НАДЕЖНОСТЬ

DEPENDABILITY

ISSN 1729-2646

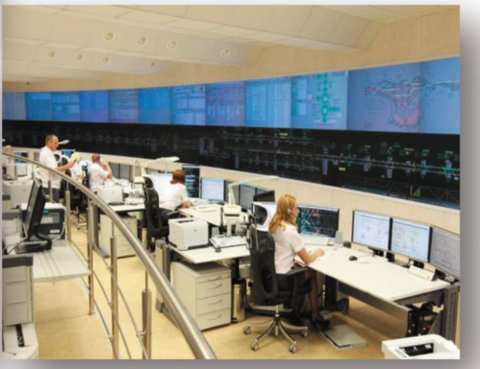
02 (49) 2014

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ / SCIENTIFIC-TECHNICAL JOURNAL

В НОМЕРЕ / IN THIS RELEASE:

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

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.

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.

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.

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.

СОДЕРЖАНИЕ/CONTENTS

Пегушин С.Л., Шумихин А.Г.

ИССЛЕДОВАНИЕ НАДЕЖНОСТИ СИСТЕМ АВТОМАТИЗАЦИИ НЕФТЕПЕРЕРАБАТЫВАЮЩИХ ПРОИЗВОДСТВ НА ОСНОВЕ АНАЛИЗА ЕДИНОЙ БАЗЫ ПРОЕКТНЫХ И ЭКСПЛУАТАЦИОННЫХ ДАННЫХ АСУТП

Надежность организационных и технических автоматизированных управляющих систем является важной составляющей их качества и необходимым условием обеспечения безопасности опасных производственных объектов нефтепереработки. Оценка надежности и ремонтопригодности автоматизированных систем управления предусмотрена национальными и международными стандартами и другими нормативными документами. Цель такой оценки – получение количественной информации о свойствах систем, необходимой для выработки и реализации обоснованных, эффективных проектных и эксплуатационных решений по обеспечению надежности и безопасности производственных объектов.

Формирование единой базы данных стадий жизненного цикла автоматизированных систем, в том числе проектных и эксплуатационных данных, например АСУТП, по отказам технических и программных средств дает возможность определить реальные показатели надежности состояния эксплуатируемого оборудования с учетом проектных решений и особенностей монтажа.

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

Расчет показателей надежности при эксплуатации оборудования ПАЗ следует вычислять по реальным статистическим данным.

К типовым отказам в период эксплуатации КТС ПАЗ можно отнести: отказ электроники, обрыв линии связи, метрологический отказ, заклинивание штока отсечной трубопроводной арматуры, потерю питания электрического и пневматического.

В таблице 1 приведены типовые виды причин отказов элементов системы ПАЗ, приводящие к их отказам в период эксплуатации.

Структурная модель обеспечения надежности АСУТП представлена на рис. 1.

Выражения для вычисления вероятностей отказа и безотказной работы для элементов, представленных в таблице 1, полученные на основе логических функций работоспособности (надежности), будут следующими:

Рис. 1. Структурная модель обеспечения надежности АСУТП

Таблица 1. Виды причин отказов элементов систем ПАЗ

Причины отказа / Элемент системы	Отказ электроники	Обрыв линии связи	Метрологический отказ	Заклинивание штока	Потеря электро- и пневмопитания
Датчик измерения	+	+	+		+
Барьер	+	+	+		+
Клапан	+	+	+	+	+
Модуль ввода/вывода	+	+	+		+
Контроллер	+	+	+		+
Блок питания	+				+

1. Для датчика:

$$Q_{датчик} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + \\ + q_2q_3q_4 - q_1q_2q_3q_4;$$

$$P_{датчик} = 1 - Q_{датчик} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - \\ - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

где q_1, q_2, q_3, q_4 – вероятности отказов электроники, линии связи, метрологического, отказа в результате потери питания соответственно, P – вероятность безотказной работы, Q – вероятность отказа.

2. Для барьера искрозащиты:

$$Q_{барьер} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + + q_2q_3q_4 - q_1q_2q_3q_4;$$

$$P_{барьер} = 1 - Q_{барьер} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

где q_1, q_2, q_3, q_4 - вероятности отказов электроники, линии связи, метрологического, отказа в результате потери питания соответственно, P – вероятность безотказной работы, Q – вероятность отказа.

3. Для отсечного клапана с электропневматическим позиционером:

$$Q_{клапан} = q_1 \vee q_2 \vee q_3 \vee q_4 \vee q_5 = q_1 + q_2 + q_3 + q_4 + q_5 - q_1q_2 - q_1q_3 - q_1q_4 - q_1q_5 - q_2q_3 - q_2q_4 - q_2q_5 - - q_3q_4 - q_3q_5 - q_4q_5 + q_1q_2q_3 + q_1q_2q_4 + q_1q_2q_5 + q_1q_3q_4 + q_1q_3q_5 + q_1q_4q_5 + q_2q_3q_4 + q_2q_3q_5 + q_2q_4q_5 + + q_3q_4q_5 - q_1q_2q_3q_4 - q_1q_2q_3q_5 - q_1q_2q_4q_5 + q_1q_2q_3q_4q_5;$$

$$P_{клапан} = 1 - Q_{клапан} = 1 - q_1 - q_2 - q_3 - q_4 - q_5 + q_1q_2 + q_1q_3 + q_1q_4 + q_1q_5 + q_2q_3 + q_2q_4 + q_2q_5 + + q_3q_4 + q_3q_5 + q_4q_5 - q_1q_2q_3 - q_1q_2q_4 - q_1q_2q_5 - q_1q_3q_4 - q_1q_3q_5 - q_1q_4q_5 - q_2q_3q_4 - q_2q_3q_5 - q_2q_4q_5 - - q_3q_4q_5 + q_1q_2q_3q_4 + q_1q_2q_3q_5 + q_1q_2q_4q_5 - q_1q_2q_3q_4q_5,$$

где q_1, q_2, q_3, q_4, q_5 - вероятности отказов электроники, линии связи, метрологического, отказа в результате потери питания, заклинивания штока соответственно, P – вероятность безотказной работы, Q – вероятность отказа.

4. Для модуля ввода/вывода:

$$Q_{I/O} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + + q_2q_3q_4 - q_1q_2q_3q_4;$$

$$P_{I/O} = 1 - Q_{I/O} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

где q_1, q_2, q_3, q_4 - вероятности отказов электроники, линии связи, метрологического, отказа в результате потери питания соответственно, P – вероятность безотказной работы, Q – вероятность отказа.

5. Для контроллера:

$$Q_{контроллер} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + + q_2q_3q_4 - q_1q_2q_3q_4;$$

$$P_{контроллер} = 1 - Q_{контроллер} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

где q_1, q_2, q_3, q_4 - вероятности отказов электроники, линии связи, метрологического, отказа в результате потери питания соответственно, P – вероятность безотказной работы, Q – вероятность отказа.

6. Для блока питания:

$$Q_{питание} = q_1 + q_2 - q_1q_2;$$

$$P_{питание} = 1 - Q_{питание} = 1 - q_1 - q_2 + q_1q_2,$$

где q_1, q_2 – вероятности отказов электроники, отказа в результате потери питания соответственно, P – вероятность безотказной работы, Q – вероятность отказа.

Для оценки надежности по статистическим данным относительная частота отказов за каждый месяц определяется по следующей формуле [1]:

$$q_i = \frac{n_i}{N},$$

где n_i – количество отказавших элементов по *i*–му виду отказов, N – общее количество эксплуатируемых на установке элементов.

Вероятность отказа элементов за год можно оценить на основе следующей формулы для интенсивности отказов:

$$\lambda_i = \frac{N_1 - N_2}{N_{ср}\Delta t},$$

где N_1 – количество работающих элементов в момент времени t_1, N_2 – количество работающих элементов в момент времени t_2, $\Delta t = t_1 - t_2$, $N_{ср}$ – среднее количество работающих элементов, i – индекс, соответствующий типу элемента.

Вычисленная интенсивность отказов позволяет вместе с интенсивностью восстановлений планировать техническое обслуживание автоматических систем ПАЗ [2].

Вероятность отказа всех элементов КТС можно найти по формуле полной вероятности:

$$Q(A) = \sum_{K=1}^{N} Q(H_K) \cdot Q(A \mid H_K),$$

где $H_1, H_2, ..., H_K$ – полная группа гипотез, $Q(H)$ – вероятность отказа элемента КТС (гипотезы). Следовательно, если система включает в себя датчик измерения, барьер искрозащиты, клапан мо-

дуль ввода/вывода, контроллер, блок питания, то формула полной вероятности при условии того, что все элементы могут отказать равновероятно, будет иметь вид:

$$Q = \frac{1}{6} \cdot Q_{датчик} + \frac{1}{6} \cdot Q_{барьер} + \frac{1}{6} \cdot Q_{клапан} + \frac{1}{6} \cdot Q_{I/O} + \frac{1}{6} \cdot Q_{контроллер} + \frac{1}{6} \cdot Q_{питание};$$

Вероятность безотказной работы в этом случае равна $P = 1 - Q$.

В таблице 2 в качестве примера применения единой базы данных АСУТП представлен фрагмент расчета надежности системы ПАЗ установки 37-10 нефтеперерабатывающего производства за 12 месяцев 2010 г. с использованием данных по отказам оборудования системы.

Таблица 2. Расчет показателей надежности системы ПАЗ

Наименование оборудования	**Общее количество оборудования N**	**Количество отказавшего оборудования n**	**Относительная частота (вероятность) отказов**	**Относительная частота (вероятность) безотказной работы**	**Интенсивность потока отказов**	**Относительная частота (вероятность) отказов в системе ПАЗ**	**Относительная частота (вероятность) безотказной работы системы ПАЗ**	**Интенсивность потока отказов системы ПАЗ**
Датчики измерения давления	14	0	0	1	0	0	1	0
Датчики измерения расхода	2	0	0	1	0			
…								
Запорно-регулирующие клапаны и отсекатели	8	0	0	1	0			

Из данных таблицы 2 следует, что отказы системы ПАЗ в течение месяца отсутствуют, что можно объяснить достаточностью технического обслуживания.

Для формирования рекомендаций и норм по обслуживанию систем автоматизации можно воспользоваться методологией FMEA (анализ причин и последствий отказов). На основе таблиц FMEA оцениваются рейтинги частот возникновения отказов и их обнаружения, разрабатываются нормы по обслуживанию систем автоматизации, позволяющие повысить их надежность.

В качестве примера в таблицах 3 и 4 приведены результаты определения по методологии FMEA рейтингов частоты возникновения отказов и вероятностей их обнаружения для системы ПАЗ печи подогрева экстрактного раствора установки селективной очистки масел 37-10.

Таблица 3. Рейтинг частоты возникновения отказов

Рейтинг	Частота возникновения	Интервал между отказами, час.	Критерий
10	Почти всегда	Менее 2	
9	Очень высокая	2 – 10	
8	Высокая	11 – 100	Простой более 8 час.
7	Достаточно высокая	101 – 400	Простой более 4 час.
6	Средняя вероятность	401 – 1000	Простой 1 – 4 час.
5	Низкая вероятность	1001 – 2000	Простой 0,5 – 1 час.
4	Редко	2001 – 3000	Простой менее 30 мин. Без потери продукции
3	Очень редко	2001 – 3000	Процесс требует регулирования
2	Единичные случаи	3001 – 6000	Процесс находится под контролем, но требуется некоторая регулировка
1	Почти никогда не возникают	6001 – 10000	Процесс находится под контролем

Таблица 4. Рейтинг вероятности обнаружения отказов

Рейтинг	Вероятность обнаружения	Критерий
10	Практически не обнаруживается	Планово-предупредительное обслуживание (ППО) не позволяет выявить потенциальные причины отказа
9	Очень редко обнаруживается	Ничтожны шансы, что ППО позволит выявить причины отказа
8	Редко обнаруживается	Чрезвычайно малы шансы обнаружения при ППО причин отказа
7	Очень малая вероятность	Очень малы шансы обнаружения отказа при ППО
6	Малая вероятность	Малы шансы обнаружения отказа при ППО
5	Умеренная вероятность	Умеренные шансы обнаружения отказа при ППО
4	Средняя вероятность	Средние шансы обнаружения отказа при ППО
3	Высокая вероятность	Большие шансы обнаружения отказа при ППО
2	Очень высокая вероятность	Очень большие шансы обнаружения отказа при ППО
1	Практически всегда обнаруживается отказ	ППО позволяет практически всегда выявить потенциальные причины отказа

Таким образом, в статье показана целесообразность создания единой базы проектных и эксплуатационных данных по отказам технических средств систем управления и применения ее для анализа причин и последствий отказов и выработки мероприятий по их предупреждению.

Литература

1. **Острейковский В.А.** Теория надежности. – М.: Высшая школа, 2003 – 463 с.

2. Планирование технического обслуживания автоматических систем противоаварийной защиты производственных объектов с учетом оценки надежности и ремонтопригодности. Пегушин С.Л., Шумихин А.Г. Вестник Пермского национального исследовательского политехнического университета. Химическая технология и биотехнология. 2012. № 14. С. 13-21.

Pegushin S.L., Shumikhin A.G.

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

The reliability of management and technical control systems is an important constituent of their quality and indispensable condition of safety ensurance of hazardous production facilities of oil refining. Assessment of reliability and maintainability of automated control systems are provided for by national and international standards and other regulations. The purpose of this assessment is to obtain quantitative information about the properties of systems required to develop and implement well-grounded, effective design and operational decisions to ensure the dependability and safety of industrial facilities.
Construction of a common database of life cycle stages of automated control systems, including design and operational data, e.g. of ICS, as regards hardware and software failures, allows us to define real dependability indices of equipment in operation in view of design solutions and installation peculiarities.

