЛПР компромиссного решения из множества допустимых по локальным критериям. Если требуется определить единственное наилучшее решение, то множество допустимых решений сводится к множеству Парето и в нем происходит поиск решения на основе некоторой схемы.

Седьмой этап реализует собственно достигнутое решение. План реализации выбранного решения должен дать ответы на вопросы, кто и что должен делать, какими средствами и в какие сроки. Конкретизация решения по исполнителям может производиться посредством задачи о назначениях исполнителей на выполнение комплекса работ, по срокам и объектам работ – методами сетевого планирования и управления.

Процесс принятия решений может проходить на различных иерархических уровнях. Различают концептуальный, операциональный и детальный уровни принятия решений [22]. В табл. 3 приведены особенности каждого уровня общей иерархии принятия решений и их взаимосвязь при исследовании СТС.

Так, при исследовании основных концепций проведения операции, определении предварительного перечня подцелей операции и задач подсистем сложной технической системы, формировании ее «концептуального» облика необходимо многократно и оперативно решать задачу синтеза через анализ, с целью отбраковки заведомо «худших» альтернатив. Здесь используются концептуальные модели.

На операциональном уровне исследований, когда определены цели, задачи и условия функционирования подсистемы, выявлена рациональная логика развития операции, можно учесть дополнительные факторы и построить более сложную модель для оценивания эффективности выполнения задач подсистемами сложной технической системы. Результатом этого этапа являются обобщенный облик подсистем и средств достижения цели, формулировка общих требований к качеству их элементов. Используемые на операциональном уровне модели, как правило, реализуются в виде сложных имитационных систем.

Уровень детального исследования предполагает создание подробных математических, физических и натурных моделей элементов подсистем для анализа их качества. Так как на этом этапе оперируют, как правило, фактическим материалом, используя методы планирования эксперимента, математической статистики и другие, то модели этого уровня являются в основном статистическими. Такая трехуровневая декомпозиция общей задачи принятия решений позволяет установить жизнеспособность выдвинутой концепции проведения операции и порождает единый (системный) взгляд на операцию и процесс принятия решений как с точки зрения ее цели, так и с учетом возможности других подсистем и средств. Она позволяет проводить оценку принимаемых решений на нижележащих уровнях с использованием известных методов исследования операций (условия и цели точно определены).

Выводы

1. Процедура принятия решений является сложным событием и одним из основных процессов при создании объектов СТС на всех этапах жизненного цикла. Принятие решения при этом происходит в результате наблюдения целого цикла событий: целевыявления, формирования новых и альтернативных идей выработки, обоснованных решений, получение оценки возможных решений, собственное принятие решений реализации решений.

2. Решение задачи по созданию эффективных объектов СТС сводится, как правило, к выбору одной или нескольких альтернатив из числа заданных. Для того чтобы обоснованно сделать такой выбор, необходимо четко определить цель, задачи и критерии (показатели качества), по которым будет проводиться сама оценка некоторого набора альтернативных вариантов.

Литература

1. Линдсей П., Норман Д. Переработка информации у человека. – М.: Мир, 1974. – 550 с.
2. Азгальдов Г.Г., Райхман Э.П. О квалиметрии. – М.: Изд-во стандартов, 1973. – 172 с.
3. Азгальдов Г.Г. Теория и практика оценки качества товаров. Основы квалиметрии. – М.: Экономика, 1982. – 256 с.
4. Андрианов Ю.М. Квалиметрия машиностроительной продукции. – Л.: Машиностроение, 1990. – 271 с.
5. Методы квалиметрии в машиностроении / А.И. Владимиров, В.Я. Кершенбаум, М.П. Поликарпов и др.; Под ред. В.Я. Кершенбаума, Р.В. Хвастунова – М.: Технонефтегаз, 1999. – 211 с.
6. Федюкин В.К., Дурнев В.Д., Лебедев В.Г. Методы оценки и управления качеством промышленной продукции. Учебник – М.: Информационно-издательский дом «Филинь», Рилант, 2000. – 328 с.
7. Федюкин В.К. Квалиметрия. – СПб.: СПбГИЭУ, 2009. М. – 365 с.
8. Кириллов В.И. Квалиметрия и системный анализ. – Минск: Новое знание: М.: ИНФРА-М, 2012. – 440 с.
9. Семенов С.С., Харчев В.Н., Иоффин А.И. Оценка технического уровня оружия – важный фактор его развития // Военный парад. – 1995 – № 1-2. – С. 174-176 (С. 87-89 – на англ. яз.).
10. Семенов С.С., Харчев В.Н., Иоффин А.И. Оценка технического уровня образцов вооружения и военной техники. – М.: Радио и связь, 2004. – 552 с.
11. Семенов С.С. Оценка технического уровня систем наведения управляемого авиационного оружия класса «воздух-поверхность» // Вестник компьютерных и информационных технологий. – 2006. – № 8 – С. 7-11; № 9 – С. 13-23; № 10 – С. 12-18.
12. Семенов С.С., Щербинин В.В. Метод оценки технического уровня систем наведения управляемых авиационных бомб // Вопросы оборонной техники. Сер. 9. Специальные системы управления, следящие приводы и их элементы. – М.: ФГУП «НТЦ «Информтехника», 2010. – Вып. 1 (242) – 2 (243). – 108 с. – С. 29-32.
13. Семенов С.С. Опыт научного признания новых методических подходов к оценке технического уровня образцов вооружения и военной техники на при-мере управляемых авиационных бомб // Боеприпасы. – 2007. – № 5-6. – 214 с.
14. Спиркин А.Г. Основы философии. – М.: Политиздат, 1988. – 592 с. – С. 179.
15. Цвиркун А.Д. Структура сложных систем. – М.: Советское радио, 1975. – 200 с.
16. Прангишвили И.В. Системный подход и общесистемные закономерности. – М.: СИНТЕГ, 2000. – 528 с.
17. ГОСТ Р ИСО/МЭК 15288 – 2005. Национальный российский стандарт. Информационная технология. Системная инженерия. Процессы жизненного цикла систем ISO/IEC 15288:2002 (System engineering – System life cycle processes (IDT)). – М. Федеральное агентство по техническому регулированию и метрологии, 2006. – 54 с.
18. Половинкин В., Дышкантюк А. Системный подход к оценке жизненного цикла вооружения ВМФ и методы его реализации // Морской сборник. – 2009. – № 7. – С. 23-28.
19. Райфа Г. Анализ решений (введение в проблему выбора в условиях неопределенности). – М.: Наука, Гл. ред. физ.- мат. лит., 1977. – 408 с.
20. Андрейчиков А.В., Андрейчикова О.Н. Системный анализ стратегических решений в инноватике. Математические, эвристические и интеллектуальные методы системного анализа и синтеза инноваций. – М. Книжный дом «ЛИБРОКОМ», 2013. – 304 с.
21. Самков Т.Д. Теория принятия решений: конспект лекций. – Новосибирск: – НГТУ, 2010. – 107 с.
22. Надежность и эффективность в технике: Справочник. Т.3. Эффективность технических систем / Под общ. ред. В.Ф. Уткина, Ю.В. Крючкова. – М.: Машиностроение, 1988. – 328 с.



Semienov S.S., Poltavsky A.V., Maklakov V.V.

PROCESS OF DECISION-MAKING IN DEVELOPMENT OF COMPLEX TECHNICAL SYSTEMS AND THE TASK OF CHOICE OF ALTERNATIVES

Developing highly competitive products involves making well-grounded and correct decisions which can be ensured by a systemic approach to the creation of new products and advanced decision-making methods. One of the primary concepts of system analysis is the concept of decision-making. The paper considers the primary lifecycle stages of a complex engineering system (CES), the statement of the decision-making problem in respect to CES development and conditions of selection of solution methods as part of alternative solutions analysis. The authors demonstrate the significance of the decision-making process at various stages. From the standpoint of state-of-the-art concepts, the paper provides a detailed description of the decision-making procedure proper that involves seven stages – from the purpose of problem solution to its implementation.

Keywords: complex engineering system, multilevel complex engineering systems, system analysis, lifecycle, lifecycle stage, decision-making process, decision-maker, alternative, efficiency indicators and criteria.

Introduction

The decision-making theory provides the recipe for the choice of human behavior in various situations. As the society and information technology develop, the conditions in which people find themselves get more complex as well.

The rational decision-making theory is to answer two questions:

- 1) What information is relevant to this choice;
- 2) How to compare them in order to come to the correct conclusion.

The main property of a rational decision is its optimality, i.e. other conditions being equal, the chosen alternative must have the highest rating.

This simple principle of maximized gain and minimized loss appears to be the most reasonable in simple situations [1]. In case of technical objects (engineering systems) our incorrect actions can cause them to not perform their main functions, as well as financial and time loss. In the age of scientific and technical progress, the advent of the new era of innovation based upon new and, first of all, information technologies, the choice of the correct and scientifically grounded decision becomes more and more relevant.

Both in Russia and abroad, a whole system of product quality assurance has been developed. A new science, qualimetry, has emerged that deals with the measurement of the quality of various objects [2, 3].

This science is based on state-of-the-art methods and models of quality and performance evaluation of developed products and is successfully developing as evidenced by a multitude of articles in periodical publications, as well as a number of educational books and monographs [4-8].

In 1990s, with regards to special-purpose products, a method of performance evaluation of weapons and military equipment (WME) using mathematical methods of decision-making and expert evaluation theory [9] was suggested and later tested and used for the purpose of WME evaluation [10-12]. This computer-assisted method was widely discussed in the defense systems engineering community due to its simplicity, affordability, dependability and quick delivery of results [13].

This article analyzes the distinctive features and specifies the primary concepts of system analysis, concept of goal setting for decision-making and choice in the development of complex engineering systems, as well as the main stages of decision-making.

1. Distinctive features of state-of-the-art engineering systems

Most state-of-the-art engineering systems are complex, therefore we should focus the discussion on CESs that can be defined as follows: «System is an entity internally organized on the basis of a certain principle, in which all the elements are so closely related that they act as an integral whole towards the environment and other systems» [14]. No formal and strict definition of a complex or large system exists yet. Let us note the primary system properties a CES must have [15, 16]. Those are the integrity

Table 1. CES lifecycle stages, goal and alternatives at stages as per GOST ISO 15288- 2002

Lifecycle stages	Goal	Alternative solutions
1. Design	– Customer requirement definition – Concept study – Development of proposals for viable decisions	– Next stage execution – Resumption of stage – Transition back to the previous stage – Project execution delay – Project interruption
2. Development	– System requirements specification – Design of draft decision – System construction – System verification and validation	
3. Production	– System production – Inspection and testing	
4. Operation	– Use of the system for satisfaction of customer requirements	
5. Maintenance	– Maintenance of system capabilities	
6. Decommissioning	– Storage, archiving and decommissioning	
7. Disposal		

Notes.

Verification is the evidence-based confirmation of the fact that the specified requirements have been met. In the context of system lifecycle, the verification is a package of measures aimed at comparing the results of a system lifecycle with the respective required values. The lifecycle results (without limitations) are the specified requirements, project description and system itself.

Validation is the evidence-based confirmation of the fact that the requirements specified for a certain use or application have been met. In the context of system lifecycle, validation is a package of measures that guarantee and ensure that a system is capable of performing the specified functions in accordance with the specified goals and purposes in specific operational conditions.

and modularity of an object, presence of more or less stable connections (relations) among the system elements, though not any connections are considered defining from the system point of view, but only significant ones that define the integrative properties of systems, presence of integrative properties intrinsic to the system as a whole, but not to individual elements, and organization of evolutionary systems that manifests itself in the structural features of the system, its complexity, ability to preserve itself and develop.

The system analysis recommends beginning the decision-making process with the identification and clear definition of the ultimate goals, considering the problem as an integral system and identifying all consequences and connections of each specific solution, coordinating subsystems goals with the common system goal, identifying and analyzing possible ways of reaching the goal and choosing the most efficient ones.

Decisions have to be taken at all stages of CES lifecycle. According to the national Russian standard «Information Technology. System Engineering. System life cycle processes ISO/IEC 15288:2002», there are six lifecycle stages (table 1) [17]: design; development; manufacture; application; application support management; decommissioning and disposal.

The stages can be used to design structures that help use lifecycle processes in modeling the lifecycle itself. The scale and accuracy of process application within the described stages and subject to their duration depend on the changing engineering and business requirements of the CES (project) that define and use the lifecycle. An example of information support (IS) of CES in the area of WME is shown in fig. 1[18].

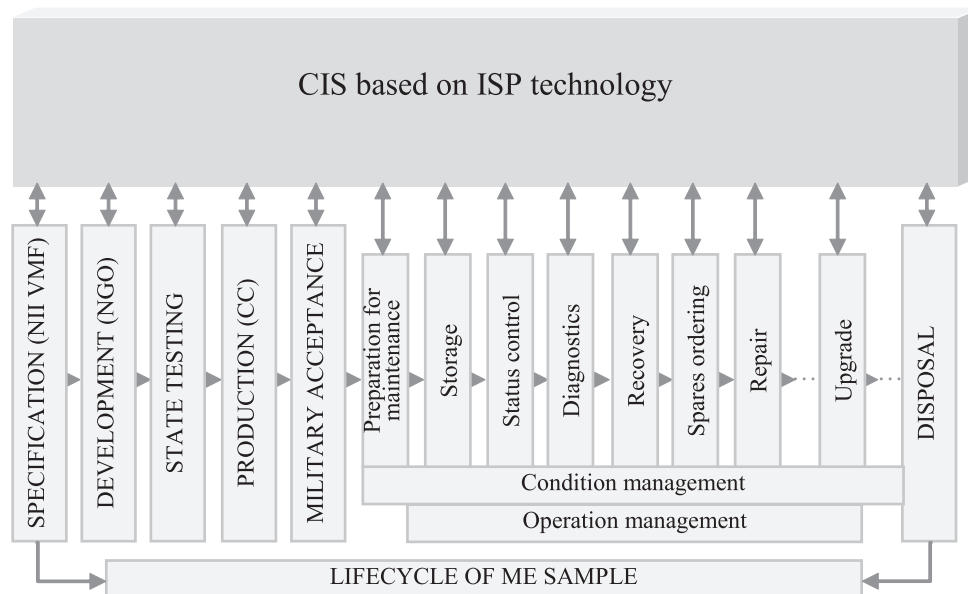


Fig. 1. Implementation of IS technologies at WME lifecycle stages: CIS – common information space, ISP – information support of products, ME – military equipment

2. Concept of goal setting for decision-making and choice

The choice strategy can be based on the suggested suites of methods, developed models and algorithms. In the process of development, the decision-maker has to solve decision-making tasks at the stages of strategic forecasting, planning, resources distribution, generation (synthesis) of alternatives, etc. The solution of such tasks comes down to choosing one or more best alternatives from defined sets [19]. In order to make such choice, it is required to clearly define the goal, tasks and criteria (a whole set of quality indicators), that will be used in evaluations for a certain set of alternatives.

There is abundance of various methods of specifying the task for making substantiated decisions while choosing among CES objects [20]. We will consider one of the alternative methods as applied to criteria extremalization choice.

Let x be a solution whose alternatives are defined within the allowable set X . The quality of decisions made by the decision-maker is defined by n scalar criteria $R_j, j = 1, 2, \dots, n$, the evaluations based on which form the efficiency vector $r = r_1, \dots, r_n$. This particular vector is connected to the alternative x by the function $F: X \rightarrow R$ that can be defined analytically, statistically or heuristically. It is required to find a set of best alternatives Y that meets the following requirements:

$$Y_x = \{ \forall y \in | \exists X \in X : r(x) \succ r(y) \}.$$

In this case it is assumed that the criterial evaluation $r(x)$ for the alternative x depends only on this alternative and does not depend at all on any other alternatives in the set X .

With respect to CES development, the procedure of control task definition in decision-making consists of three stages: the task of analysis and theoretical research for task definition, development of a concept, suite of methods and mathematical models, organization of the testing process and implementation capabilities. The content of the stages is given in table 2.

Table 2. Technology of task definition of management and decision-making as part of CES design

Stages	Stages content
Stage No. 1. Theoretical research	System description and CES models construction CES models analysis CES management synthesis (optimization) task Decision stability study
Stage No. 2. Models construction	Models identification Simulation experiments
Stage No. 3. Implementation	Project efficiency analysis and deployment

The choice of a specific method (or suite of methods) in order to solve a problem depends on the quantity and quality of available information. Such data are required for the implementation of the scientifically substantiated choice concept. It can be divided into four categories: information on alternatives, information on choice criteria, information of preferences, and information of the multitude of solvable tasks.

It should be specified that the efficiency indicator identifies the quantitative degree of attaining the goal, and the efficiency criterion is a certain rule that helps choose the most preferable CES variant based on the efficiency indicator.

The decision-making itself is an important stage of the choice process. This process is complex and multi-staged. It is though poorly covered in papers dedicated to decision-making.

3. Decision-making procedure used in the development of complex engineering systems

Let us consider the decision-making process involved in the development of engineering solutions. GOST ISO 15288-2002 has introduced the concept of «project processes» that include:

- project planning process;
- process evaluation process;

- project control process;
- decision-making process;
- risk management process;
- configuration management process;
- information management process.

Project processes are used for establishment and implementation of plans, evaluation of project progress as compared to plan and project execution control up to its completion. Individual project processes can be performed at any point of the lifecycle and at any level of project hierarchy both in accordance with project plans, and in emergency mode. The level of accuracy and formalization of project processes depends on project complexity and project risks.

The planning of operations research, evaluation and control are the key processes for practically all types of management.

The purpose of the project evaluation management process is defining the project status. In the course of this process, on a regular basis or concurrently with important events, project progress evaluation and performance assessment are performed. In case of significant irregularities, evaluation results are brought to the attention of stakeholders in order to ensure adequate administrative action.

As a result of successful project evaluation:

- project performance indicators and evaluation results become available;
- project parties' roles, duties and authority adequacy is evaluated;
- adequacy of the resources and services required for project implementation is evaluated;
- project performance irregularities are analyzed;
- stakeholders are informed of the project status.

In system analysis, it is normally believed that choice itself is decision-making. However, having analyzed the project process elements, we can see that between the “project evaluation” and “decision-making” there is the “process control process” element.

The purpose of the project control process is to organize project plan performance and assurance of project performance according to plans and time schedule within the project budget and guaranteed engineering purposes implementation.

As a result of control, the following happens in the decision-making process:

- corrective actions are defined and performed, should project results not correspond to respective planned tasks;
- project replanning is initiated, if project goals and restrictions have changed, or assumptions made at planning turned out to be wrong;
- transition from one planned stage or event to another is authorized (provided the previous stage or event was successful);
- project goals are reached.

According to GOST ISO 15288-2002, the purpose of the decision-making process is to choose the alternative that most suits the project goals. This process represents the reaction to decision-making requests that arise over the course of the system's lifecycle. Those requests aim to reach specified, desirable or optimal results regardless of the nature or source of such requests. Alternative actions are analyzed and the direction is chosen. The decisions and their substantiations are documented for future decision-making support.

As a result of successful decision-making:

- the decision-making strategy is defined;
- possible alternative actions are identified;
- the most preferable action is chosen;
- the decision taken, its substantiation and assumptions are documented and brought to the attention of stakeholders.

The decision-making process is a process that results in the solution to the defined problem. A significant number of scientific papers is dedicated to the decision-making theory. In general, from the process point of view, the decision-making process is well analyzed in a guidance paper published by the Novosibirsk State Technical University. The process can be represented as a series of decision stages [21]:

- Stage 1. Goal identification.
- Stage 2. Goal development.
- Stage 3. Decisions generation.
- Stage 4. Choice of decision.
- Stage 5. Decisions evaluation.
- Stage 6. Decision-making.
- Stage 7. Decision implementation.

Stage 1 is important and determinant as it answers the following questions: what problem and in what conditions must be solved; how it should be solved; what assets will be used to solve it.

At the second stage, system purposes are defined. The better the system purposes are defined, the easier it will be to choose the means to achieve them. The methodological foundation of the goal definition stage is the system analysis with the use of expert methods.

At the third stage, alternatives are generated, various ways of reaching the goal are found. Alternatives can be generated by means of brainstorming, scenario generation and business games.