Keywords: *oil refining, production process, automated control system, reliability, causes and consequences of failures, analysis.*

Reliability parameters in operation of safety instrumented systems (SIS) for refineries should be computed using actual statistics.

Typical failures during the operation of SIS technical facilities include failures of electronics, communication line breaks, metrological failure, jamming of rods of cutoff pipeline accessories, loss of electrical and pneumatic power supply.

Table 1 shows typical kinds of failure causes of SIS components leading to their failures during operation.

The structural model of ensuring the reliability of ICS is shown in Fig. 1.

Expressions for calculating the probabilities of failure and failure-free operation for the components presented in Table 1, obtained on the basis of logical functions of availability (reliability), are as follows:

1. For measuring sensor:

$$Q_{sensor} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + \\ + q_2q_3q_4 - q_1q_2q_3q_4;$$

$$P_{sensor} = 1 - Q_{sensor} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

where q_1, q_2, q_3, q_4 are probabilities of failures of electronics, communication lines, metrology, and failure as a result of power loss, respectively, P is the probability of failure-free operation, Q is the probability of failure.

2. For spark protection barrier:

$$Q_{barrier} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + q_2q_3q_4 - q_1q_2q_3q_4;$$

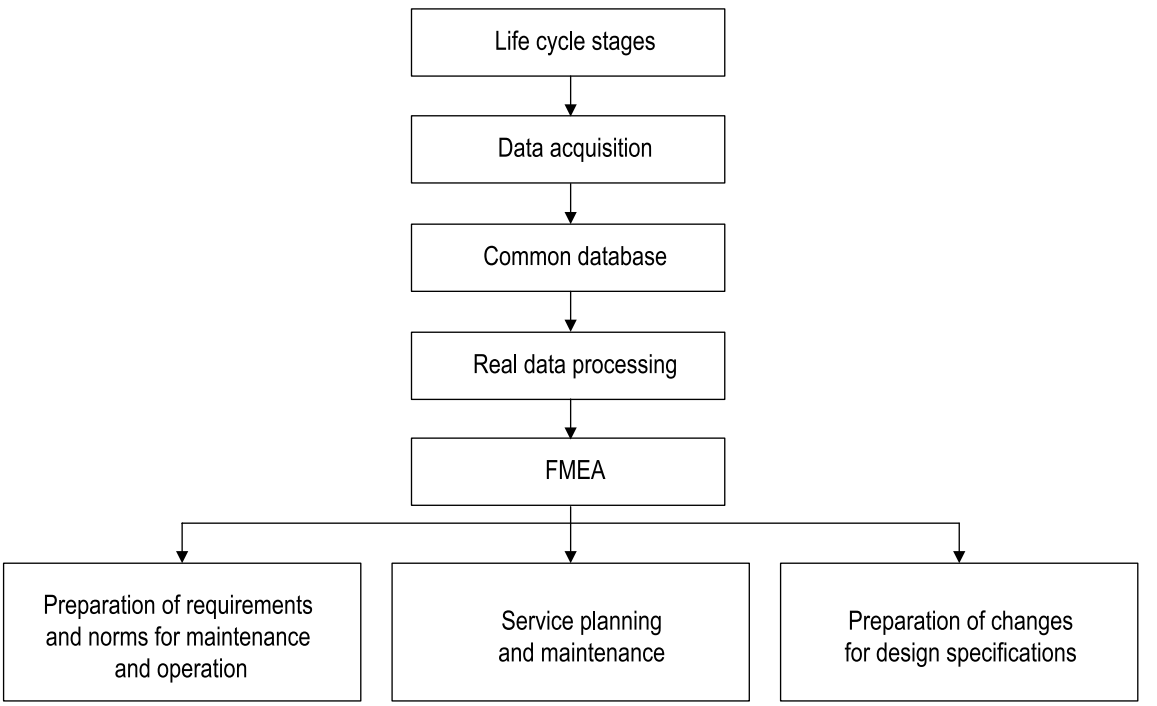


Fig. 1. The structural model of ensuring the reliability of ICS

Table 1. Types of SIS components' failure causes

Failure causes / System component	Electronics failure	Communication line break	Metrological failure	Rod jamming	Loss of electric and pneumatic power
Measuring sensor	+	+	+		+
Barrier	+	+	+		+
Valve	+	+	+	+	+
Input/output unit	+	+	+		+
Controller	+	+	+		+
Power supply unit	+				+

$$P_{barrier} = 1 - Q_{barrier} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

where q_1, q_2, q_3, q_4 are probabilities of failures of electronics, communication lines, metrology, and failure as a result of power loss, respectively, P is the probability of failure-free operation, Q is the probability of failure.

3. For cutoff valve with electro-pneumatic positioner:

$$Q_{valve} = q_1 \vee q_2 \vee q_3 \vee q_4 \vee q_5 = q_1 + q_2 + q_3 + q_4 + q_5 - q_1q_2 - q_1q_3 - q_1q_4 - q_1q_5 - q_2q_3 - q_2q_4 - q_2q_5 - q_3q_4 - q_3q_5 - q_4q_5 + q_1q_2q_3 + q_1q_2q_4 + q_1q_2q_5 + q_1q_3q_4 + q_1q_3q_5 + q_1q_4q_5 + q_2q_3q_4 + q_2q_3q_5 + q_2q_4q_5 + q_3q_4q_5 - q_1q_2q_3q_4 - q_1q_2q_3q_5 - q_1q_2q_4q_5 + q_1q_2q_3q_4q_5,$$

where q_1, q_2, q_3, q_4, q_5 are probabilities of failures of electronics, communication lines, metrology, and failure as a result of power loss and rod jamming, respectively, P is the probability of failure-free operation, Q is the probability of failure.

4. For I/O unit:

$$Q_{I/O} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + q_2q_3q_4 - q_1q_2q_3q_4;$$

$$P_{I/O} = 1 - Q_{I/O} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

where q_1, q_2, q_3, q_4 are probabilities of failures of electronics, communication lines, metrology, and failure as a result of power loss, respectively, P is the probability of failure-free operation, Q is the probability of failure.

5. For controller:

$$Q_{controller} = q_1 + q_2 + q_3 + q_4 - q_1q_2 - q_1q_3 - q_1q_4 - q_2q_3 - q_2q_4 - q_3q_4 + q_1q_2q_3 + q_1q_2q_4 + q_1q_3q_4 + q_2q_3q_4 - q_1q_2q_3q_4;$$

$$P_{controller} = 1 - Q_{controller} = 1 - q_1 - q_2 - q_3 - q_4 + q_1q_2 + q_1q_3 + q_1q_4 + q_2q_3 + q_2q_4 + q_3q_4 - q_1q_2q_3 - q_1q_2q_4 - q_1q_3q_4 - q_2q_3q_4 + q_1q_2q_3q_4,$$

where q_1, q_2, q_3, q_4 q_4 are probabilities of failures of electronics, communication lines, metrology, and failure as a result of power loss, respectively, P is the probability of failure-free operation, Q is the probability of failure.

6. For power supply unit:

$$Q_{power} = q_1 + q_2 - q_1 q_2;$$

$$P_{power} = 1 - Q_{power} = 1 - q_1 - q_2 + q_1 q_2,$$

where q_1, q_2 are probabilities of failures of electronics, and failure as a result of power loss, respectively, P is the probability of failure-free operation, Q is the probability of failure.

For reliability assessment by using statistical data, the relative failure rate per month is determined by the following formula [1]:

$$q_i = \frac{n_i}{N},$$

where n_i is the number of failed components due to the i-th type of failures, N is the total number of operating components of the installation.

The probability of components' failure per year can be estimated based on the following formula for a failure rate:

$$\lambda_i = \frac{N_1 - N_2}{N_{cp}\Delta t},$$

where N_1 is the number of components operating at the time point t_1, N_2 is the number of components operating at the time point t_2, $\Delta t = t_1 - t_2$, N_{cp} is the average number of operating components, i is the index corresponding to the component type.

The calculated failure rate allows together with the recovery rate planning maintenance of SIS automated systems [2].

The probability of failure of all the components of technical equipment can be determined by the formula of a total probability:

$$Q(A) = \sum_{K=1}^{N} Q(H_K) \cdot Q(A \mid H_K),$$

where $H_1, H_2, ..., H_K$ are the complete set of hypotheses, $Q(H)$ is the probability of technical equipment component failure (hypotheses). Therefore, if the system includes a measuring sensor, spark protection barrier, valve, I/O unit, controller, power supply unit, then the total probability formula, provided that all components may fail with an equal probability, will have the following form:

$$Q = \frac{1}{6} \cdot Q_{transducer} + \frac{1}{6} \cdot Q_{barrier} + \frac{1}{6} \cdot Q_{valve} + \frac{1}{6} \cdot Q_{I/O} + \frac{1}{6} \cdot Q_{controller} + \frac{1}{6} \cdot Q_{power\ sup\ ply};$$

In this case, the probability of failure-free operation is equal to $P = 1 - Q$.

Table 2, as an example of the application of ICS common database, shows a fragment of calculation of the reliability of SIS 37-10 installation system of oil refining per 12 months in 2010, using data from equipment failures of the system.

Table 2. Calculation of SIS reliability indices

Name of equipment	Total number of equipment, N	Number of failed equipment, n	Relative density (probability) of failure	Relative density (probability) of failure-free operation	Failure rate	Relative density (probability) of failures in SIS	Relative density probability) of failure-free operation of SIS	Failure rate of SIS
Pressure measuring sensors	14	0	0	1	0	0	1	0
Flow measuring sensors	2	0	0	1	0			
…								
Shutdown valves and cutoff devices	8	0	0	1	0			

The data in Table 2 show that SIS failures during a month are unavailable, which can be explained by sufficiency of maintenance.

To develop recommendations and standards for maintenance of automation systems, it is possible to apply the methodology of FMEA (failure mode and effect analysis). Table-based FMEA is applied for assessment of ratings of failure frequencies and their detection, as well as for development of regulations for maintenance of automation systems that enhance their dependability.

As an example, Table 3 and Table 4 show the results of FMEA application for construction of ratings of failure frequency and the probability of failure detection for SIS of a furnace for heating of extractive solution of the 37-10 installation for selective oil cleaning.

Table 3. Rating of failure frequency

Rating	Frequency of occurrence	Interval between failures, hour	Criterion
10	Almost always	Under 2	
9	Very high	2 – 10	
8	High	11 – 100	Downtime is over 8 h.
7	Sufficiently high	101 – 400	Downtime is over 4 h.
6	Average probability	401 – 1000	Downtime is 1 – 4 h.
5	Low probability	1001 – 2000	Downtime is 0,5 – 1 h.
4	Rare	2001 – 3000	Downtime is under 30 min. Without product loss
3	Very rare	2001 – 3000	The process needs to be adjusted
2	Single instances	3001 – 6000	The process is under control, but needs some adjustment
1	Almost never occur	6001 – 10000	The process is under control

Table 4. Rating of the probability of failure detection

Rating	The probability of detecting	Criterion
10	Virtually undetectable	Preventive maintenance (PM) does not allow detecting potential causes of failures
9	Detected very rarely	Negligible chances that PM will allow detecting potential causes of failures
8	Detected rarely	Extremely small chances of failure cause detection when carrying out PM
7	Very small probability	Very small chances of failure cause detection when carrying out PM
6	Small probability	Small chances of failure detection when carrying out PM
5	Moderate probability	Moderate chances of failure detection when carrying out PM
4	Average probability	Average chances of failure detection when carrying out PM
3	High probability	High chances of failure detection when carrying out PM
2	Very high probability	Very high chances of failure detection when carrying out PM
1	Failure is practically always detected	PM allows practically always detecting potential causes of failure

Thus, the paper shows the expedience of building up a common database of design and operational data as regards failures of control systems' equipment and its application for the analysis of failure cause and consequences and the development of measures to prevent them.

References

1. **Ostreikovsky V.A.** The theory of reliability. – Moscow: Higher School, 2003 – 463 p.

2. **Pegushin S.L., Shumikhin A.G.** Maintenance planning of SIS automatic systems of production facilities in view of assessment of reliability and maintainability. Bulletin of the Perm National Research Polytechnic University. Chemical Technology and Biotechnology. , 2012.# 14. pp. 13-21.

Медведев А.М.

ПЕЧАТНЫЕ ПЛАТЫ. ФИЗИЧЕСКАЯ НАДЕЖНОСТЬ МЕЖСОЕДИНЕНИЙ

Устойчивость металлизации отверстий к термомеханическим напряжениям обеспечивается прочностью и пластичностью гальванически осаждаемой меди.
Различия в коэффициентах теплового расширения меди и диэлектрика оснований печатных плат создают мощные термомеханические факторы разрыва металлизации отверстий, разрушения внутренних межсоединений в многослойных структурах печатных плат. Стандартные нормы требований к толщине металлизации отверстий, ее прочности и пластичности меди, установились в процессе производства ординарных печатных плат применительно к использованию традиционных технологий пайки оловянно-свинцовыми припоями. Возврат к рассмотрению проблемы пластичности меди обусловлен в первую очередь переходом на бессвинцовые припои, которые отличаются высокой температурой пайки, инициированным общеевропейской директивой RoHS [1]. Более высокие температуры создают большие деформации металлизации отверстий, что заставляет пересмотреть требования к пластичности меди. Вместе с тем, повсеместно наблюдается тенденция к уменьшению диаметра металлизированных отверстий, а значит и уменьшению площади поперечного сечения металлизации. Меньшие сечения имеют меньшее сопротивление разрыву. Поэтому наряду с хорошей пластичностью, металлизация отверстий печатных плат должна обеспечивать и более высокую прочность на разрыв. В связи с этим была исследована деформация металлизации отверстий при нагреве до температур пайки. Цель исследований – пересмотр норм на пластичность меди в отверстиях печатных плат. Показано, что пластичность медных осаждений в отверстиях современных печатных плат не должна быть менее 6% [2]. Современные электролиты меднения позволяют получить пластичность меди 12-18% [3].