The choice of solutions from a number of alternatives is made by the decision-maker at the fourth stage based on the generated criterion that helps judge if the goal has been met. The criterion of an alternative's usefulness may be any of its properties or a set of properties measured qualitatively or quantitatively. In order to describe the goal, several criteria are often introduced in such a way as to describe the goal as completely as possible. The criteria for solution selection are defined using expert analysis and mathematical statistics.

At the fifth stage, based on the alternatives evaluation model, that takes into account the current situation, goals, a multitude of restrictions, alternative solution, the available solutions are evaluated based on the decision-maker's preferences. This task can be completed under the conditions of uncertainty caused by the influence of external factors on the alternatives' evaluation that can be taken into account using well-known probability theory methods. If uncertainty is absent (in case of certainty) many decision-making tasks are solved through well-known optimization methods.

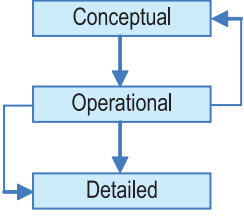
The sixth stage is the most important one, when it is required to choose the solution for its subsequent implementation using a certain algorithm that chooses the only solution that is superior in terms of a criterion or the optimality principle.

In case of decision-making based on many partial criteria (vectorial optimization tasks), additional difficulties arise in the identification of the best, from the decision-maker's point of view, compromise solution out of a number of allowable ones based on local measures. If it is required to identify the only best solution, then the set of allowable solutions comes down to a Pareto set and the search is made within it based on a certain scheme.

The seventh stage implements the achieved solution. The plan of solution implementation must answer the question as to who and what should do, by what means and within what timeframe. Responsible parties can be specified by means of work package performer appointment task, while the timeframes and work objects are specified by means of network planning and management.

Decision-making can be performed at various hierarchical levels. There are the conceptual, operational and detailed decision-making levels [22]. Table 2 sets forth the distinctive features of each of the levels of the overall decision-making hierarchy and their connections with regards to CES research.

Table 2. Decision levels hierarchy

Decision levels	Object of study	Goal of study	Model	Efficiency indicators and criteria
	System	Analysis of operations execution concepts. Identification of the list of subgoals and tasks, subsystems, their operating conditions. System «image» generation	Analytical	Operation goal attainment ratio. Suitability criterion. Adaptability criterion
	Subsystem	Analysis of methods of task performance by subsystems. Definition of the general images of subsystems and devices, general requirements to the quality of their elements	Simulation	Ratio of task performance by subsystems. Suitability criterion. Optimality criterion
	Element	Detailed analysis of the quality of elements	Statistical	Detailed analysis of the quality of elements

Notes. In order to reach the set goal, a purposeful activity, an operation, is required. An operation is a system of purposeful actions that share a common design and a common goal. The concept of operation includes three defining factors [22]: 1) human control activities (decision-maker) that organize the operation by choosing a rational way of using active means in order to achieve the operation's goals; 2) active means (engineering systems, resources) at the disposal of the managerial body and used in the operation in accordance with the chosen method (management strategy); 3) other means (systems) that directly interact with the active means.

Thus, in the course of research of primary operation performance concepts, definition of the preliminary list of subtasks of operations and purposes of subsystems of a complex engineering system and development of its conceptual design, it is required to repeatedly and promptly solve the synthesis task through analysis in order to eliminate the demonstrably worse alternatives. For that purpose, conceptual models are used.

At the operational level of research, when the subsystem goals, tasks and operating conditions have been defined and the rational logic of operation progress has been identified, additional factors can be taken into consideration and a more complex model can be designed in order to evaluate the performance of subsystems of a complex engineering system. The result of this stage is the consolidated concept of subsystems and means, as well as the general requirements to the quality of their elements. The models used at the operational level are usually implemented as complex simulation models. At the detailed research level, elaborate mathematical, physical and full-scale models are created in order to analyze the quality of subsystem elements. As this stage is normally evidence-based and uses the methods of experiment design, mathematical statistics, etc., this level's models are predominantly statistical. This three-level decomposition of the overall decision-making task allows establishing the viability of the suggested procedure performance concept and generate an integrated (systemic) vision of decision-making operation and process both in terms of their goal, and subject to the capabilities of other subsystems and assets. They enable the evaluation of the decisions taken at lower levels using well-known methods of operations research (conditions and goals are well defined).

Conclusions

1. The decision-making procedure is a complex event and one of the main processes of CES design at all lifecycle stages. Decision-making is the result of a series of events: goal identification, generation of new and alternative ideas, grounded decisions, evaluation of possible solutions, decision-making and implementation.

2. The development of efficient CES objects normally comes down to choosing one or more alternatives out of a number of specified ones. Making grounded decisions requires a clear goal, tasks and criteria (quality indicators) that are used for the evaluation of a set of alternatives.

References

1. **Lindsey P., Norman D.** Human Information Processing. Moscow. Mir, 1974. – 550 p.
2. **Azgaldov G.G., Raikhman E.P.** On Qualimetry. Moscow. Izdatelstvo standartov, 1973. – 172 p.
3. **Azgaldov G.G.** Theory and Practice of Product Quality Evaluation. Foundations of Qualimetry. Moscow. Ekonomika, 1982. – 256 p.
4. **Andrianov Yu.M.** Qualimetry of Automotive Products. Leningrad. Mashinostroenie, 1990. – 271 p.
5. Methods of Qualimetry in Engineering / Vladimirov, A.I., Kershenbaum, V.Ya., Polikarpov, M.P. et al.; Edited by **Kershenbaum, V.Ya., Khvastunov, R.V.** Moscow. Tekhnoveftegaz, 1999. – 211 p.
6. **Fediukin V.K., Durnev V.D., Lebedev V.G.** Industrial Products Evaluation and Quality Management Methods. Textbook – Moscow. Filin Information and Publishing House, Rilant, 2000. – 328 p.
7. **Fediukin V.K.** Qualimetry. Saint-Petersburg. SPbGIEU, 2009. Moscow. – 365 p.
8. **Kirillov V.I.** Qualimetry and System Analysis. – Minsk. Novoie znanie: Moscow. INFRA-M, 2012. – 440 p.
9. **Semionov S.S., Kharchev V.N., Ioffin A.I.** Weapon System Performance Evaluation as a Significant Factor of its Development // Voennyi Parad. – 1995 – № 1-2. – P. 174-176 (P. 87-89 in English).
10. **Semionov S.S., Kharchev V.N., Ioffin A.I.** Performance Evaluation of Weapon Systems and Hardware. – Moscow. Radio i svyaz, 2004. – 552 p.
11. Semionov S.S. Performance Evaluation of the Guidance Systems of Air-to-Surface Aircraft Weapon Systems // Vestnik kompiuternykh i informatsionnykh tekhnologiy. – 2006. – No. 8 – P. 7-11; No. 9 – P. 13-23; No. 10 – P. 12-18.
12. Semionov S.S., Shcherbinin V.V. Method of Performance Evaluation of the Guidance Systems of Guided Aerial Bombs // Voprosi oboronnoy tekhniki. Ser. 9. Special control systems, tracking drives and their elements. Moscow. FGUP NTTs Informtekhnika, 2010. – Issue 1 (242) – 2 (243). – 471 p. – P. 29-32.
13. **Semionov S.S.** Experience of Scientific Recognition of New Methods of Weapon Systems and Hardware Performance Evaluation through the Example of Guided Aerial Bombs // Boyepripasy. – 2007. – No. 5-6. – 214 p.
14. Spirkin A.G. Fundamentals of Philosophy. Moscow. Voenizdat, 1988. – 592 p. – P. 179.
15. Tsvirkun A.D. Structure of Complex Systems. Moscow. Sovetskoye radio, 1975. – 200 p.
16. **Prangishvili I.V.** System Approach and Systemic Consistency. Moscow. Sinteg, 2000. – 528 p.
17. GOST R ISO/IEC 15288 – 2005. Russian National Standard. Information Technology. System Engineering. ISO/IEC 15288:2002. System engineering – System life cycle processes (IDT). – Moscow. Federal Agency for Technical Regulation and Metrology, 2006. – 54 p.
18. **Polovinkin V., Dyshkantiuk A.** Systemic Approach to Naval Weapon Systems Lifecycle Evaluation and Implementation Methods // Morskoy sbornik. – 2009. – No. 7. – P. 23-28.
19. **Raiffa H.** Decision Analysis (Introductory Lectures on Choices Under Uncertainty). Moscow. Nauka, Main office of physics and mathematics literature, 1977. – 408 p.
20. **Andreichikov A.V., Andreichikova O.N.** System Analysis of Strategic Decisions in Innovation Theory. Mathematical, heuristic and intellectual methods of system analysis and innovation synergy. – Moscow. Knizhny dom LIBROKOM, 2013. – 304 p.
21. **Samkov T.D.** Theory of Decision-Making: Lecture Notes. – Novosibirsk: – NGTU, 2010. – 107 p.
22. Technology Dependability and Efficiency: Reference book. Efficiency of engineering systems / Edited by **Utkin, V.F., Kriuchkov, Yu.V.** Moscow. Mashinostroenie, 1988. – 328 p.

21.09.1935**20.09.2014**

Константин Николаевич Стась

На 79-м году жизни, не дожив одного дня до своего дня рождения, ушел из жизни Константин Николаевич Стась – организатор и главный редактор журнала «Ядерные измерительно-информационные технологии», издатель журнала «Надежность».

Свою трудовую деятельность Константин Николаевич начал в 1958 году в Союзном научно-исследовательском институте приборостроения (СНИИПе) Министерства среднего машиностроения (затем Министерства по атомной энергии, а теперь Госкорпорации «Росатом»). В 1960 году К.Н.Стась закончил Московский инженерно-физический институт факультет «Теоретической и экспериментальной физики» по кафедре «Дозиметрия и защита», получил звание инженер-физик и начал активно участвовать в работах СНИИПа по разработке методов радиометрии газов и жидкостей. Уже в скором времени он возглавил Лабораторию по разработке методов и аппаратуры для контроля радиоактивных газов в шахтах. Участвовал в экспедициях на урановые шахты в Среднюю Азию. Под его научным руководством Лаборатория стала лидером в стране по данному направлению, а методы и приборы, предложенные Константином Николаевичем с коллегами, успешно применялись и до сих пор применяются на предприятиях атомной отрасли, атомных станциях и других радиационных объектах России.

Глубокие научные знания, творческая активность, трудолюбие и энергия Константина Николаевича не остались незамеченными Руководством Института и Министерства. Он был выдвинут на должность Заместителя генерального директора Института, а затем на должность первого Заместителя генерального директора. На этих должностях Константин Николаевич проработал почти 18 лет. Именно здесь в полной мере раскрылись его организаторские способности. В Институте он руководил работами, связанными с предприятиями атомной отрасли. В сферу его деятельности также входили конструирование, технология изготовления и стандартизация изделий ядерного приборостроения.

Разработанные им методы и приборы легли в основу его диссертации на соискание ученой степени кандидата технических наук, которую он успешно защитил в 1974 году. В 1984 году ему было присвоено ученое звание старший научный сотрудник (доцент).

Константин Николаевич активно участвовал в работах по ликвидации последствий аварии на Чернобыльской АЭС, был одним из инициаторов разработки нового класса приборов – бытовых дозиметров для населения. Массовый выпуск и широкое использование этих приборов привело к существенному уменьшению радиофобии в стране. В последние годы полем его деятельности были аппаратура радиационного контроля и ядерные измерительно-информационные технологии.

К. Н. Стась – автор более 150 монографий, статей, изобретений и докладов на отечественных и международных конференциях. Метод определения радона по скрытой энергии К.П.Маркова, Н.В.Рябова и К.Н. Стася получил широкое признание, как в нашей стране, так и за рубежом. Большое внимание он уделял подготовке кадров, был научным руководителем нескольких аспирантов, которые успешно защитили свои диссертации.

Более 20 лет Константин Николаевич был руководителем Российской части Технического Комитета 45 «Ядерное приборостроение» Международной электротехнической комиссии (МЭК), возглавлял Российские делегации на сессиях ТК45 МЭК. Руководство ТК45 МЭК и зарубежные эксперты ценили Константина Николаевича за его широкую эрудицию в области ядерного приборостроения, высокий интеллект, дружелюбие, открытость, жизнерадостность и умение отстаивать свою позицию. Благодаря его усилиям Российская делегация пользовалась авторитетом в ТК45 МЭК. Он был инициатором практически всех стандартов ТК45 МЭК, разработанных российскими экспертами.

Журнал «Ядерные измерительно-информационные технологии», который создал и возглавлял Константин Николаевич, включен в перечень ведущих журналов и изданий ВАК, а также является журналом МЭК/ТК45 «Ядерное приборостроение». В нем ведущие отечественные и зарубежные ученые и специалисты публикуют свои статьи по проблемам и достижениям в области ядерной и радиационной безопасности, создания современной аппаратуры радиационного контроля, материалы итогов заседаний ТК45 МЭК, разработки стандартов по ядерному приборостроению.

Константин Николаевич был организатором и президентом АНО «ИЗИНТЕХ», который проводил семинары для специалистов в области ядерных измерительно-информационных технологий. Он также был руководителем издательского ООО «Группа ИДТ». Издательство выпустило целый ряд интересных научных и научно-популярных книг отечественных и зарубежных авторов.

За успешную работу и высокий профессионализм Константин Николаевич был удостоен почетных званий «Заслуженный машиностроитель РФ», «Заслуженный работник атомной отрасли», был членом-корреспондентом Международной академии информатизации. За высочайшие научные и производственные достижения Константин Николаевич был награжден двумя орденами и многочисленными медалями.

Константин Николаевич был честным, душевным и отзывчивым человеком, всегда готовым оказать помощь в решении возникших проблем.

Память о нем надолго останется в наших сердцах.

Заместитель главного редактора журнала «Ядерные измерительно-информационные технологии», д.т.н., профессор Борис Поленов

21.09.1935**20.09.2014**

Konstantin Nikolayevich Stasj

In his 79th year, one day before his birthday, died Konstantin Nikolayevich Stasj, the founder and editor-in-chief of Nuclear Measuring and Information Technology journal, the editor of Dependability journal.

In 1958 Konstantin Nikolayevich began his career in the Union R&D Institute for Instrumentation Manufacturing (SNIIP) of Ministry of Middle Engineering (further on Ministry of Nuclear Energy, now State Corporation Rosatom). In 1960 K.N. Stasj graduated from Moscow Engineering and Physics Institute, Theoretical and Experimental Physics faculty, chair of Dosimeters and protection with a degree of engineer-physicist and started to actively participate in the works of SNIIP as to development of methods of gas and liquid radiometric measurement. Very soon he became head of the Laboratory of methods and equipment for monitoring gases in mines. He took part in expeditions to uranium mines in Central Asia. Under his scientific guidance, the Laboratory became a leading unit in the country in the scientific area, and methods and equipment offered by Konstantin Nikolayevich and his colleagues have been successfully applied and are still used at the enterprises of nuclear industry, nuclear power plants and other radiation objects of Russia.

Profound scientific knowledge, creative activity, diligence and energy of Konstantin Nikolayevich didn't go unnoticed by heads of the Institute and the Ministry. He was promoted to the position of Director General Deputy of the Institute, then to the position of First Director General Deputy. In these positions Konstantin Nikolayevich worked for 18 years. It was here that his administrative talents revealed themselves fully. At the Institute he was in charge of works related to nuclear industry enterprises. The sphere of his activity also included designing, construction technology and standardization of products for nuclear instrumentation manufacturing.

Methods and instruments developed by him provided the basis for his PhD engineering thesis that he defended with success in 1974. In 1984 he was awarded a scientific degree of senior researcher (professor associate).

Konstantin Nikolayevich actively contributed to liquidation of consequences caused by the Chernobyl NPP accident, and he was one of the scientists who initiated the development of a new class of equipment

– consumer radiation dosimeters. Mass production and application of these instruments have radically reduced the radiophobia around the country. For the last years he specialized in radiation controlling equipment and nuclear measuring and information technology.

K.N. Stasj authored over 150 monographs, papers, patents and reports made at domestic and international conferences. The method of radon detection with latent energy by K.P. Markov, N.V. Ryabov and K.N. Stasj was widely accepted both locally and abroad. He paid much attention to the training of researchers, and he was scientific teacher for several postgraduate students who defended their theses with success.

For more than 20 years Konstantin Nikolayevich headed the Russian part of Technical Committee Nuclear Instrumentation Manufacturing of International Electrotechnical Committee (IEC), led Russian delegations at IEC TC45 sessions. IEC TC45 heads and foreign experts esteemed Konstantin Nikolayevich for his broad erudition in nuclear instrumentation manufacturing, intelligence, friendliness, open-mindedness, cheerfulness and capability to hold his ground. Thanks to his efforts, the Russian delegation had authority with IEC TC45. He initiated practically all the standards of IEC TC45 developed by Russian experts.

Nuclear Measuring and Information Technology journal that was founded and headed by Konstantin Nikolayevich was included in the list of leading journals and editions of State Commission for Academic Degrees and Titles, and it is also an official edition of IEC TC45 Nuclear Instrumentation Manufacturing. It publishes papers by major domestic and foreign researchers and experts about issues and achievements in the field of nuclear and radiation safety, development of advanced radiation control equipment, IEC TC45 meeting reports, and draft standards in nuclear instrumentation manufacturing.

Konstantin Nikolayevich was founder and president of ANO IZINTECH which held seminars for specialists in nuclear measuring and information technology. He was also head of the publishing house IDT Group Ltd. The publishing house issued a number of interesting scientific and popular scientific books by domestic and foreign authors.

For his successful work and high professionalism, Konstantin Nikolayevich was awarded honorary titles Honored Engineer of Russian Federation, Honored Worker of Nuclear Industry, was member of International Academy of Informatization. Konstantin Nikolayevich was awarded two orders and many medals for great scientific and industrial achievements.

Konstantin Nikolayevich was an honest, sincere and sympathetic man who was always ready to give a helping hand in case of troubles.

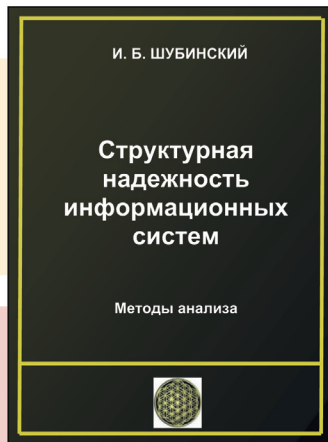
Memories of him will for long stay in our hearts.

Deputy of editor-in-chief of Nuclear Measuring and Information Technology journal, doctor of technical sciences, professor Boris Polenov

НАДЁЖНОСТЬ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

ПРЕДСТАВЛЯЕТ



Приобрести издание
можно через редакцию
ООО «Журнал «Надёжность»

8 (495) 967-77-05, доб.186
8-916-105-81-31
(Патрикеева Евгения)

E.Patrikeeva@gismps.ru,
www.dependability.pro

И. Б. ШУБИНСКИЙ

Структурная надежность информационных систем

Методы анализа



Шубинский Игорь Борисович

СТРУКТУРНАЯ НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
Методы анализа

Редактор: Патрикеева Евгения Владимировна
Компьютерная верстка: Куртиш Борис Сергеевич
Корректор: Комарова Екатерина Евгеньевна

Подписано в печать 12.07.2012. Формат издания 70х100/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 17,55.
Тираж 700 экз. Заказ № 1452.

ООО «Журнал «Надёжность»,
109029, г. Москва,
ул. Нижегородская, д.27, стр.1, офис 209
Тел./факс: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

И.Б.Шубинский «Структурная надежность информационных систем» 2012г.

В книге приведены основные понятия и показатели структурной надежности информационных систем, показана общность и специфические отличия показателей надежности, применяемых в отечественных и международных стандартах. Отражены недавние изменения в подходах к моделированию надежности. Подробно описаны Марковские модели надежности и графовые полумарковские методы расчета надежности, которые проиллюстрированы многочисленными примерами. Значительное внимание уделено инженерным методам расчета и приближенного прогнозирования структурной надежности информационных систем, оценкам погрешностей расчетов, а также статистической оценке показателей надежности. В конце каждой главы содержатся контрольные вопросы по наиболее сложному и значимому материалу главы.

Книга рассчитана, в первую очередь, на специалистов, занимающихся практической работой по разработке, производству, эксплуатации и модификации информационных систем. Она предназначена научным работникам в области структурной надежности различных дискретных систем, преподавательскому составу, аспирантам и студентам, специализирующимся в области информационных систем, а также в области автоматизированных систем управления.