Ключевые слова: *печатные платы, межсоединения, пластичность меди.*

Существо проблемы

Элементы межсоединений подвергаются воздействию термических нагрузок в процессе изготовления, монтажа и циклических изменений температур в процессе эксплуатации аппаратуры. Различия в температурных коэффициентах линейного расширения (ТКЛР) проводящих структур и диэлектрика вызывают в элементах электрических соединений термомеханические напряжения различной интенсивности. В продольных исправлениях, армированных стеклотканью, различия в ТКЛР настолько незначительны, что они не сказываются на прочности соединений продольной структуры.

В трансверсальном направлении, перпендикулярном плоскости армирования, различия в линейном расширении настолько значительны ($17 \cdot 10^{-6}$ для меди и $(100...400) \cdot 10^{-6}$ для диэлектрического основания), что возникающие при температурных нагрузках термомеханические напряжения способны разрушить межслойные соединения.

Известно, что устойчивость металлизированных отверстий к термомеханическим нагрузкам обеспечивается толщиной и пластичностью металлизации. Стандартные нормы требований к металлизации по этим критериям качества установились в процессе многолетней практики изготовления и эксплуатации электронной аппаратуры с печатным монтажом с отношением толщины платы к диаметру отверстия от *1:1* до *3:1*. При размере сквозных отверстий менее 0,3 мм это отношение может достигать соотношений *10:1...20:1*. В таких конструкциях многослойных печатных плат (МПП) отношение жесткостей сечений металлизации отверстий и окружающего их материала основания платы складывается не в пользу металлизации: в условиях температурных воздействий значительно увеличивается деформация металлизации отверстий (рис. 1). Это явление усугубляется уменьшением пластичности медной металлизации с ростом температуры пайки.

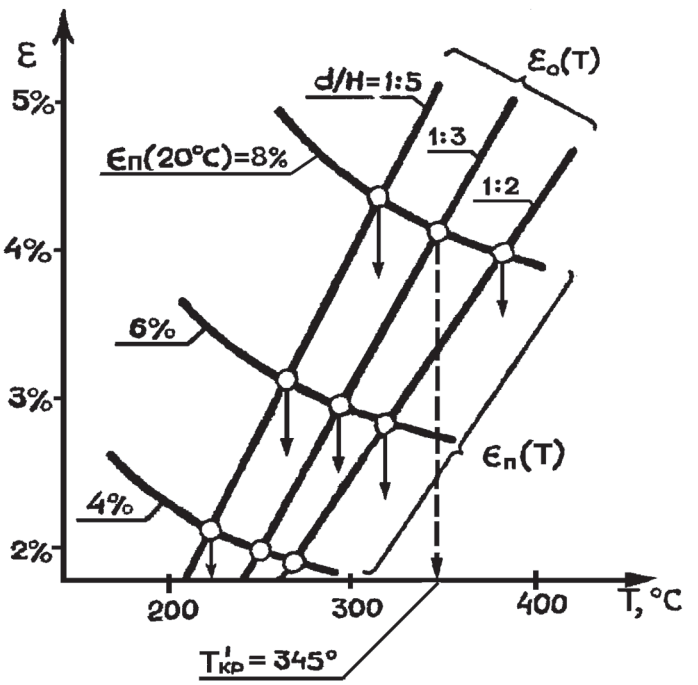


Рис. 1. Ужесточение требований к пластичности металлизации по мере уменьшения диаметра сквозного отверстия

Статистика показывает, что особенно большой поток отказов межслойных соединений наблюдается в аппаратуре, систематически подвергающейся воздействию циклических изменений температур (термоциклов). По данным длительной эксплуатации одного из авиационных комплексов отказы печатного монтажа распределяются следующим образом: металлизированные отверстия – 24 %, внутренние соединения – 72 %, печатные проводники внутренних слоев – 0,1%, изоляция – 2 %, пайки – 2,5 %, обрывы проводов – 0,3 %, остальное – 0,6 %. Сопоставления количества отказов МПП в стационарной аппаратуре, эксплуатирующейся в условиях относительного постоянства температур, и самолетной, показывают разницу почти в три порядка, что убеждает нас в том, что, если уровень переменных термомеханических напряжений превосходит определенный предел, идет процесс постепенного накопления повреждений, который завершается усталостными разрушениями соединений.

Модель термомеханических нагружений

Термомеханические напряжения при нагреве приводят к растяжению металлизации вдоль оси отверстия (осевые напряжения) и изгибу контактных площадок, наибольшая концентрация которого сосредотачивается на стыке с металлическим цилиндром отверстия (напряжение изгиба). Типичное искажение формы отверстия при нагреве схематично показано на рис. 2 и на фотографии микрошлифа – рис. 3.

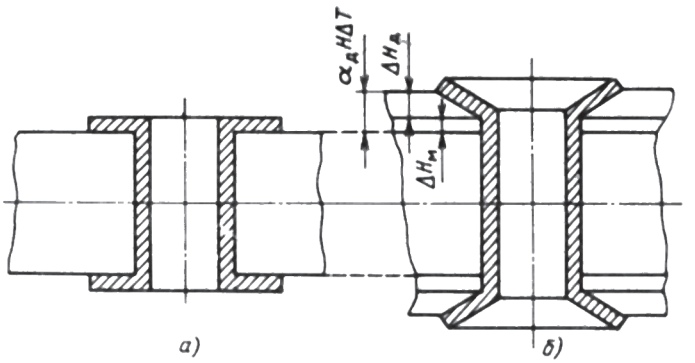


Рис. 2. Искажение формы металлизированного отверстия при нагреве

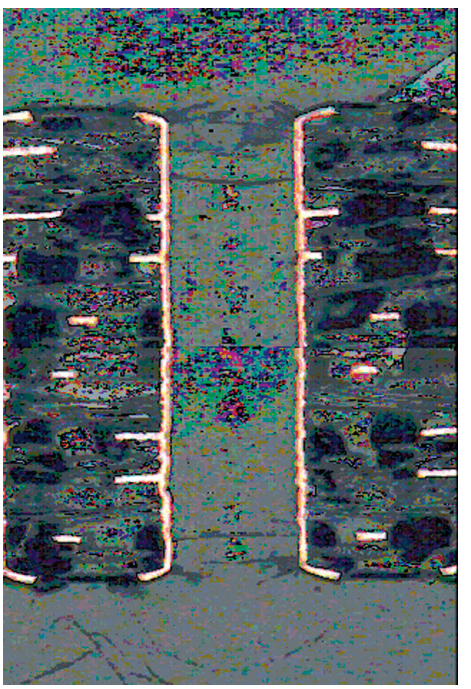


Рис. 3. Микрошлиф металлизированного отверстия после термоудара

В общем случае относительная деформация σ_Z металлизации при температурных воздействиях может быть представлена как сумма упругой ε_Y и температурной ε_T деформаций. Упругая деформация $\varepsilon_Y = \sigma E$ (E – модуль упругости). Температурная деформация $\varepsilon_T = \alpha(T\text{-}T_0)$. Отсюда термомеханические напряжения $\sigma = E[(\sigma_Z - \alpha(T\text{-}T_0)]$. Термомеханические усилия в каждом из элементов металлизированного отверстия:

$$F = E[(\sigma_Z - \alpha(T\text{-}T_0)]\, h\, dZ.$$

Для определения термомеханических характеристик деформации металлизации запишем уравнение равновесия из условия, что сумма всех термомеханических усилий, возникающих в компонентах системы «металлизация – стенки отверстия», должна быть равна нулю (рис. 4):

$$\int_0^{h_M} E_M[(\varepsilon_Z - \alpha_M(T - T_0)]hdZ + \int_{h_Д}^{0} E_Д[(\varepsilon_Z - \alpha_Д(T - T_0)]hdZ = 0$$

После интегрирования и преобразования можно показать, что деформация меди в трансверсальном направлении Z равна:

$$\varepsilon_Z = (\alpha_Д - \alpha_M)\,(T - T_0)\,(1 + J_M/J_Д)^{-1}, \qquad (1)$$

где $\alpha_Д$ и α_M ТКЛР, J_M и $J_Д$ – условные жесткости меди и диэлектрика.

Если ε_Z превышает предел пластичности медного осадка в отверстии (или $\sigma_P > \sigma_{ПЧ}$), происходит кольцевой разрыв металлизации.

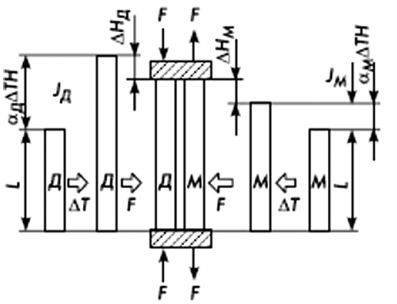


Рис. 4. Модель осевых термомеханических напряжений

Если силы сцепления металлизации со станками отверстия малы, напряжения сдвига могут реализоваться в разрыве внутреннего соединения. Напряжение сдвига, очевидно, должно увеличиваться по мере увеличения расстояния стыка от нейтральной оси *0--0* (рис. 5). Расстояние сдвига, если бы он произошел, можно определить, исходя из общих представлений. Но если силы сцепления удерживают металлизацию на стыках отверстия, то развивающееся при повышении температуры напряжение сдвига равно $\sigma_{Сдв} = G(\alpha_Д - \alpha_M)\Delta T$. Значение разрушающего напряжения сдвига определяют исходя из экспериментальных значений усилия вырыва металлизации из отверстия. На рис. 6 показана фотография разрушения внутреннего соединения в результате сдвига металлизации относительно стенок отверстия.

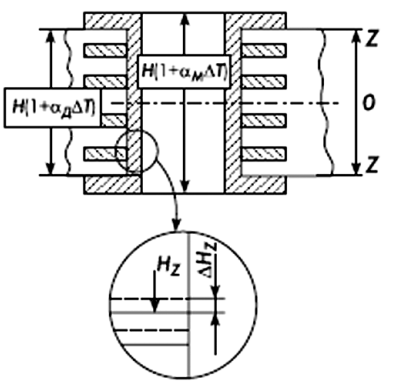


Рис. 5. Сдвиг металлизации с торцов контактных площадок внутренних слоев

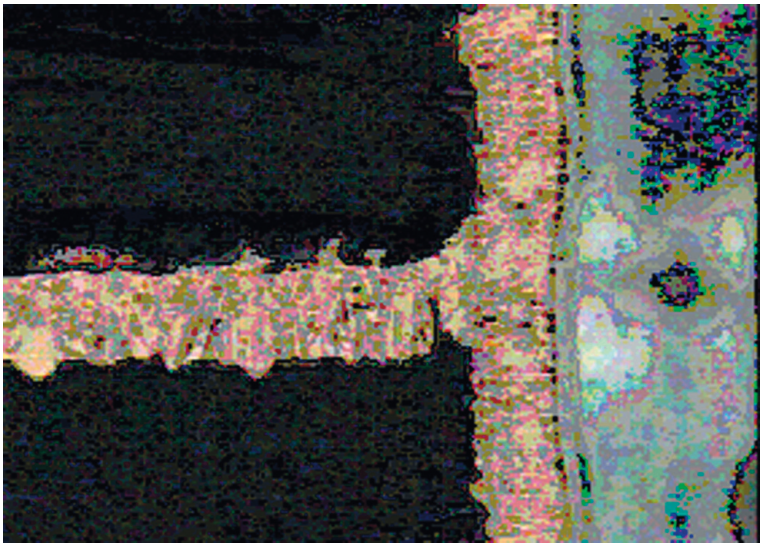


Рис. 6. Фотография микрошлифа разрушенного внутреннего соединения

На рис. 7 показана диаграмма температурной деформации свободно расширяющихся цилиндров меди, полимерных композиционных диэлектриков и результирующей температурной деформации их совокупности, а на рис. 8 – диаграмма деформация – напряжение. Кривая температурного расширения диэлектрического основания имеет перелом на температуре стеклования *Tg*. Зона упругой деформации меди ограничена значением ε_y.

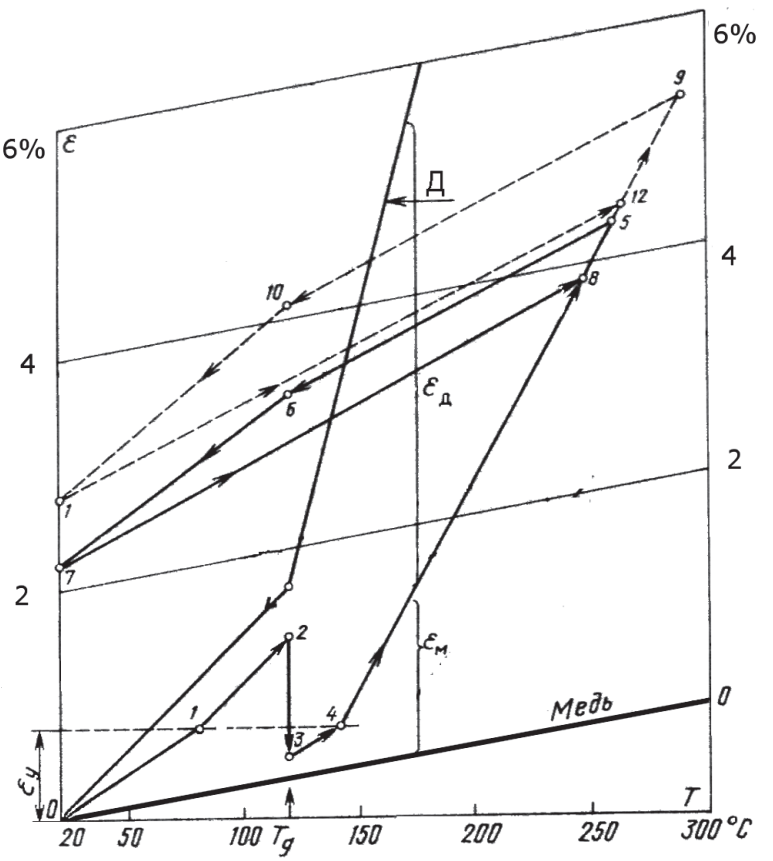


Рис. 7. Диаграмма температурной деформации металлизации отверстия, полученная графоаналитическим методом

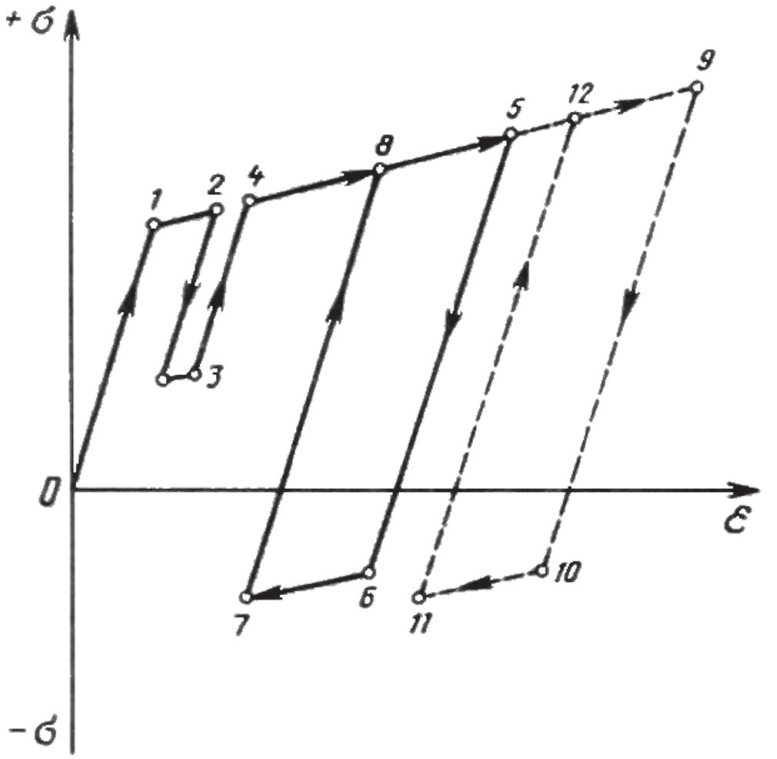


Рис. 8. Диаграмма деформация-напряжение

На участке *0-1* модуль сдвига меди соответствует участку упругости, т.е. имеет значение G_M, модуль сдвига диэлектрика равен $G_Д$. Распределение деформаций диэлектрика и меди подчиняется соотношению: $\alpha_Д/\alpha_M = G_M S_M / G_Д S_Д$, где S_M и $S_Д$ – площади поперечного сечения нагружения медного цилиндра и диэлектрика вокруг него, воспринимавшего нагрузку. Когда в точке *1* деформация меди переходит на участок текучести (участок *1-2*), ее модуль уменьшается, поэтому металлизация отверстия деформируется почти вслед за свободным расширением диэлектрика. При температуре стеклования *Tg* диэлектрическое основание теряет свою жесткость, за счет этого медный цилиндр разгружается. Его деформация принимает значение, соответствующее точке *3*. При переходе за температуру стеклования *Tg* диэлектрик начинает интенсивно расширяться. Однако на начальном этапе это не приводит к большому расширению меди, пока ее деформация не выходит за пределы упругости (участок *3-4*). Соотношение деформаций диэлектрика и меди на этом участке:

$$\alpha_Д/\alpha_M = G_M' S_M / G_Д' S_Д. \quad (2)$$

Кривые *5-6-7-8-5* и *9-10-11-12-9* демонстрируют изменения линейных размеров металлизированного отверстия при охлаждении и повторном цикле нагрев–охлаждение для температур пайки 260°С и 290°С соответственно. Наличие гистерезиса в температурной диаграмме деформаций свидетельствует о наличии определенной доли пластической деформации меди – предвестницы усталостных разрушений при циклических температурных нагрузках.

Методика экспериментальных исследований

Известны основные принципы исследований напряжений в металлизации сквозных отверстий на основе использования микрометрических датчиков перемещений, регистрирующих приращение толщины диэлектрического основания и металлического цилиндра сквозного отверстия по мере

нагрева МПП. Повышение точности измерений в широком температурном диапазоне обеспечивается использованием кварцевых держателей образцов и стержней передачи перемещений. Были попытки использования накладных тензометрических микродатчиков для измерения малых удлинений (экстензометров) для исследования деформации металлизации сквозных отверстий во время пайки. Сопоставление результатов измерения температурных расширений этими двумя методами, полученными разными авторами, демонстрирует их неоднозначность из-за неопределенности баз отсчета в первом случае и слабой чувствительности тензометрии для малоразмерных образцов, к каким относятся отверстия МПП – во втором случае.

Автор воспользовался собственной методикой исследования термомеханических напряжений, по которой само исследуемое металлизированное отверстие используется в качестве тензодатчика для измерения его температурных деформаций. Для этого он исходил из следующих предпосылок. Связь изменения омического сопротивления с деформацией: $\Delta R/R = k\varepsilon$, где k – тензочувствительность элемента (в данном случае – самого металлизированного отверстия). Поскольку $R = \rho H/S$, дифференциальная форма выражения $\Delta R/R$ имеет вид $dR/R = d\rho/\rho + dH/H - dS/S$, где ρ – удельное электрическое сопротивление металлизации, H – толщина платы (длина металлизированного цилиндра сквозного отверстия), S – площадь поперечного сечения металлизации отверстия в перпендикулярном направлении относительно его оси. При малом относительном удлинении $d\varepsilon = dH/H$ относительное изменение площади сечения $dS/S = -2\mu(dH/H)$. Поэтому $dR/R = d\rho/\rho + \varepsilon + 2\varepsilon\mu$, где μ – коэффициент Пуассона. Тогда тензочувствительность элемента – металлизации отверстия:

$$k = (dR/R)\,\varepsilon^{-1} = (1 + 2\mu) + (d\rho/\rho)^{-1}. \quad (3)$$

Выражение (3) состоит из двух частей: геометрической части, зависящей от ρ и отображающей изменение электрического сопротивления только за счет изменения размеров металлического цилиндра вследствие его продольной деформации, и физической части, связанной с изменением удельного сопротивления металлизации при удлинении $d\rho/\rho = B\,dV/V$ и отражающей линейную зависимость между изменением удельного сопротивления и относительным изменением объема dV/V, B – коэффициент Бриджмена. В случае одноосного нагружения, возникающего в металлизации отверстия при нагреве,

$$d\rho/\rho = B\,(1 - 2\,\mu)\,\varepsilon. \quad (4)$$

Объединяя (3) и (4), получаем:

$$k = 1 + 2\mu + B(1 - 2\mu). \quad (5)$$

Непосредственное влияние температуры на изменение сопротивления металлизации учитывается исходя из известного соотношения: $\Delta R/R = (T + 234)^{-1}$. Для чистой меди $B = 1$, по крайней мере, для температурного диапазона от 0 до 300°С. Отсюда по (5) численное выражение тензочувствительности металлизации отверстий равно 2. Т.е. относительное удлинение металлизации на 1% приводит к изменению сопротивления металлизации отверстия на 2%. Для исследований деформаций в пределах 6% с различимостью в 0,1% необходимая точность измерения сопротивлений практически обеспечивалась четырехзондовым методом с приборами первого класса точности. Для обеспечения контактирования четырех зондов провода к контактным площадкам припаивались холодными галлиевыми припоями, которые после образования твердых растворов выдерживают без разрушения температуры до 800°С (рис. 9).

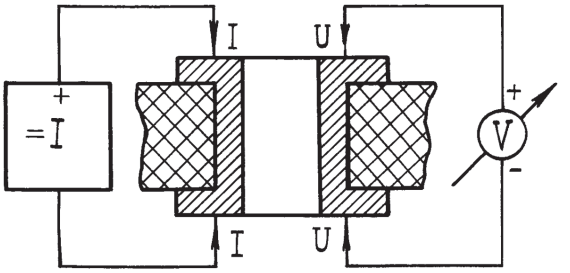


Рис.9. Схема измерения сопротивления металлизации отверстия четырехзондовым методом

Результаты экспериментальных исследований деформации

Результаты измерений деформации металлизированного отверстия диаметром 0,8 мм в МПП толщиной 1,6 мм, показанные на рис.10, дают хорошее совпадение с результатами графоаналитического анализа, проведенного на базе нелинейной модели термомеханических деформаций сквозных металлизированных отверстий.

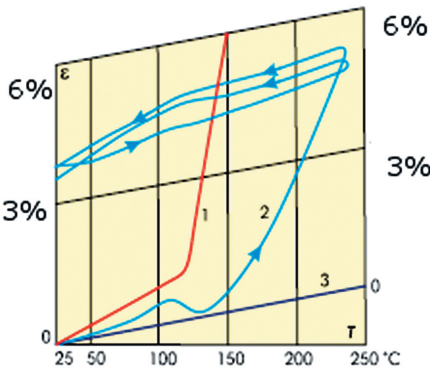


Рис. 10. Экспериментально полученные диаграммы температурной деформации металлизированного отверстия: 1 и 3 – диаграммы свободного расширения диэлектрика и меди; 2 – экспериментальная диаграмма деформации металлизированного отверстия

Сочетание больших деформаций металлизации отверстий при температурных нагрузках и уменьшение пластичности меди может при определенных условиях приводить к разрыву металлизации отверстий или сдвигу металлизации относительно стенок отверстий, если не принять мер для увеличения пластичности гальванических осаждений при температурах, соответствующих возможному нагреву МПП. В табл.1 приведены пороговые значении температур разрушения межсоединений в МПП.

Таблица 1. Пороговая температура начала разрушений

Отношение толщины МПП к размеру отверстия, H/d	**2:1**	**3:1**	**5:1**	**10:1**	**20:1**
Пластичность металлизации, %	Пороговая температура, °C				
4	290	250	220	210	190
6	320	290	260	240	220
8	380	350	320	280	260

При больших температурных деформациях, недостаточной пластичности металлизации и непрочном сцеплении металлизации со стенками сквозных отверстий МПП возможно разрушение внутренних соединений. Для выявления такого дефекта достаточно после термоудара (оплавления) спровоцировать окисление (влага + тепло) соприкасающихся поверхностей физического контакта

металлизации отверстий с торцами внутренних контактных площадок и по результатам измерений сопротивления внутренних соединений диагностировать надежность МПП.

Усталостные малоцикловые разрушения возможны только при переходе в область пластических деформаций. И чем глубже температурные деформации уходят в область пластических деформаций, тем раньше начинаются отказы соединений в процессе эксплуатации. Предложенными средствами контроля состояния соединений в МПП начало пластических деформаций обнаруживается как появление гистерезиса в диаграмме *температура – сопротивление* элемента цепи. Проведенные исследования позволяют количественно оценить влияние толщины металлизации сквозных отверстий на температуру, соответствующую началу пластических деформаций (табл.2).

Таблица 2. Начала пластической деформации при нагреве

Толщина металлизации в отверстии МПП, мкм	**Отношение толщины МПП к диаметру сквозного металлизированного отверстия (*H/d*)**		
	2:1	**3:1**	**5:1**
	Температура начала пластической деформации, °С		
10	75	60	50
15	85	73	55
20	95	80	60
25	100	85	65
30	110	90	70

Локальные дефекты, особенно в виде кольцевых утонений, значительно уменьшают устойчивость металлизации отверстий к циклическому воздействию температур.

Данные исследований демонстрируют бесполезность проведения термоциклирования для разбраковки монтажных изделий путем выявления ослабленных элементов соединений: циклические нагрузки разрушают дефектные элементы и создают усталостные ослабления соединений, близкие к границе различия качественных и дефектных элементов. Это обусловлено еще и тем, что граница качества между дефектными и качественными элементами размыта. Между ними всегда существуют промежуточные состояния, которые характеризуют возможность отказов соединений, вызванных усталостными явлениями.

Заключение

Надежность межсоединений в современной электронной аппаратуре технологически обеспечивается за счет высокого уровня пластичности металлизации печатных плат, устойчивой к малоцикловым усталостным разрушениям, спровоцированным групповым нагревом при многокаскадной пайке и наладочном ремонте печатных узлов.

Литература

1. **Медведев А.М.** Форум по бессвинцовой технологии пайки // Технологии в электронной промышленности. – 2007. – № 3.

2. **A. Medvedev.** Optimierte Leiterplatten für die bleifreie Löttechnologie (Physikalische Grundlagen der Verbindungszuverlässigkeit) – Electronishe Baugruppen und Leiterplatten – EBL 2008". Schwabenlandhalle Fellbach. 13 – 14.02.2008.

3. **Шкундина С.Е., Семенов П.В., Ващук Г.А.** Отраслевой стандарт открывает дорогу к использованию новых химических процессов и высококачественных материалов.// ПРОИЗВОДСТВО ЭЛЕКТРОНИКИ: Технологии, оборудование, материалы. – 2010. №1

Medvedev A.M.