Приобрести издание можно через редакцию журнала «Надёжность»
по тел. 8 (495) 967-77-05, доб.186; 8-916-105-81-31 (Патрикеева Евгения),
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

Igor B. Shubinsky STRUCTURAL DEPENDABILITY OF INFORMATION SYSTEMS 2012

The book presents the basic concepts and parameters of the structural dependability of information systems. It discusses general and specific differences in dependability indices used in domestic and international standards, along with recent developments in approaches to dependability modeling. Markov reliability models together with graph semi-Markov methods for calculating reliability are described in detail and illustrated by numerous examples. Considerable attention is paid to the engineering methods of calculation and the approximate prediction of structural dependability and error estimation of information systems as well as to the statistical assessment of dependability parameters. At the end of each chapter there are checklists of the most complex and significant subjects of the chapter.

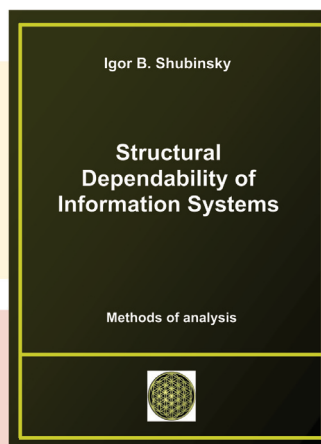
The book is intended primarily for professionals involved in practical work on the development, production, operation and modification of information systems. It is designed for scientists in the field of structural dependability of various discrete systems, academic staff and graduates (students) specializing in information systems as well as in the field of automated control systems.

Publication can be purchased through the editorial board of Journal Dependability Ltd.
by phone 8 (495) 967-77-05, ext.186; 8-916-105-81-31 (Patrikeeva Evgenia)
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

НАДЁЖНОСТЬ

DEPENDABILITY SCIENTIFIC AND TECHNICAL JOURNAL

REPRESENTS



Igor B. Shubinsky

Structural Dependability of Information Systems

Methods of analysis



Publication can be purchased
through the editorial board
of Journal Dependability Ltd.

8 (495) 967-77-05, ext.186;
8-916-105-81-31
(Patrikeeva Evgenia)

E.Patrikeeva@gismps.ru,
www.dependability.pro

Igor B. Shubinsky

STRUCTURAL DEPENDABILITY OF INFORMATION SYSTEMS
Methods of analysis

Editor: Patrikeeva Evgenia
Make-up: Kurtish Boris S.
Proofreading: Komarova Catherine E.

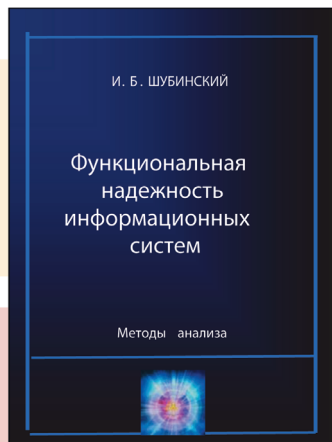
Copy deadline 12.07.2012. Format of the edition 70х100/16.
Offset printing. Offset paper. Conv. Sheet L 24,05.
Circulation of 700 copies. Order number 1452.

Journal Dependability Ltd.
109029, Moscow,
Nizhegorodskaya str., 27, bldg. 1, office 209
Tel. / Fax: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

НАДЁЖНОСТЬ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

ПРЕДСТАВЛЯЕТ



Приобрести издание
можно через редакцию
ООО «Журнал «Надёжность»

8 (495) 967-77-05, доб.186
8-916-105-81-31
(Патрикеева Евгения)

E.Patrikeeva@gismps.ru,
www.dependability.pro

И. Б. ШУБИНСКИЙ
**Функциональная
надёжность
информационных
систем**

Методы анализа

Шубинский Игорь Борисович
ФУНКЦИОНАЛЬНАЯ НАДЁЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
Методы анализа

Редактор: Патрикеева Евгения Владимировна
Компьютерная верстка: Куртиш Борис Сергеевич
Корректор: Комарова Екатерина Евгеньевна

Подписано в печать 12.07.2012. Формат издания 70х100/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 24,05.
Тираж 700 экз. Заказ № 1453.

ООО «Журнал «Надёжность»,
109029, г. Москва,
ул. Нижегородская, д.27, стр.1, офис 209
Тел./факс: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

И.Б.Шубинский «Функциональная надёжность информационных систем» 2012г.

В книге впервые представлена теория функциональной надёжности информационных систем как составная часть общей теории надёжности. Она включает понятия и определения; основные угрозы нарушения функциональной надёжности информационных систем; систему показателей; методы оценки функциональной надёжности цифровых устройств; методы и модели оценки функциональной надёжности программного обеспечения. В отдельной главе рассмотрена функциональная надёжность критически важных информационных систем, в том числе понятие критически важной системы, особенности оценки сбояных ошибок, оценки функциональной надёжности операторов, оценки опасных отказов и рисков, требования к функциональной надёжности и к архитектуре программного обеспечения критически важных информационных систем.

В конце каждой главы содержатся контрольные вопросы по наиболее сложному и значимому материалу главы.

Книга рассчитана, в первую очередь, на специалистов, занимающихся практической работой по разработке, производству, эксплуатации и модификации информационных технологий и информационных систем. Она предназначена научным работникам в области надёжности программно – аппаратных средств информационных систем, преподавательскому составу, аспирантам и студентам, специализирующимся в области информационных технологий, а также в области автоматизированных систем управления.

Приобрести издание можно через редакцию журнала «Надёжность»
по тел. 8 (495) 967-77-05, доб.186; 8-916-105-81-31 (Патрикеева Евгения),
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

Igor B. Shubinsky FUNCTIONAL DEPENDABILITY OF INFORMATION SYSTEMS 2012

For the first time, this book presents the theory of functional dependability of information systems as a component of the general dependability theory. The book comprises basic concepts and definitions, major threats for the functional dependability of information systems, system parameters, methods for estimating the functional dependability of digital devices, and methods and models of estimating software functional dependability. A separated chapter considers the functional reliability of critical information systems, including the concept of a critical system, features of faults, estimation of functional reliability of operators, estimation of hazardous failures and risks, the requirements of functional dependability and the software architecture of critical information systems. A checklist of the most complex and significant subjects is provided at the end of each chapter.

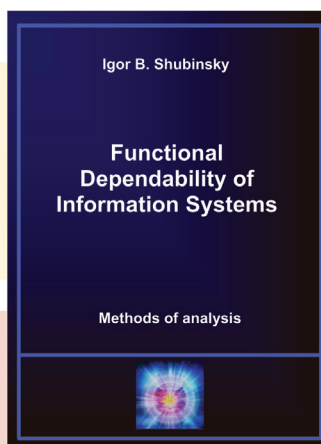
The book is primarily intended for experts who are engaged in practical development, manufacture, operation and updating of information technologies and information systems. It is intended for researchers in the field of software-hardware of information systems, academic staff, post-graduate students and students specializing in the field of information technologies as well as those working in the field of automated control systems.

Publication can be purchased through the editorial board of Journal Dependability Ltd.
by phone 8 (495) 967-77-05, ext.186; 8-916-105-81-31 (Patrikeeva Evgenia)
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

НАДЁЖНОСТЬ

DEPENDABILITY SCIENTIFIC AND TECHNICAL JOURNAL

REPRESENTS



Publication can be purchased
through the editorial board
of Journal Dependability Ltd.

8 (495) 967-77-05, ext.186;
8-916-105-81-31
(Patrikeeva Evgenia)

E.Patrikeeva@gismps.ru,
www.dependability.pro

Igor B. Shubinsky

**Functional
Dependability of
Information Systems**

Methods of analysis

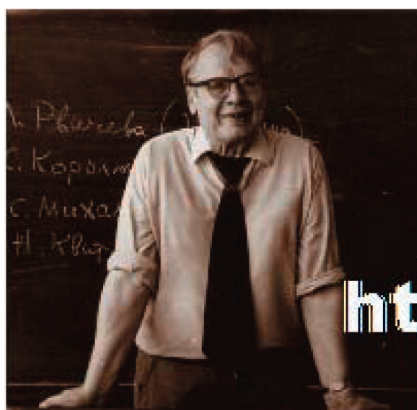
Igor B. Shubinsky

STRUCTURAL DEPENDABILITY OF INFORMATION SYSTEMS
Methods of analysis

Editor: Patrikeeva Evgenia
Make-up: Kurtish Boris S.
Proofreading: Komarova Catherine E.

Journal Dependability Ltd.
109029, Moscow,
Nizhegorodskaya str., 27, bldg. 1, office 209
Tel. / Fax: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

Copy deadline 12.07.2012. Format of the edition 70х100/16.
Offset printing. Offset paper. Conv. Sheet L 24,05.
Circulation of 700 copies. Order number 1452.



<http://Gnedenko-Forum.org/>

Дорогие коллеги!

В 2005 году была основана неформальная Ассоциация специалистов по надежности, прикладной вероятности и статистике (I.G.O.R.), которая имеет свой сайт в Интернете GNEDENKO FORUM. Сайт назван в честь выдающегося математика Бориса Владимировича Гнеденко (1912-1995). Целью Форума является улучшение профессиональных и персональных контактов специалистов по математической статистике, теории вероятностей и их важных ветвей, как Теория надежности и контроля качества, Теория массового обслуживания, Теории управления запасами и т.п.

Начиная с января 2006 года Форум издает ежеквартальный Международный электронный журнал

«Надежность: Теория и приложения» (“Reliability: Theory & Applications”).

Журнал зарегистрирован в Библиотеке Конгресса США (ISSN 1932-2321). Все права сохраняются за авторами, так что статьи затем могут быть свободно опубликованы в любых других изданиях или представлены на конференции.



**Вступайте в Форум
Гнеденко!**

Добро

пожаловать!

В наших рядах уже более

500 специалистов

из **44** стран мира.

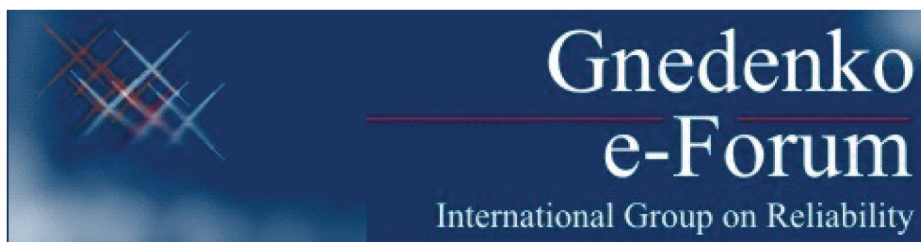
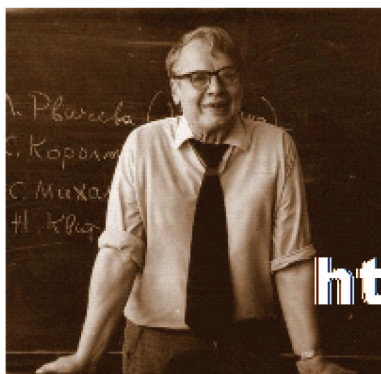
Для вступления в
Форум присылайте
фото и краткое резюме
по адресу:

Проф. Игорь Ушаков,
igusha22@gmail.com

или

к.т.н. Александр Бочков,
a.bochkov@gmail.com

Membership is free.



<http://Gnedenko-Forum.org/>

Dear colleagues!

In 2005 the informal Association of Experts in Reliability, Applied Probability and Statistics (I.G.O.R.) was established with its own Internet website GNEDENKO FORUM. The site has been named after the outstanding mathematician Boris Vladimirovich Gnedenko (1912-1995). The Forum's purpose is an improvement of personal and professional contacts between experts in the mathematical statistics, probability theory and their important branches, such as reliability theory and quality control, the theory of mass service, storekeeping theory, etc.

Since January 2006, the Forum has published a quarterly international electronic magazine

"Reliability: Theory and Applications".

The magazine is registered with the Library of Congress in the USA (ISSN 1932-2321). All rights reserved for authors so that articles can be freely published in any other publications or presented at conferences.



Join Gnedenko Forum!
Welcome!

**More than 500 experts
from 44 countries
worldwide have already
joined us!**

To join the Forum, send a
photo and a short CV to the
following address:

Prof. Igor Ushakov,
igusha22@gmail.com

or

Alexander Bochkov, PhD
a.bochkov@gmail.com

Membership is free.

АВТОРЫ НОМЕРА / AUTHORS OF THIS ISSUE**Викторова Валентина Сергеевна**

доктор технических наук, старший научный сотрудник, заведующий лабораторией, Институт проблем управления им. В.А.Трапезникова РАН (ИПУ РАН)
Тел.: +7 (910) 403-65-90
e-mail: viktorova_v@mail.ru

Зиннуров Тагир Альмирович

кандидат технических наук, старший преподаватель кафедры Мосты и транспортные тоннели, Казанский государственный архитектурно-строительный университет (КГАСУ)
Тел.: +7(950) 316-01-07
e-mail: leongar@mail.ru

Карцан Игорь Николаевич

кандидат технических наук, доцент, начальник военного института, Сибирский государственный аэрокосмический университет им. Академика М.Ф. Решетнева (СибГАУ)
Тел.: +7 (927) 133-09-81
e-mail: avkryanev@mephi.ru

Майстренко Игорь Юрьевич

кандидат технических наук, доцент кафедры Мосты и транспортные тоннели, Казанский государственный архитектурно-строительный университет (КГАСУ). Тел.: +7 (905) 313-22-53
e-mail: igor_maystr@mail.ru

Маклаков Владимир Васильевич

доктор технических наук, заведующий лабораторией, Институт проблем управления им. В.А. Трапезникова РАН. e-mail: lab-54@bk.ru

Нетес Виктор Александрович

доктор технических наук, профессор, начальник отдела прикладных задач развития телекоммуникаций, НТЦ «Комсет»
Тел.: + 7 (495) 921-34-12

Носов Михаил Васильевич

кандидат технических наук, профессор, заслуженный работник Высшей школы РФ, профессор кафедры «Инфокоммуникационных технологий и систем связи», Академия гражданской защиты МЧС России
Тел.: +7 (919) 721-48-29
e-mail: nosov.1933@mail.ru

Пегушин Станислав Леонидович

аспирант, Пермский Национальный Исследовательский Политехнический Университет
Тел.: +7 (951) 928-27-20
e-mail: staslp@mail.ru

Полтавский Александр Васильевич

доктор технических наук, старший научный сотрудник, Институт проблем управления им. В.А. Трапезникова РАН
e-mail: lab-54@bk.ru

Семенов Сергей Сергеевич

кандидат технических наук, руководитель группы анализа и перспективного проектирования, ОАО «Государственное научно-производственное предприятие «Регион»
e-mail: gnppregion@sovintel.ru

Степанянц Армен Суренович

старший научный сотрудник, Институт проблем управления им. В.А.Трапезникова РАН (ИПУ РАН)
Тел.: +7 (905) 718-25-17
e-mail: armen-stepanyats@mail.ru

Тарасьев Юрий Иванович

Заместитель генерального директора – директор по научной и экспертной работе, член ТК 259, член ТК 119, ЗАО «Научно-производственная фирма «Центральное конструкторское бюро арматуростроения» (ЗАО «НПФ «ЦКБА»)
Тел.: +7 (921) 308-62-84. e-mail: tarasev@ckba.ru

Терсков Виталий Анатольевич

доктор технических наук, профессор, профессор кафедры «Математика и информатика», Красноярский институт железнодорожного транспорта (КриЖТ), Иркутский государственный университет путей сообщения (ИрГУПС)
e-mail: dmitryshkras@rambler.ru

Шеенок Дмитрий Александрович

аналитик ООО «Сибирские интеграционные системы». Тел.: +7 (923) 303-36-37
e-mail: dmitryshkras@rambler.ru

Шпер Владимир Львович

кандидат технических наук, доцент, член ТК 119, Национальный исследовательский технологический университет «МИСиС». Тел.: +7 (916) 318-90-64. e-mail: vlad.shper@gmail.com

Шубинский Игорь Борисович

доктор технических наук, профессор, директор ЗАО «ИБ Транс». Тел.: +7 (495) 786-68-57
e-mail: igor-shubinsky@yandex.ru

Шумихин Александр Георгиевич

доктор технических наук, профессор, член Международной академии системных исследований, член-корреспондент Академии инженерных наук РФ, заведующий кафедрой АТП, Пермский Национальный Исследовательский Политехнический Университет
Тел.: +7 (342) 2-391-506
e-mail: atp@pstu.ru

Юсупов Ильдар Ильдусович

аспирант кафедры Мосты и транспортные тоннели, Казанский государственный архитектурно-строительный университет (КГАСУ)
Тел.: +7(9169) 64-05-20
e-mail: tpmost@mail.ru

АВТОРЫ НОМЕРА / AUTHORS OF THIS ISSUE

Viktorova Valentina Sergeevna

Doctor of Engineering, Head of laboratory, Senior Researcher V.A. Trapeznikov Institute of Control Problems of the Russian Academy of Sciences
Tel.: +7 (910) 403-65-90
E-mail: viktorova_v@mail.ru

Zinnurov Tagir Almirovich

PhD Engineering, senior lecturer of Chair of Bridges and Transport Tunnels, Kazan State Architecture and Construction University (KGASU)
Tel.: +7(950) 316-01-07
E-mail: leongar@mail.ru

Kartsan Igor Nikolaevich

PhD Engineering, professor assistant, Director of military institute SibGAU
Tel.: +7 (927) 133-09-81
E-mail: avkryanev@mephi.ru

Maystrenko Igor Yurjevich

PhD Engineering, professor assistant of Chair of Bridges and Transport Tunnels, Kazan State Architecture and Construction University (KGASU)
Tel.: +7 (905) 313-22-53
E-mail: igor_maystr@mail.ru

Maklakov Vladimir Vasilievich

Head of laboratory, Doctor of Engineering V.A. Trapeznikov Institute of Control Problems of the Russian Academy of Sciences
E-mail: lab-54@bk.ru

Netes Victor Alexandrovich

Doctor of Technical Sciences, Professor, Head of Division of Telecommunications Development Applied Tasks, NTC COMSET
Tel.: + 7 (495) 921-34-12
E-mail: netes@komset.ru

Nosov Mikhail Vasilievich

PhD Engineering, Professor, Honored worker of Higher School of Russian Federation, Professor of Chair of Infocommunication technology and telecommunication systems, Academy of civil protection (MChS) of Russia
Tel.: +7 (919) 721-48-29
E-mail: nosov.1933@mail.ru

Pegushin Stanislav Leonidovich

Post graduate student, Perm National Polytechnic Institute
Tel.: +7 (951) 928-27-20
E-mail: staslp@mail.ru

Poltavsky Alexander Vasilievich

Senior researcher, Doctor of Engineering, V.A. Trapeznikov Institute of Control Problems of the Russian Academy of Sciences
E-mail: lab-54@bk.ru

Semenov Sergey Sergeevich

Head of the Group for Analysis and Advanced Engineering, PhD Engineering, JSC Region State-Owned Research and Manufacturing Enterprise
E-mail: gnppregion@sovintel.ru

Stepanyants Armen Surenovich

Senior Researcher V.A. Trapeznikov Institute of Control Problems of the Russian Academy of Sciences
Tel.: +7 (905) 718-25-17
E-mail: armen-stepanyants@mail.ru

Tarashev Yuri Ivanovich

Deputy Director General – Director for scientific and expert activities, Member of TK 259, member of TK 119, Closed Company NPF Central Design Bureau of Fittings Industry (CJSC NPF CPBA)
Tel.: +7 (921) 308-62-84
E-mail: tarasev@ckba.ru

Terskov Vitaly Anatoljevich

Doctor of Engineering, Professor of Mathematics and Informatics Chair, KriZht IrGUPS
E-mail: dmitryshkras@rambler.ru

Sheenok Dmitry Alexandrovich

Analyst of Siberian Integration Systems Ltd.
Tel.: +7 (923) 303-36-37
E-mail: dmitryshkras@rambler.ru

Shper Vladimir Ljvovich

PhD Engineering, member of TK 119, National Research Technological University MISiS
Tel.: +7 (916) 318-90-64
E-mail: vlad.shper@gmail.com