PRINTED CIRCUIT BOARDS. RELIABILITY OF INTERCONNECTIONS

Stability of metallization of holes to thermomechanical pressure is provided with durability and plasticity of electrodeposited copper.
Distinctions in factors of thermal expansion of copper and dielectric of bases of printed circuit boards create powerful thermomechanical factors of rupture of metallization of apertures, destructions of internal interconnections in multilayered structures of printed-circuit boards. Standard norms of requirements for the depth of metallization of apertures, its durability and plasticity of copper were established in the course of manufacture of ordinary printed-circuit boards with reference to use of traditional technologies of soldering by tin-lead solders. Return to consideration of the copper plasticity problem has been caused first of all by transition to lead-free solders initiated by the all-European Directive RoHS [1], featuring a high temperature of soldering. Higher temperatures create large deformations of metallization of holes, which forces us to reconsider the requirements for plasticity of copper. At the same time, there is a general tendency to reduction of the diameter of metalized holes, and consequently to reduction of the area of metallization cross-section. Smaller sections have smaller resistance to rupture. Therefore, along with good plasticity, metallization of holes of printed-circuit boards should provide higher resilience to rupture as well. In this reference, deformation of metallization of holes when heating to soldering temperatures has been studied. The purpose of researches is to revise norms as regards plasticity of copper in holes of printed-circuit boards. It has been shown that the plasticity of copper deposition in holes of modern printed-circuit boards should not be less than 6% [2]. Current copper plating electrolytes allow us to reach plasticity of copper of 12-18% [3].

Keywords*: printed circuit boards, interconnection, plasticity of copper.*

The gist of the problem

The elements of interconnections are exposed to thermal loads in the process of manufacturing, assembling and cyclic changes in temperature during operation of the equipment. Differences in temperature coefficients of linear expansion (TCLR) of conductive structures and dielectric create thermo-mechanical tensions of various intensity in electrical connections. In longitudinal directions reinforced by fiberglass patches, differences in TCLR are so small that they do not affect the strength of connections of the longitudinal structure.

In the transversal direction perpendicular to the plane of the reinforcement, the differences are so significant in linear expansion ($17 \cdot 10^{-6}$ for copper and $(100 \ldots 400) \cdot 10$ -6 for dielectric basis) that thermomechanical tensions occurring due to temperature loads can break interlayer connections.

It is known that the resistance of metalized holes to thermo-mechanical loads is ensured by the depth and plasticity of metallization. Standard requirements for metallization on these quality criteria have been established during the years of practice in manufacturing and maintenance of electronic devices with printed assemblage with a thickness of boards in relation to the diameter of a hole from *1:1* to *3:1*. With the size of through holes less than 0.3 mm this ratio can be as high as *10:1...20:1*. In such constructions of multilayer printed circuit boards (MPCB), the ration of rigidity of apertures' metallization and their surrounding material of the bottom board is not in favor of metallization, since in conditions of thermal effects the deformation of metallization of holes substantially increases (Fig. 1). This phenomenon is aggravated by the decline in copper metallization of plasticity with an increasing temperature of soldering.

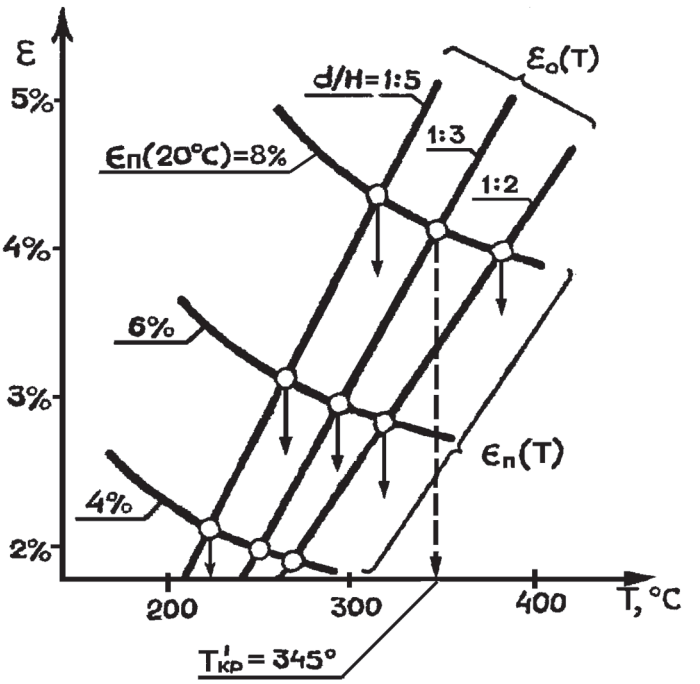


Fig. 1. The toughening of requirements for the plasticity of metallization with the diminution of the diameter of through holes

Statistics show that an especially big stream of failures in interlayer connections is observed equipment systematically exposed to cyclic changes in temperature (thermo cycles). According to the data of the long-term operation of one of aviation systems, printed circuit failures are distributed as follows: metalized holes are 24%, inner connections are 72%, printed conductors of internal layers are 0.1%, isolation is 2%, soldering is 2.5%, breaks of wires are 0.3%, others are 0.6%. Comparison of the number of failures of MPCB in stationary equipment functioning in a relative constancy of temperatures and in airborne equipment shows the difference in nearly three orders of magnitude, that making us believe that, if the level of variable thermo-mechanical tensions exceeds a certain limit, there is a process of gradual accumulation of damages, which ends in fatigue destructions of connections.

Model of thermo-mechanical stressing

Thermo-mechanical stress during heating causes the stretching of metallization along the axis of a hole (axial tensions) and the curving of contact pads, with the largest concentration of which being on the junction with the metal cylinder of a hole (curve tension). A typical distortion of the form of a hole in case of heating is schematically shown in Fig. 2 and in the picture of microslice in Fig. 3.

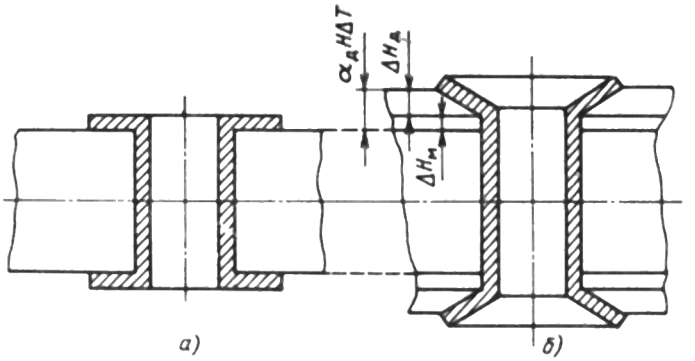


Fig. 2. Distortion of metalized holes when heated

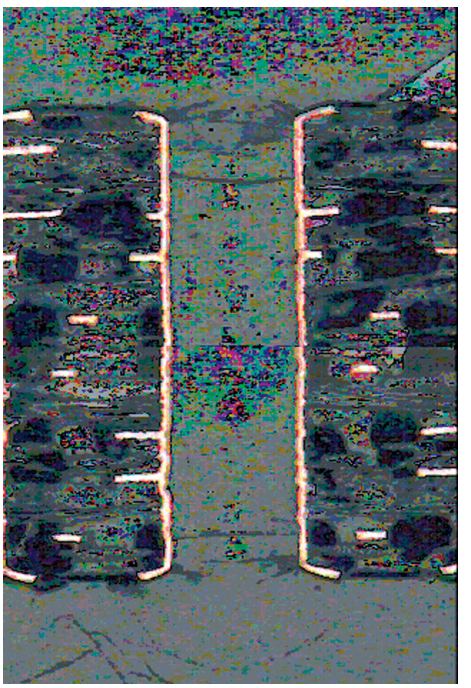


Fig. 3. Microslice of metalized holes after a thermo shock

In general, the relative deformation σ_Z of metallization under temperature loads can be represented as the sum of the elastic ε_Y and temperature ε_T deformations. Elastic deformation is $\varepsilon_Y = \sigma E$ (E is module of elasticity). Temperature deformation is $\varepsilon_T = \alpha(T\text{-}T_0)$. Hence, the thermo-mechanical stress is $\sigma = E\,[(\sigma_Z - \alpha(T\text{-}T_0)]$. Thermo-mechanical efforts in each of the elements of a metalized hole:

$$F = E[(\sigma_Z - \alpha(T\text{-}T_0)]\ h\ dZ.$$

To determine the characteristics of thermo-mechanical deformation of metallization, let us write an equation of equilibrium assuming that the sum of all thermo-mechanical efforts arising in components of *metallization-hole walls* system has to be zero (Fig. 4):

$$\int_0^{h_M} E_M[(\varepsilon_Z - \alpha_M(T - T_0)]hdZ + \int_{h_Д}^{0} E_Д[(\varepsilon_Z - \alpha_Д(T - T_0)]hdZ = 0.$$

After integration and transformation it can be shown that the deformation of copper in transversal direction *Z* is:

$$\varepsilon_Z = (\alpha_D - \alpha_M)\,(T - T_0)\,(1 + J_M/J_D)^{-1}, \quad (1)$$

where α_D and α_M are TCLR, J_M and J_D are relative rigidity of copper and dielectric.

If ε_Z exceeds the limit of elasticity of copper deposit in a hole (or $\sigma_R > \sigma_{PL}$), ring rapture of metallization occurs.

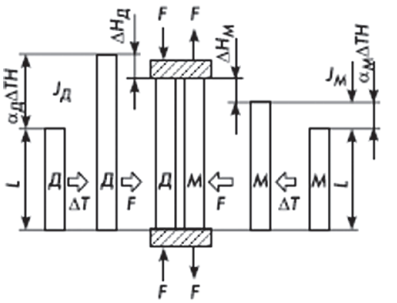


Fig. 4. Model of axial thermo-mechanical stresses

If the forces of adhesion of metallization with walls of a hole are small, shift tensions can be realized in rupture of internal connections. Shift stress should evidently increase with an increasing distance of junction from the neutral axis *0--0* (Fig. 5). The distance of shift, if it occurs, can be determined on the basis of general views. But if the coupling forces hold metallization on junctures of a hole, then an increasing tension of shift in the conditions of rising temperature stress is equal to $\sigma_{Sh} = G(\alpha_D - \alpha_M)\Delta T$. The value of destructive shift stress is determined based on the experimental values of pulling of metallization from a hole. Figure 6 shows a picture of destruction of an internal connection resulting from shift of metallization in relation to the walls of a hole.

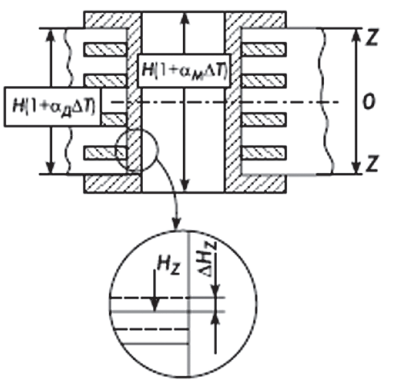


Fig. 5. Shift of metallization from ends of contact pads of inner layers

Fig. 7 shows a chart of temperature deformation of freely expanding cylinders of copper, polymeric composite dielectrics and the resulting temperature deformation of their aggregate, and Figure 8 shows a deformation-strain diagram. The curve of temperature expansion of dialectic basis has a fracture at the temperature of glass transition *Tg*. The zone of elastic deformation of copper is limited to the value ε_y.

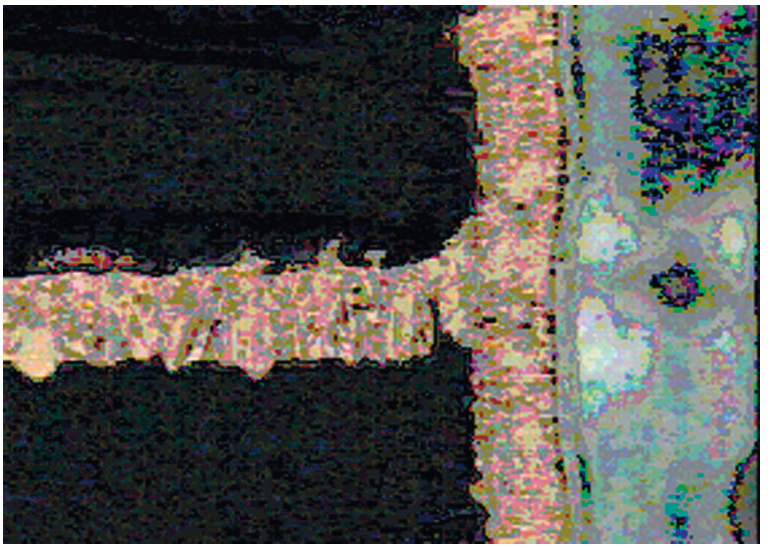


Fig. 6. Picture of the microslice of destructed internal connection

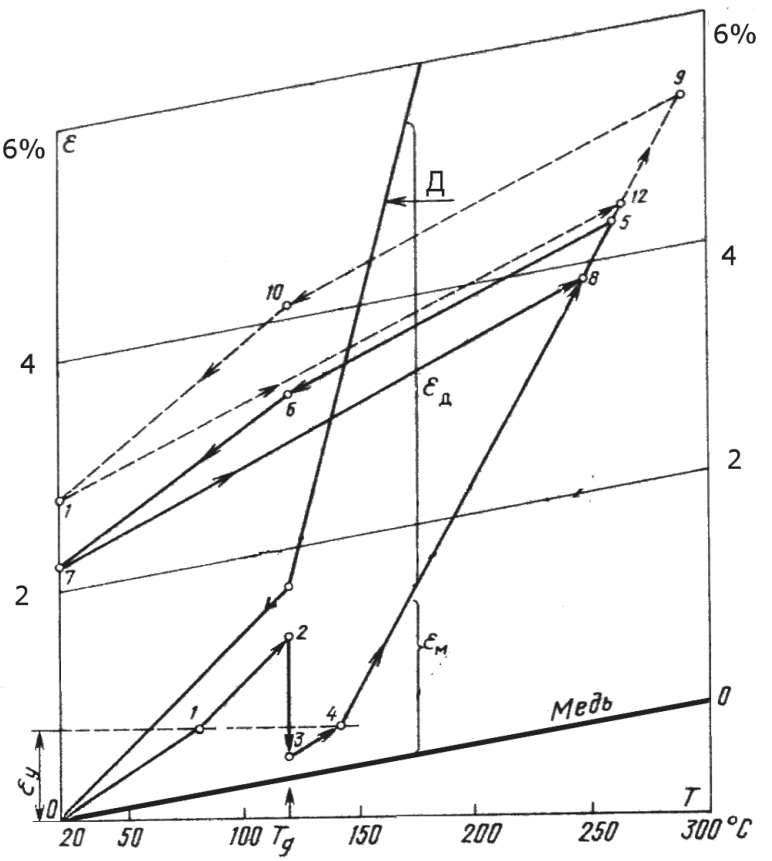


Fig. 7. Graph of temperature deformation of metallization of aperture received by graphical and analytical method

On 0-1 section, the shift module of copper corresponds to a section of elasticity, i.e. has a value G_M, the module of dielectric is equal to $G_Д$. The distribution of deformations of dielectric and copper yields to the ratio: $\alpha_D/\alpha_M = G_M S_M / G_D S_D$, where S_M and S_D are squares of cross section of loading of a copper cylinder and dielectric around it suffering from the load. When at point 1 the deformation of copper moves to a section of fluidity (1-2), its module decreases, so metallization of a hole is deformed practically following the free expansion of dielectric. Under the temperature of glass transition *Tg*, dielectric

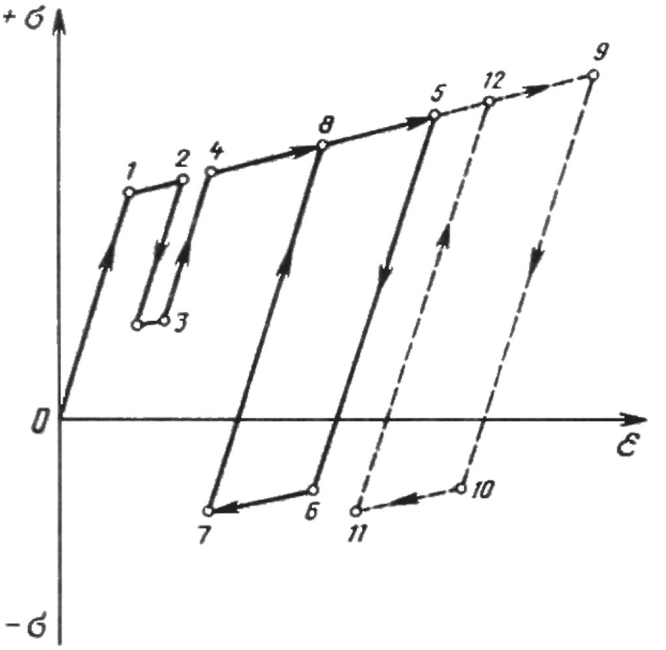


Fig. 8. Chart of deformation-strain

basis loses its rigidity, and due to that a copper cylinder is unloaded. Its deformation takes on a value that corresponds to point 3. When moving beyond the glass transition temperature *Tg*, dielectric begins to grow intensively. However, initially this does not result in a large extension of copper till its deformation does not exceed the limits of elasticity (section 3-4). Correlation of deformations of dielectric and copper on this section looks like:

$$\alpha_D/\alpha_M = G_M' S_M / G_D' S_D. \quad (2)$$

Curves 5-6-7-8-5 and 9-10-11-12-9 show the changes of the linear dimensions of a metalized hole in case of cooling and a repeated cycle of heating-cooling for soldering temperatures 260°C and 290°C, respectively. The presence of hysteresis in the diagram of temperature deformations reveals a certain percentage of plastic deformation of copper, which is a harbinger of fatigue destruction under cyclic temperature stress.

Methodology of experimental researches

One knows the basic principles of researching stresses in metallization of through holes using micrometrical sensors of shifting that register growth of thickness of the dielectric basis and metal cylinder of a through hole as MPCB is heating. Increase of the accuracy of measurements in a wide temperature range is ensured by using a quartz sample holders and shift passing rods. There have been attempts to use attachable strain gauge microsensors for measuring small elongations (extensometers) to study deformations of metallization of through holes during soldering. Comparison of measurement results of thermal expansions using these two methods obtained by different authors demonstrates their ambiguity due to the uncertainty of a starting base in the first case and low sensitivity of strain measuring to small samples, where MPCB belongs to, in the second case.

The author has used his own methodology to study thermo-mechanical stresses when the hole to be analyzed itself is used as a stain gauge sensor to measure its temperature deformations. In this case one uses the following assumptions. The relation of ohmic resistance change with deformation:

$\Delta R/R = k\varepsilon$, where k is the tensosensitivity of an element (in this case of a metalized hole itself). Since $R = \rho H/S$, the differential form of expression $\Delta R/R$ looks like $dR/R = d\,\rho/\rho + dH/H\text{-}dS/S$, where ρ is the electrical resistivity of metallization, H is the thickness of a board (length of the metalized cylinder of a hole), S is the square of cross-section of hole metallization perpendicular to its axis. For low relative lengthening $d\varepsilon = dH/H$, the relative change of cross-section square is $dS/S = -2\,\mu(dH/H)$. So $dR/R = d\rho/\rho + \varepsilon + 2\varepsilon$, where μ is Poisson's coefficient. Then the tensosensitivity of an element, i.e. the metallization of a hole is

$$k = (dR/R)\,\varepsilon^{-1} = (1 + 2\mu) + (d\rho/\rho)^{-1}. \quad (3)$$

Expression (3) consists of two parts: the geometrical part depending on ρ and reflecting electrical resistance changes only by changes in the size of a metal cylinder due to its longitudinal deformation, and the physical part linked with the change of total resistance of metallization when extending $d\rho/\rho = B\,dV/V$ and reflecting the linear dependence between the change in total resistance and the relative change of volume dV/V. B is Bridgman's coefficient. In the case of one-axial loading occurring in metallization of a hole during heating,

$$d\rho/\rho = B\,(1 - 2\,\mu)\,\varepsilon. \quad (4)$$

Combining (3) and (4), we get:

$$k = 1 + 2\mu + B(1 - 2\mu). \quad (5)$$

The direct effect of temperature on a change of metallization resistance is taken into account based on a known relation: $\Delta R/R = (+\,234)^{-1}$. For pure copper $B = 1$, at least for the temperature range from 0 to 300°C. Hence, according to (5), the numeric expression of tensosensitivity of hole metallization is equal to 2. I.e. a relative elongation of metallization by 1% leads to a change of resistance of hole metallization by 2%. For researches of deformation within 6% with the distinction of 0.1%, the required accuracy of measurement of resistances was almost ensured by a four-probe method with instruments of the first class precision. To make sure that four probes are contacted, wires to contact pads were soldered using cold gallium soldering that after the formation of solid solutions can withstand temperatures up to 800°C without rupture (Fig. 9).

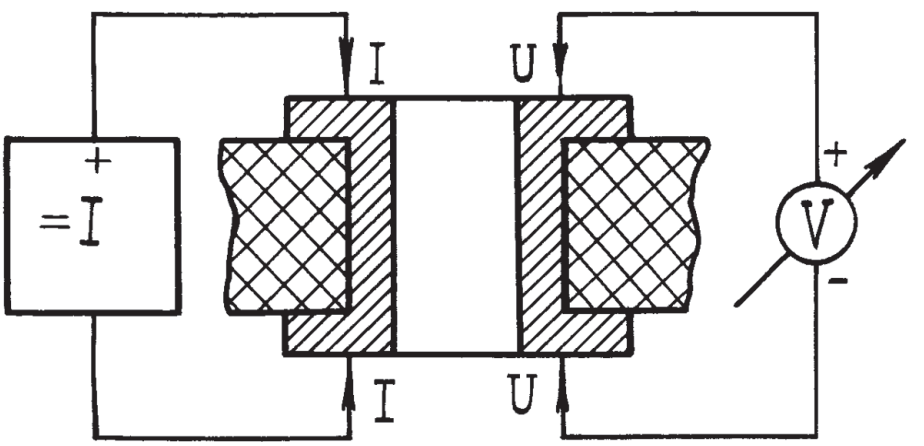


Fig. 9. Scheme of measuring the resistance of hole metallization by four-probe method

Results of experimental studies of deformation

Results of measurement of deformation of a metalized hole with a diameter of 0.8 mm in MPCB of 1.6 mm thick, shown in Fig. 10, are in good agreement with the results of the graphical and analytical analysis based on a nonlinear model of thermo-mechanical deformation of through metalized holes.

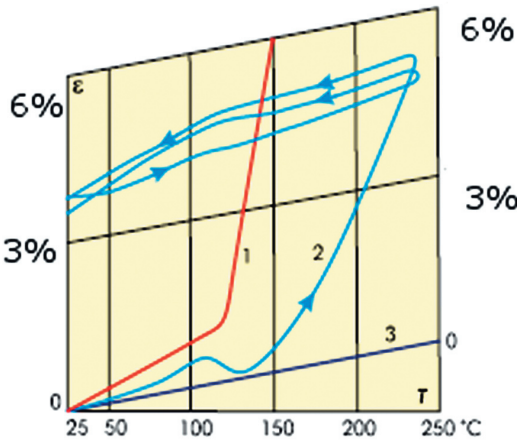


Fig. 10. Experimentally obtained diagrams of temperature deformation of metalized holes: 1 and 3 are charts of free expansion of dielectric and copper; 2 is the experimental chart of deformation of metalized holes

The combination of large deformations of metallization of holes under thermal loads and reduced plasticity of copper may in certain circumstances lead to rupture of hole metallization or metallization shift in relation to the walls of holes, if one does not take measures to increase the plasticity of galvanic deposition for temperatures corresponding to MPCB possible heating. Table 1 shows the threshold temperature values for destruction of interconnections in MPCB.

Table 1. Threshold temperature of the beginning of destruction

Ratio of MPCB thickness to diameter of a hole, *H/d*	**2:1**	**3:1**	**5:1**	**10:1**	**20:1**
Plasticity of metallization, %	Threshold temperature, °C				
4	290	250	220	210	190
6	320	290	260	240	220
8	380	350	320	280	260

In case of high temperature deformations, insufficient plasticity of metallization and shaky coupling of metallization with walls of MPCB through holes, destruction of internal connections may happen. To identify such defect, it is enough after a thermal shock (reflowing) to provoke oxidation (humidity + heat) of touching surfaces of physical contact of hole metallization with ends of internal contact pads, and using the results of measuring the resistance of internal connections to diagnose the reliability of MPCB.

Fatigue low-cycle destructions are only possible when moving in the area of plastic deformation. And the deeper the temperature deformation moves in the area of plastic deformation, the earlier failures of connections begin during operation. The offered methods for monitoring the status of connections in MPCB identify the start of plastic deformation as the emergence of hysteresis in the

temperature-resistance graph of a circuit element. The studies made allow us to quantify the influence of thickness of metallization of through holes on the temperature corresponding to the start of plastic deformation (Table 2).

Table 2. Start of plastic deformation during heating

Depth of metallization of MPCB hole, μ	Ratio of MPCB thickness to diameter of metalized through holes (*H/d*)		
	2:1	**3:1**	**5:1**
	Temperature of plastic deformation start, °C		
10	75	**60**	50
15	85	73	55
20	95	80	60
25	100	85	65
30	110	90	70

Local defects, particularly in the form of ring thinning, significantly reduce the resistance of the metallization of holes to cyclic temperatures.

Studies show the futility of thermal cycling for grading assembled products by identifying the weakened elements of connections: cyclic loads destroy defective items and create fatigue weakening of connections, close to the border of distinction between quality items and defective items. This is also due to the fact that the boundary of quality between good and defective and elements is blurred. There are always intermediate states between them that characterize the possibility of failure for connections due to fatigue phenomena.

Conclusion

Reliability of interconnections in modern electronic equipment is technologically provided by a high level of plasticity of metallization of printed circuit boards resistant to low-cycle fatigue destructions provoked by group heating in case of multistage soldering and troubleshooting repairs of printed circuit boards.

References

1. **Medvedev A.M.** Lead-free soldering. Technology Forum//Technology in electronics industry. 2007, #3.

2. **Medvedev A.** Optimierte Leiterplatten für die bleifreie Löttechnologie (Physikalische Grundlagen der Verbindungszuverlässigkeit) – Electronishe Baugruppen und Leiterplatten – EBL 2008". Schwabenlandhalle Fellbach. 13 – 14.02.2008.

3. **Shkundina S.E., Semenov P.V., Vashchuk G.A.** Industry standard paves the way to use new chemical processes and high-quality materials// MANUFACTURING OF ELECTRONICS: Technology, machinery, materials. – 2010. – #1.

Дамзен В.А., Елистратов С.В.

ИССЛЕДОВАНИЕ НАДЕЖНОСТИ АВТОМОБИЛЬНЫХ ШИН

Рассматриваются основные причины, определяющие надежность автомобильных шин. На основании статистических данных определены значения основных измерителей долговечности шин.