Shubinsky Igor Borisovich

Professor, Doctor of Technical Sciences, Director of Closed Company IB Trans
Tel. +7 (495) 786-68-57
E-mail: igor-shubinsky@yandex.ru

Shumikhin Alexander Georgievich

Doctor of Technical Sciences, professor, member of International Academy of Systems Researches, associated member of Russian Academy of Engineering Sciences, Head of ATP Chair, Perm National Polytechnic University
Tel.: +7 (342) 2-391-506
E-mail: atp@pstu.ru

Yusupov Ildar Ildusovich

Post graduate student of Chair of Bridges and Transport Tunnels, Kazan State Architecture and Construction University (KGASU)
Tel.: +7(9169) 64-05-20
E-mail: tpmost@mail.ru

ТРЕБОВАНИЯ РЕДАКЦИИ ПО ОФОРМЛЕНИЮ СТАТЕЙ В ЖУРНАЛАХ ИЗДАТЕЛЬСКОЙ ГРУППЫ IDT PUBLISHERS

Письмо от организации, где работает автор(ы), либо лично от автора(ов) с предложением о публикации статьи направляется в редакцию журнала по фактическому адресу: 107078, г.Москва, Орликов переулок, д.5, офис 755 ООО «ЖУРНАЛ «НАДЕЖНОСТЬ» или по адресу e-mail: E.Patrikeeva@gismps.ru

(в отсканированном виде). Для журналов издательской группы IDT PUBLISHERS по адресу: 105005, г.Москва, набережная академика Туполева, д. 15, корп. 29 ООО «Издательский дом «Технологии» или по адресу e-mail: knstas@yahoo.com (в отсканированном виде).

К письму прилагается в электронном виде (на CD или по приведенному выше E-mail) текст статьи с аннотацией и ключевыми словами, информацией об авторах, с пристатейным библиографическим списком, предоставляется с одним комплектом рисунков

Внимание! Названия статьи, ФИО авторов, аннотация и ключевые слова обязательно представляются в соответствии с требованиями ВАК на русском и английском языках.

Информация о каждом авторе должна содержать следующие стандартные сведения:

- Фамилия, имя, отчество;
- Ученая степень, ученое звание, почетное звание;
- Членство в общественных союзах и т.д.;
- Место работы, должность;
- Перечень и номера журналов IDT Publishers, в которых ранее публиковались статьи автора;
- Сведения для контактов;
- Фотографии всех авторов статьи.

Текст необходимо набирать в редакторе Word 97-2003 шрифтом № 12; текст не форматируется. Абзацы организуются путем нажатия клавиши Enter. Текст статьи набирается через полтора интервала на странице формата A4; слева должно быть поле 2 см; страницы нумеруются, «красная строка» обязательна. Все буквенные обозначения, приведенные на рисунках, необходимо пояснять в основном или

подрисовочном тексте. Недопустимы отличия в обозначениях на рисунках и в тексте. Нумеровать следует только те формулы и уравнения, на которые есть ссылка в тексте.

Непосредственно в тексте набираются простые формулы (например, m^2 ; n^2t , $C = 1 + DDF - A_2$), греческие буквы и символы, например, β , $\otimes$ — шрифтом Symbol. То, что невозможно набрать непосредственно в текстовом редакторе, — с использованием редактора формул Microsoft Equation (входящего в комплект поставки Microsoft Office) или редактора формул MathType.

Не допускается представление текста, в котором формулы представлены в виде изображения.

Фотографии и рисунки к статьям предоставляются отдельными файлами с расширением TIF, или EPS или JPEG с разрешением не менее 300 dpi.

Список использованной литературы составляется в порядке цитирования и дается в конце статьи.

Ссылки на литературу в тексте отмечаются порядковыми цифрами в квадратных скобках.

Вниманию авторов, публикующихся в журналах IDT Publishers.

Представленная информация о каждом авторе помимо журнала будет размещаться на сайте techizdat.ru в разделе «Авторы» на отдельной интернет-странице.

Авторам также предоставляется возможность при публикации своих статей направить в редакцию свою электронную фотографию и дополнительные материалы для размещения их на этой индивидуальной Интернет-визитке. По своему усмотрению автор может рассказать более подробно о себе, об интересных примерах и историях решения технических проблем, о современных задачах - в соответствии с тематикой соответствующего журнала - и т.п. Желательный объем этого материала — не более 1000 знаков с пробелами.

ПОДПИСКА НА ЖУРНАЛ «НАДЕЖНОСТЬ»

Подписаться на журнал в 2015 году можно:

- Через агентство «Роспечать» — индекс 81733;

- По каталогу «Пресса России» агентства «Книга-Сервис» — индекс 11804;

- Через редакцию на любой срок
тел.: 8-916-105-81-31
e-mail: E.Patrikeeva@gismps.ru

REQUIREMENTS OF EDITION ON EXECUTION OF PAPERS IN JOURNALS OF PUBLISHING GROUP OF IDT PUBLISHERS

A letter from the organisation where the author (s) works or from the author (s) personally with the paper offered for publication should be sent to the de facto editorial office address: 107078, Moscow, 5 Orlikov lane, Office 755, LLC "JOURNAL DEPENDABILITY" or e-mail: E.Patrikeeva@gismips.ru (in scanned form). For journals of the publishing group of "IDT PUBLISHERS" the paper offered for publication should be sent to the address: 105005, Moscow, 15 Quay of Academician Tupolev, building 29, LLC "the publishing house Technology" or e-mail to: knstas@yahoo.com <mailto:knstas@yahoo.com> (in scanned form). The letter should be attached to a paper text containing the summary and keywords, information on authors, bibliographic list, and one complete set of figures. All listed items are to be presented in an electronic form (on CD or via the e-mail address provided above).

Attention! Titles of papers, names of authors, summary and keywords must be presented, in Russian and English languages, according to the requirements of the Higher Attestation Commission. The information on each author should contain the following standard data:

- Surname, name, patronymic;
- Scientific degree, academic status, honorary title;
- Membership of relevant public unions, etc.;
- Place of employment, position;
- The list and numbers of Journals of IDT Publishers in which papers of the author have been previously published;
- Contact information.

Texts should be presented in Word 97-2003 format in a 12-point typeface; the text should not be formatted. Paragraphs should be arranged by pressing the "return" key. The text of the paper should be double-spaced on pages of A4; on the left there should be a margin of 2 cm; pages should be numbered, the «first line indent» is obligatory.

All alphabetical designations represented in figures should be explained in the body text or in a legend. Inconsistencies between designations in figures and in the text are inadmissible. Numbering should only be applied to those formulas and equations that are referred to in the text.

Simple formulas appearing directly in the text (for example, m^2 , n^2t , $c = 1 + DDF - A_2$), and the Greek letters and symbols, for example, β , $\odot$ may be typed using the Symbol font. When it is not possible to type directly in the text editor, use the "Microsoft Equation" formula editor (available with the complete installation of Microsoft Office) or the "Mathtype" formula-editing program. Representation of formulae in the text in the form of images is not admissible. Photos and figures for papers should be provided in individual files with extension TIF, EPS or JPG with a resolution of not less than 300 dpi. The list of literature referred to in the paper (bibliography) is presented according to order of citation and provided at the end of paper. References to the literature in the text are marked by serial numerals in square brackets.

To authors that are published in journals of "IDT Publishers".

In addition to the journal, information on each author will be presented at the techizdat.ru site in the «Authors» section on the individual web page.

Authors of papers for publication have the opportunity to send an electronic photo and additional material to appear on this individualised Internet-business card. At their own discretion, authors can present more details about themselves, interesting examples and stories of solutions to technical problems, about contemporary problems according to subjects of corresponding journal, etc. This material should not exceed 1000 characters including spaces.

SUBSCRIPTION TO THE JOURNAL «DEPENDABILITY»

It is possible to subscribe to the journal for 2015:

- Through the agency «Rospechat»
– for the first half of the year: an index 81733;
- Under the catalogue "Press of Russia" of the agency «Books-services»:
– for half a year: an index 11804;
- Through the editorial office:
– for any time-frame
tel.: 8-916-105-81-31; e-mail: E.Patrikeeva@gismips.ru

ПЕРЕЧЕНЬ СТАТЕЙ, ОПУБЛИКОВАННЫХ В ЖУРНАЛЕ «НАДЕЖНОСТЬ» В 2014 ГОДУ

№ п/п	Название раздела, статьи	Авторы	№ журнала
Структурная надежность. Теория и практика			
1	Оценки характеристик надежности в предположении неполного восстановления	Чумаков И.А., Антонов А.В.	1
2	Математическая модель надежности комплекса «объект защиты – система безопасности» при нечеткой исходной информации	Перегуда А.И.	1
3	Обеспечение качества и анализ надежности информационно-измерительных систем на примере комплекса атлант	Никитаев В.Г., Проничев А.Н., Власов В.А., Власова С.В.	1
4	Анализ надежности сетей, состоящих из идентичных элементов	Ткачев О.А.	1
5	Резервирование как составная часть проблемы надежности в электроэнергетике	Федотова Г.А.	1
6	Исследование надежности систем автоматизации нефтеперерабатывающих производств на основе анализа единой базы проектных и эксплуатационных данных АСУТП	Пегушин С.Л., Шумихин А.Г.	2
7	Печатные платы. Физическая надежность межсоединений	Медведев А.М.	2
8	Исследование надежности автомобильных шин	Дамзен В.А., Елистратов С.В.	2
9	Математическая модель надежности изделия подверженно-го ударным нагрузкам	Перегуда А.И.	2
10	К вопросу точности задания информации при оптимизации предупредительных замен	Володарский В.А.	2
11	Имитационная модель надежностной структуры летательных аппаратов военного назначения и ее использование в задачах исследования процессов их послепродажного обслуживания	Хахулин Г.Ф., Титов Ю.П.	3
12	Управление процессом испытания оборудования на надежность	Русин А.Ю., Абдулхамед М.	3
13	Флуктуационный неразрушающий контроль твердых материалов	Якубович Б.И.	3
14	Повышение качества изделий из высокотвердой керамики для тяжелонагруженных пар трения	Душко О.В., Мышлинская И.Х.	3
15	Как нам определить что такое «надежность»	Нетес В.А., Тарасьев Ю.И., Шпер В.Л.	4
16	О показателях надежности типа средняя наработка	Викторова В.С., Степанянц А.С.	4
17	Анализ проектной надежности ответственных узлов арочного пролетного строения пешеходного путепровода на основе численных и имитационных методов	Майстренко И.Ю., Юсупов И.И., Зиннуров Т.А.	4

№ п/п	Название раздела, статьи	Авторы	№ журнала
18	Метод устранения взаимного пересечения оценок эзари-прошана в задачах анализа связности двухполюсных сетей	Носов М.В.	4
19	Применение тактики последовательных контрольных испытаний на надежность элементов АСУ ТП и автоматической противоаварийной защиты в условиях эксплуатации для ее учета при fmea-анализе	Пегушин С.Л., Шумихин А.Г.	4
Функциональная надежность. Теория и практика			
20	Методы обеспечения функциональной надежности программ	Шубинский И.Б.	4
21	Генетический алгоритм для оптимизации архитектуры бортового программного обеспечения	Терсков В.А., Шеенок Д.А., Карцан И.Н.	4
22	Обзор методов принятия решений при разработке сложных технических систем	Семенов С.С., Полтавский А.В., Маклаков В.В., Крянев А.В.	3
23	Систематический подход к защите программного обеспечения от сбоев аппаратуры	Шубинский И.Б., Шебе Х.	3
24	Систематизация критериев и значимых факторов для оценки подверженности сложных систем дестабилизирующим воздействиям	Абрамова Н.А., Макаренко Д.И.	2
25	Достоверность передачи ответственных сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования	Ададуров С.Е., Ададуров А.С., Мальцев Г.Н.	1
Функциональная безопасность. Теория и практика			
26	Оценка рисков, связанных с изломами боковых рам тележек грузовых вагонов	Ермаков А.О., Новожилов Е.О.	1
27	Модель и метод для определения подсистем, наиболее подверженных дестабилизирующим воздействиям, в иерархии составного объекта защиты	Абрамова Н.А., Макаренко Д.И., Телицына Т.А.	1
28	Некоторые положения отказобезопасности и кибербезопасности систем управления	Гапанович В.А., Розенберг Е.Н., Шубинский И.Б.	2
29	Выбор и определение функции безопасности при верификации микропроцессорных систем железнодорожной автоматики и телемеханики	Бочков К.А., Сивко Б.В.	2
30	Модель определения предельного состояния железнодорожной техники	Ермаков А.О.	3
31	Процесс принятия решений при создании сложных технических систем и задача выбора альтернатив	Семенов С.С., Полтавский А.В., Маклаков В.В.	4
Стандартизация			
32	Актуальные вопросы стандартизации терминологии в области надёжности	Нетес В.А., Тарасьев Ю.И., Шнер В.Л.	2
Хорошо забытое			
33	Метод последовательного анализа Н.О.Демидовича	Дзиркал Э.В.	3

LIST OF PAPERS PUBLISHED IN DEPENDABILITY JOURNAL IN 2014

Item No.	Section, paper title	Authors	Issue No.
Structural reliability. The theory and practice			
1	Assessment of reliability performance under the assumption of incomplete recovery	<i>Chumakov I.A., Antonov A.V.</i>	1
2	Mathematical model of dependability for a complex “facility of protection – safety system” in case of fuzzy initial information	<i>Pereguda A.I.</i>	1
3	Quality assurance and reliability analysis of information measuring systems exemplified by the system atlant	<i>Nikitaev V.G., Pronichev A.N., Vlasov V.A., Vlasova S.V.</i>	1
4	Reliability analysis of networks consisting of identical elements	<i>Tkachev O.A.</i>	1
5	Redundancy as part of the reliability problem in electric-power industry	<i>Fedotova G.A.</i>	1
6	Assessment of reliability, causes and consequences of failures of refinery automated systems based on application of a common designing and operational data base of industrial control systems	<i>Pegushin S.L., Shumikhin A.G.</i>	2
7	Printed circuit boards. Reliability of interconnections	<i>Medvedev A.M.</i>	2
8	Reliability study of car tires	<i>Damzen V.A., Yelistratov S.V.</i>	2
9	Mathematical model of the reliability of a product subject to impact stress	<i>Pereguda A.I.</i>	2
10	The issue of accuracy of information assignment for optimization of preventive replacements	<i>Volodarsky V.A.</i>	2
11	Simulation model of military aircraft dependable structure and its use in the research of after-sale service processes	<i>Khakhulin G.F., Titov Yu.P.</i>	2
12	Equipment dependability test management	<i>Rusin A.Yu., Abdulhameed M.</i>	2
13	Fluctuation nondestructive testing of solid materials	<i>Yakubovich B. I.</i>	2
14	Quality improvement of products made of highly rigid ceramics for heavy-loaded friction pairs	<i>Dushko O.V., Mishlinskaya I.H.</i>	2
15	How we should define what “dependability” is	<i>Netes V.A., Tarasyev J.I., Shper V.L.</i>	4
16	Dependability indices of mean time type	<i>Viktorova V.S., Stepanyants A.S.</i>	4
17	Analysis of design dependability of critical units of arch spans of pedestrian overpasses based on numerical and simulation methods	<i>Maystrenko I.Y., Zinnurov T.A., Yusupov I.I.</i>	4
18	Method for elimination of mutual crossing of esary-proschan estimates in tasks of analysis of bipolar networks connectivity	<i>Nosov M.B.</i>	4

Item No.	Section, paper title	Authors	Issue No.
19	Application of the tactics of dependability consecutive check tests of cam elements and automated sis under operating conditions for use of results in fmea analysis	<i>Pegushin S.L., Shumikhin A.G.</i>	4
Functional reliability. The theory and practice			
20	Methods of software functional dependability assurance	<i>Shubinsky I.B.</i>	4
21	Genetic algorithm for optimization of onboard software architecture	<i>Terskov V.A., Sheenok D.A., Kartsan I.N.</i>	4
22	Overview of decision-making techniques used in the development of complex engineering systems	<i>Semenov S.S., Poltavsky A.V., Krianev A.V., Maklakov V.V.</i>	3
23	A systematic approach to protection against glitches	<i>Shubinsky I.B., Schäbe H.</i>	3
24	Systematization of criteria and significant factors for evaluation of exposure of complex systems to disturbances	<i>Abramova N.A., Makarenko D.I.</i>	2
25	Accuracy of vital messages transmission using threshold fragmentation methods and antinoise coding	<i>Adadurov S.E., Adadurov A.S., Maltsev G.N.</i>	1
Functional safety. The theory and practice			
26	Model and method for definition of subsystems most exposed to disturbances as part of a complex facility of protection	<i>Abramova N.A., Makarenko D.I., Telitsyna T.A.</i>	1
27	Assesment of risks related to fractures and defects of side frames of freight car bogies	<i>Ermakov A.O., Novozhilov E.O.</i>	1
28	Some concepts of fail-safety and cyber security of control systems	<i>Gapanovich V.A., Rozenberg E.N., Shubinsky I.B.</i>	2
29	Selection and definition of safety function when verifying railway signalling and remote control computer-based systems	<i>Bochkov K.A., Sivko B.V.</i>	2
30	Identification of railway equipment's limit tolerance state	<i>Ermakov A.O.</i>	3
31	Process of decision-making in development of complex technical systems and the task of choice of alternatives	<i>Semenov S.S., Poltavsky A.V., Maklakov V.V.</i>	4
Standardization			
32	Current issues of terminology standardization in dependability	<i>Netes V.A., Tarasyev Y.I., Shper V.L.</i>	2
Well-forgotten old			
33	N.O. Demidovich's sequential control method	<i>Dzirkal E.V.</i>	3

ЗАЯВКА НА ПОДПИСКУ НА ЖУРНАЛ «НАДЕЖНОСТЬ»

с № _____ 20__ г. по № _____ 20__ г., количество экз. _____

Полное наименование организации	
Юридический адрес предприятия (индекс, страна, адрес)	
Почтовый адрес предприятия (индекс, страна, адрес)	
ИНН/КПП	
Расчетный счет	
Банк	
Корреспондентский счет	
БИК	
Контактное лицо: Ф.И.О., должность	
Телефон/факс, e-mail	

Реквизиты: ООО «Журнал «Надежность»

Адрес редакции: 109029, г. Москва, ул. Нижегородская, д.27, стр.1, оф. 209

Тел./факс: (495) 967-77-02 , e-mail: E.Patrikeeva@gismps.ru

ИНН 7709868505 КПП 770901001

р/с 40702810100430000017

к/с 30101810100000000787

Адрес доставки:

Кому: _____

Куда: _____

Для оформления подписки на журнал «Надежность» заполните заявку и отправьте ее по факсу или электронной почте.

По всем вопросам, связанным с подпиской, обращайтесь в редакцию журнала.

Стоимость годовой подписки 4180-00 руб, в т.ч. НДС 10%.

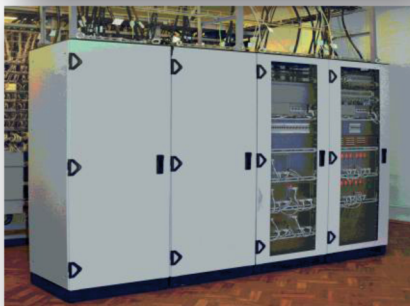
Периодичность – 4 номера в год.

ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ

ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ И ПРОЕКТНО-КОНСТРУКТОРСКИЙ ИНСТИТУТ ИНФОРМАТИЗАЦИИ, АВТОМАТИЗАЦИИ И СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ»
(ОАО «НИИАС»)



ОАО «НИИАС» – ведущее предприятие ОАО «РЖД» в области создания комплексов и систем обеспечения безопасности движения, управления движением, геоинформационного обеспечения, мониторинга состояния подвижного состава и инфраструктуры железных дорог



Цели:

- ☐ эффективность,
- ☐ безопасность
- ☐ надежность перевозок



Основные направления деятельности

- Интеллектуальные системы управления
- Технологии управления перевозками и транспортного обслуживания
- Системы автоматики и телемеханики
- Центры автоматизированного управления
- Информационные системы
- Геоинформационные системы и спутниковые технологии
- Системы транспортной безопасности
- Системы управления инфраструктурой
- Системы управления топливно-энергетическими ресурсами
- Испытания, сертификация и экспертиза
- Информационная безопасность
- Нормативно-правовое обеспечение



www.vniias.ru