Ключевые слова: *автомобильные шины, надежность шин, ресурс автомобильных шин.*

Автомобиль представляет собой сложную систему, состоящую из множества элементов. Каждый из элементов вносит свой вклад в надежность всей системы. Одним из таких элементов являются автомобильные шины. И хотя процесс замены неисправного элемента на исправный не представляет больших трудностей, автомобиль выходит из строя. Следовательно, происходит снижение показателей надежности транспортного средства. При отдельном рассмотрении автомобильных шин к ним применимы все свойства надежности: безотказность, долговечность, ремонтопригодность, сохраняемость. В большинстве случаев надежность шин оценивают по совокупности показателей. Показателями, определяющими надежность шины, могут быть износ протектора (до минимально допустимой величины протектора), пробои и порезы, усталостные дефекты каркаса или все показатели сразу. Так, в [1] представлены функции вероятности безотказной работы грузовых шин по перечисленным показателям. Примеры распределения партии восстановленных шин, снятых с эксплуатации по пробегу и определение ожидаемого пробега шин представлены в [2].

На основании статистических данных по обращениям в шиномонтажную мастерскую проведен анализ надежности автомобильных шин. В качестве показателей надежности предлагается использовать вероятность безотказной работы шин, вероятность отказов, частоту отказов, интенсивность отказов, гамма-процентный ресурс шин, закон распределения выхода шин из строя по пробегу. Такие свойства надежности, как ремонтопригодность и сохраняемость автомобильных шин, в данной работе не рассматривались. При сборе информации о ресурсе шин фиксировался факт снятия шин с эксплуатации, и ремонтные операции в статистических данных не отражались. В соответствии с нормативной документацией завод-изготовитель автомобильных шин гарантирует их сохраняемость в течение 5 лет с даты изготовления.

По исходным данным было проведено распределение шин по пробегу со следующими параметрами: количество интервалов разбиения $m = 15$; длина интервалов $\Delta t = 11334$ км. В результате получена гистограмма частот распределения отказов шин по пробегу (рис. 1).

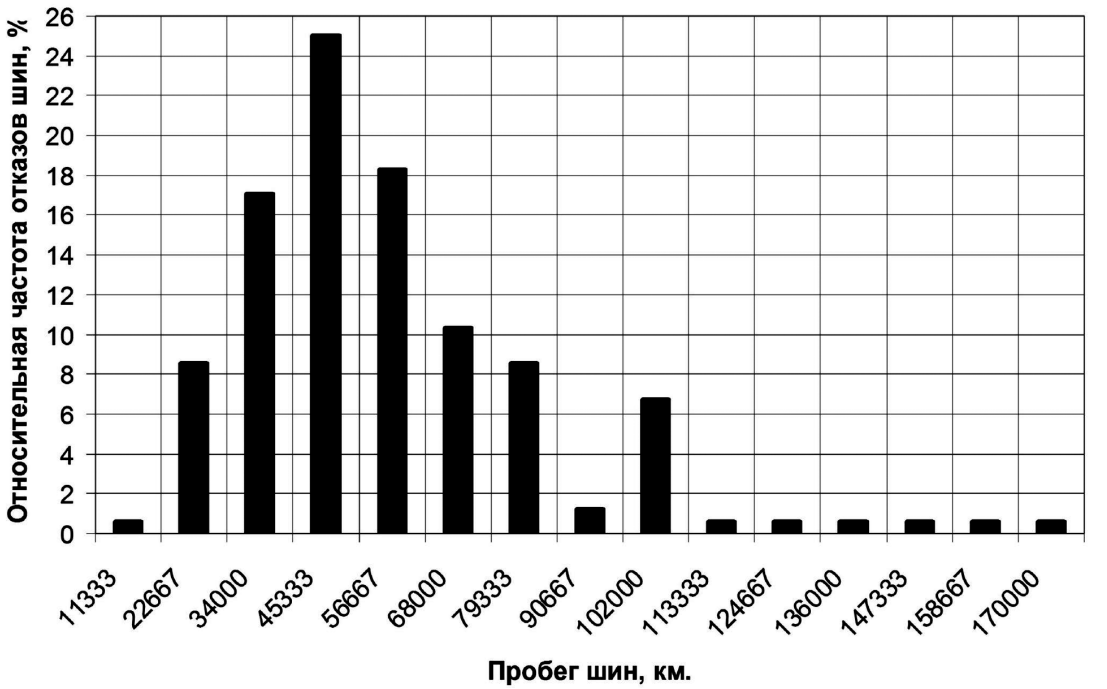


Рис. 1. Гистограмма частот распределения отказов шин по пробегу

В соответствии с [3] вероятностью безотказной работы называется количественная мера того, что при определенных условиях эксплуатации в заданном интервале времени или в пределах заданной наработки не произойдет ни одного отказа, и определяется по формуле:

$$P(t) = \frac{N - n(t)}{N}, \tag{1}$$

где: N – число испытываемых объектов; n(t) – число отказавших элементов за время t.

Вероятностью отказа называется количественная мера того, что при определенных условиях эксплуатации в заданном интервале времени возникает хотя бы один отказ. Отказ и безотказная работа являются событиями несовместными и противоположными. Следовательно, вероятность отказа определяется по формуле [3]:

$$Q(t) = 1 - P(t). \tag{2}$$

Расчетные значения по формулам (1) и (2) представлены в виде графиков на рис. 2.

По графику можно определить гамма-процентный ресурс шин. Он определяется как суммарная наработка, в течение которой объект не достигнет предельного состояния с вероятностью гамма, выраженной в процентах [4]. Тогда 90 % гамма-процентный ресурс составит 23000 км пробега, что соответствует вероятности безотказной работы шин равной 0,9. Кроме того, из анализа интегральных функций (рис. 2) видно, что 50 % вероятность безотказной работы шин составляет 45000 км пробега.

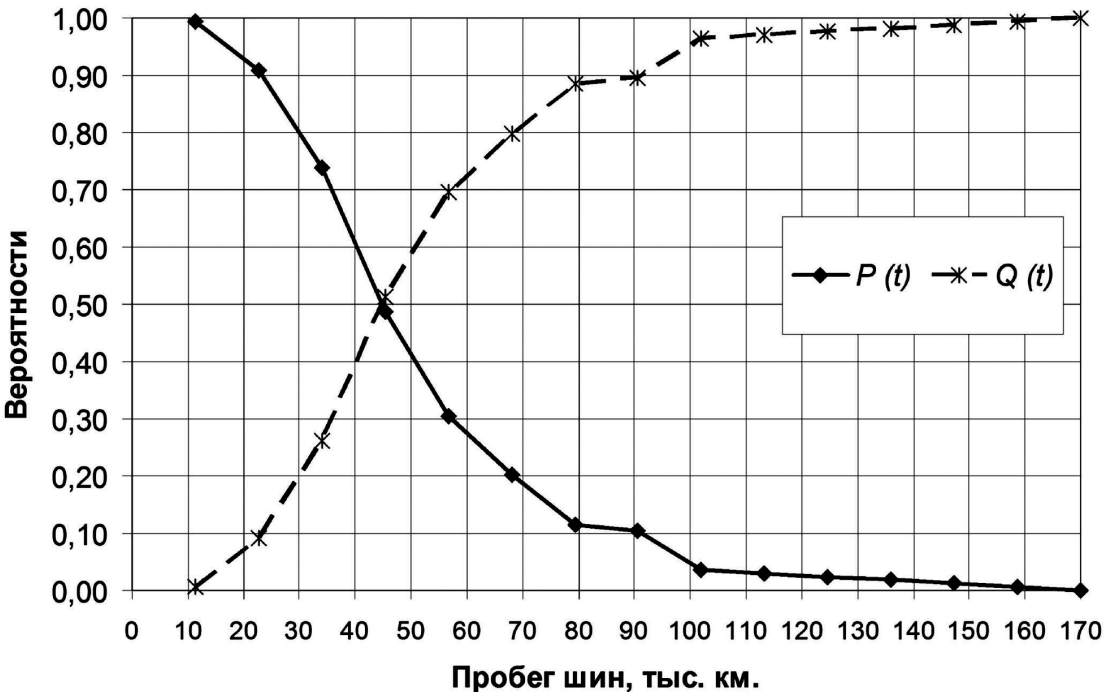


Рис. 2. Интегральные функции безотказной работы P(t) и отказов Q(t)

Частота отказов по статистическим данным – отношение числа отказавших элементов в единицу времени к первоначальному числу работающих (испытываемых), которая определяется по формуле [3]:

$$f(t) = \frac{n(\Delta t)}{N \cdot \Delta t}, \tag{3}$$

где: n(Δt) – число отказавших элементов в интервале времени от (t – Δt)/2 до (t + Δt)/2.

Интенсивностью отказов по статистическим данным называется отношение числа отказавших изделий в единицу времени к среднему числу изделий, исправно работающих в данный отрезок времени[3].

$$\lambda(t) = \frac{n(\Delta t)}{N_{\varphi} \cdot \Delta t}, \tag{4}$$

где: $N_{ср}$ – среднее число исправно работающих изделий в интервале Δt.

Величины частоты и интенсивности отказов имеют одинаковый порядок значений и размерность, поэтому могут изображаться в одних координатах. Результаты расчетов по формулам (3) и (4) представлены на рис. 3.

Среднее время (пробег) безотказной работы вычисляется по формуле [3]:

$$T_1 \approx \frac{\sum_{i=1}^{m} n_i \cdot t_{cpi}}{N}, \tag{5}$$

где: t_{cpi} находится по следующей формуле: $t_{cpi} = (t_{i-1} + t_i)/2$

где: t_{i-1} – время начала i-го интервала; t_i – время конца i-го интервала.

В результате расчетов по формуле (5) получаем, что средний пробег безотказной работы шин составляет $T_1 = 50790$ км.

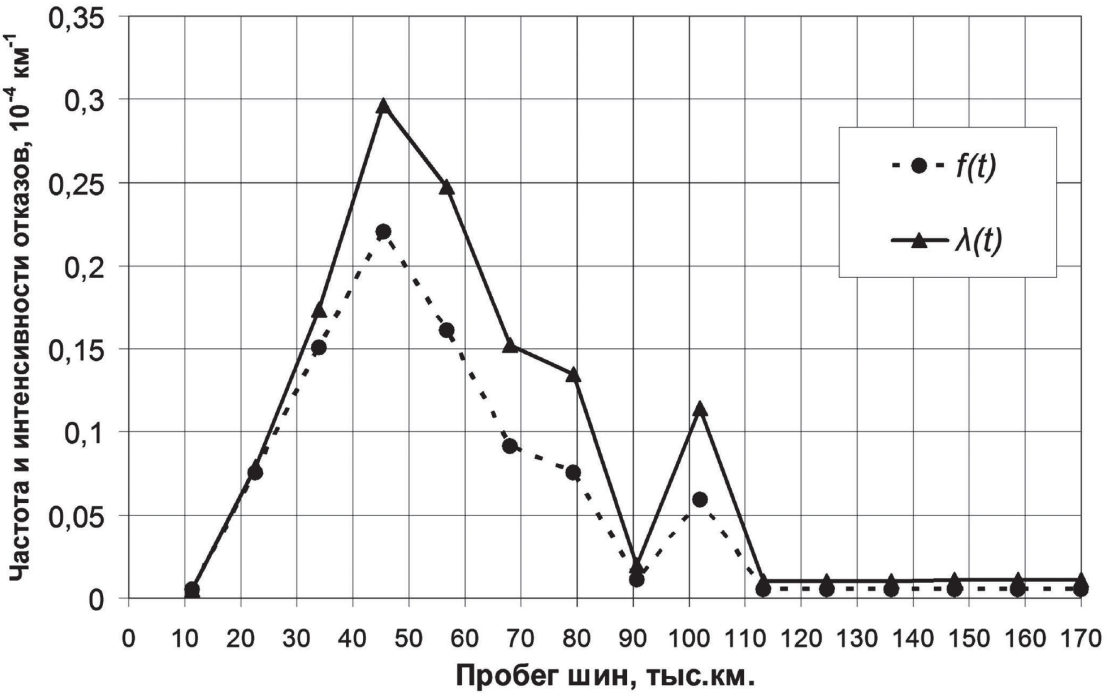


Рис. 3. График зависимости частоты f(t) и интенсивности λ(t) отказов автомобильных шин от пробега

В общем случае результаты наблюдений выхода шин из строя (рис. 1) могут подчиняться некоторому теоретическому закону распределения. Проверка соответствия теоретического распределения результатам наблюдений проводится с помощью критерия соответствия χ^2. Выбранное теоретическое распределение подтверждается, если выполняется условие [5]:

$$\chi^2 < \chi^2_{\alpha}, \tag{6}$$

где: χ^2 – расчетное значение параметра; χ^2_{α} – теоретическое значение параметра.

Для 10 %-ного уровня значимости и числа степеней свободы равном 6, табличное значение $\chi^2_{\alpha} = 10{,}645$ [5]. При подборке теоретических распределений получены следующие результаты:

1. Нормальное распределение – $\chi^2 = 39{,}16$
2. Гамма-распределение – $\chi^2 = 14{,}97$
3. Логарифмически нормальное распределение – $\chi^2 = 9{,}26$

Условие (6) выполняется только для логарифмически нормального распределения:

$9{,}26 < 10{,}645$.

Следовательно, при определении надежности шин принимается логарифмически нормальный закон распределения. На рис. 4 представлены кривые теоретического распределения и экспериментальных данных.

Соответствие экспериментальных данных логарифмически нормальному закону распределения означает, что случайная величина (пробег шины) зависит от большого числа независимых факторов [6]. Действительно, на надежность автомобильных шин влияют многие факторы: качество шин, состояние дороги, скорость автомобиля, мастерство водителя, давление в шинах, углы установки колес и другие.

На основании представленных данных можно сделать следующие выводы. Статистические данные по пробегу шин легковых автомобилей соответствуют логарифмически нормальному закону распределения случайной величины. При этом теоретический пробег шин несколько ниже реаль-

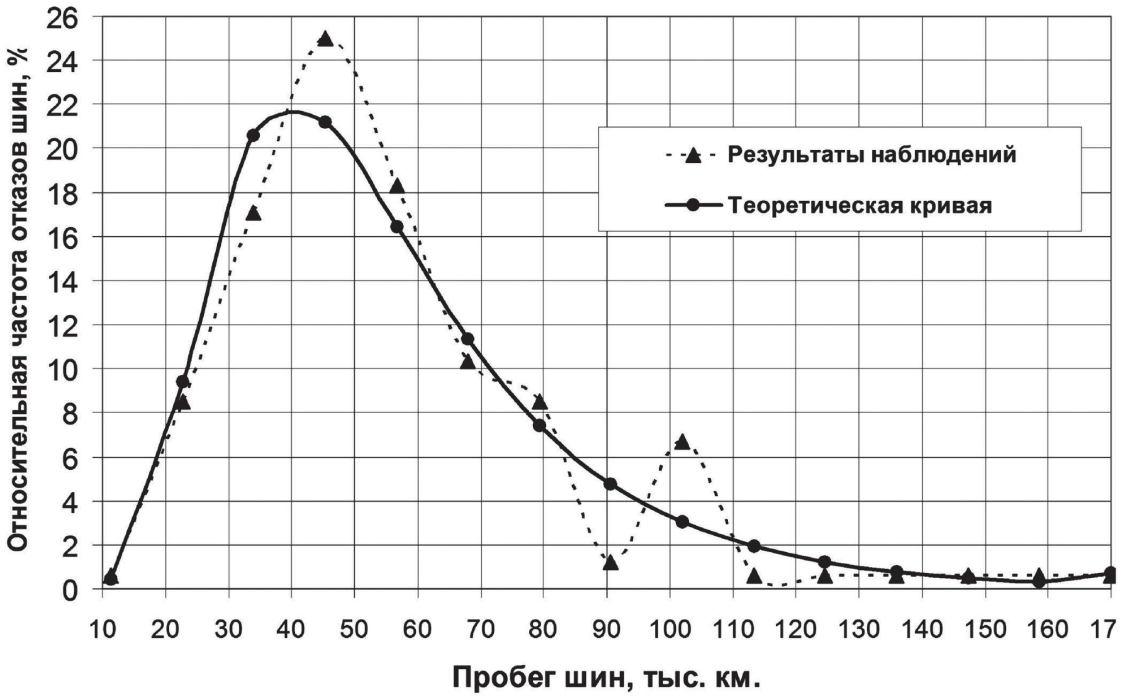


Рис. 4. Кривые теоретического распределения и экспериментальных данных отказов автомобильных шин

ного. В соответствии с гистограммой (рис. 1) наибольшее количество шин, примерно 42%, выходят из строя при пробеге 45-56 тысяч километров. А по теоретическому закону максимум выходов из строя шин (41,5 %) приходится на пробег 34-45 тысяч километров (рис. 4). Тогда теоретическая вероятность безотказной работы составляет 0,5-0,3, а экспериментальная вероятность безотказной работы – 0,74-0,5. Десятипроцентная вероятность отказа шин наступает при пробеге более 23000 километров. В то же время средний пробег безотказной работы составляет 50790 километров. Наибольший пробег шин доходит до 170000 километров. До пробега более 90000 километров «доживают» лишь 12 % шин и вероятность их отказа составляет 0,9. Однако это показывает, что имеется возможность увеличения надежности автомобильных шин в эксплуатации за счет повышения качества факторов, определяющих их ресурс.

Литература

1. **Третьяков О.Б.** Автомобильные шины. Конструкция, механика, свойства, эксплуатация / О.Б. Третьяков, В.А. Гудков, А.А. Вольнов, В.Н. Тарновский. – М.: КолосС, Химия, 2007. – 432 с.

2. **Евзович В.Е.** Восстановление изношенных пневматических шин / В.Е. Евзович – М.: Автополис-плюс, 2005. – 624 с.

3. **Корчагин А.Б.** Надежность технических систем и техногенный риск: учебное пособие в двух частях. Часть 2. Практикум / А.Б. Корчагин, В.С. Сердюк, А.И. Бокарев. – Омск: Издательство ОмГТУ, 2011. – 140 с.

4. **Курчаткин В.В.** Надежность и ремонт машин / В.В. Курчаткин, Н.Ф. Тельнов, К.А. Ачкасов и др.; под ред. В.В. Курчаткина. – М.: Колос, 2000. – 776 с.

5. **Львовский Е.Н.** Статистические методы построения эмпирических формул / Е.Н. Львовский. Учебное пособие для втузов. – 2-е изд., перераб. и доп. – М.: Высшая школа, 1988. – 239 с.

6. **Айвазян С.А.** Прикладная статистика: Основы моделирования и первичная обработка данных. Справочное издание / С.А. Айвазян, И.С. Енюков, Л.Д. Мешалкин. – М.: Финансы и статистика, 1983. – 471 с.

Damzen V.A., Yelistratov S.V.

RELIABILITY STUDY OF CAR TIRES

The paper analyzes the primary factors defining the reliability of car tires. Using statistical data, the values of the key indicators of tire reliability have been identified.

Keywords: *car tires, tire reliability, car tire life.*

An automobile is a complex system composed of many elements. Each element contributes to the reliability of the whole system. One of those elements is car tires. While replacing a failed element does not cause significant difficulties, in the process the car goes out of order. That entails a reduction of the vehicle's reliability factors. Individually, car tires are analyzed based on the whole range of reliability factors: fail-free operation, durability, maintainability, storability. In most cases the reliability of tires is evaluated as per totality of the factors. Among the factors defining the reliability of tires are tread wear

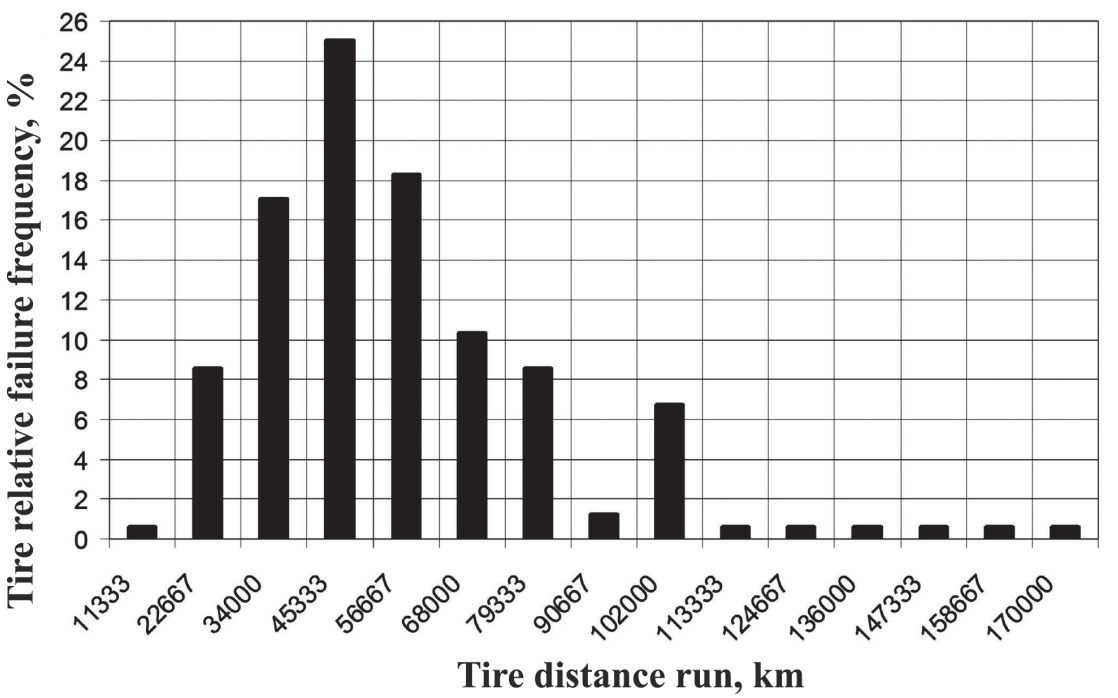


Fig. 1. Bar chart of tire failure frequency distribution depending on the distance run

(down to the minimum allowed size), punctures and cuts, fatigue-related defects of tire carcass or all factors simultaneously. Thus, [1] shows the probability function of dependable operation of truck tires as per the above factors. Examples of distribution of recovered tires taken out of operation based on distance run and identification of expected distance run are presented in [2].

Based on statistical data gathered by tire repair centers, an analysis of car tire reliability has been conducted. We suggest using the following reliability factors: probability of tire dependable operation, probability of failure, failure density, failure rate, gamma-percentile tire life, distribution law of tire failure depending on distance run. Such reliability factors as maintainability and storability of car tires are not considered in this paper. The tire life information gathered reflects the fact of tire decommissioning while repair operations are not included in the statistical data. As provided in relevant regulatory documents, the manufacturer of car tires guarantees their storability within 5 years from the date of manufacture.

Based on the input data, the tires were grouped according to the distance run with the following parameters: number of partition intervals m = 15; length of intervals Δt = 11334 km. As a result, a bar chart of tire failure frequency distribution depending on the distance run was constructed (Fig. 1).

As per [3], the probability of dependable operation is the quantitative measure of non-occurrence of a single failure under certain operational conditions within a given time interval or within a given operation time and is determined from the formula:

$$P(t) = \frac{N - n(t)}{N}, \tag{1}$$

where N is the number of tested units; n(t) is the number of units that failed within the time t.

The probability of failure is the quantitative measure of at least one failure occurring under certain operational conditions within a given time interval. Failure and dependable operation are incompatible and opposite events. Therefore, the probability of failure is determined from the formula [3]:

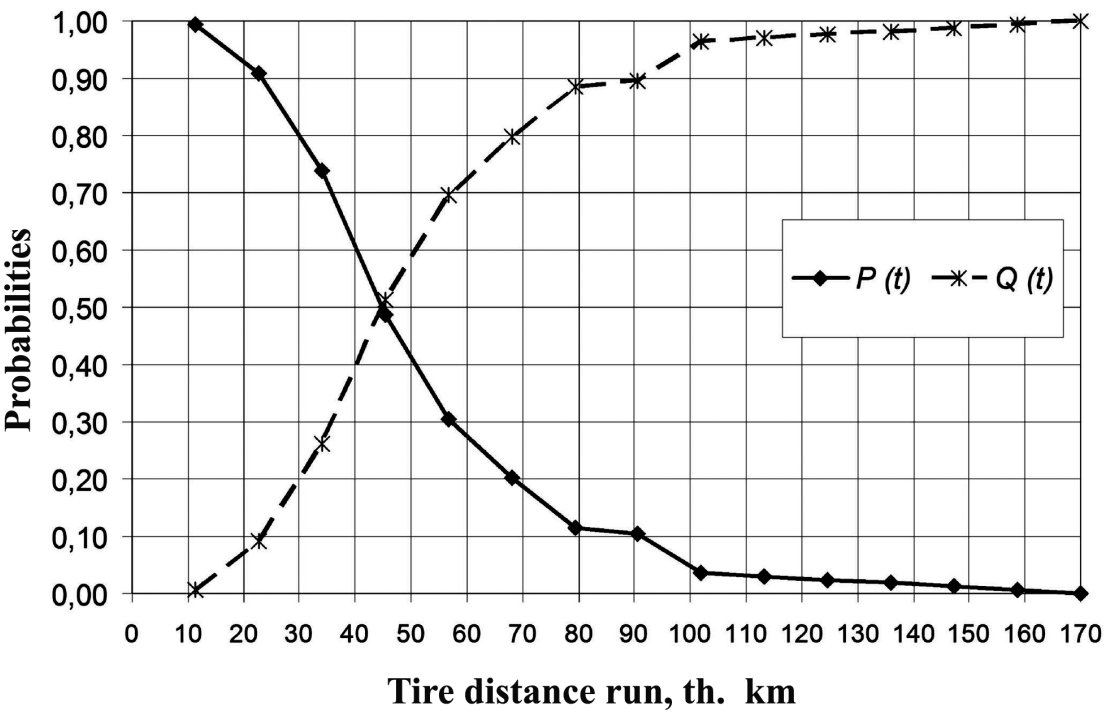


Fig. 2. Integral functions of dependable operation P(t) and failures Q(t)

$$Q(t) = 1 - P(t). \quad (2)$$

Calculated values as per formulas (1) and (2) are represented in the form of graphs in Fig. 2.

The tire's gamma-percentile life can be determined by the graph. It is defined as the total operation time during which a unit does not reach a certain condition with a probability expressed as a percentage [4]. Then a 90% gamma-percentile life will amount to 23000 km of distance run which corresponds to the probability of tire dependable operation of 0,9. Furthermore, integral function analysis (Fig. 2) shows that a 50% probability of tire dependable operation is 45000 km of distance run.

The failure density according to statistical data is the relation of the number of failed elements per unit time to the initial number of operable (tested) ones and is determined from the formula [3]:

$$f(t) = \frac{n(\Delta t)}{N \cdot \Delta t}, \quad (3)$$

where n(Δt) is the number of failed elements within the time interval from (t – Δt)/2 to (t + Δt)/2.

The failure rate according to statistical data is the relation of the number of failed units per unit time to the average number of units operating dependably within a given time period [3]:

$$\lambda(t) = \frac{n(\Delta t)}{N_{\varphi} \cdot \Delta t}, \quad (4)$$

where N_{cp} is the average number of operable units within the time interval Δt.

The values of failure density and failure rate are identical in order and degree, and therefore can be expressed within the same coordinate space. Calculation data as per formulas (3) and (4) are represented in Fig. 3.

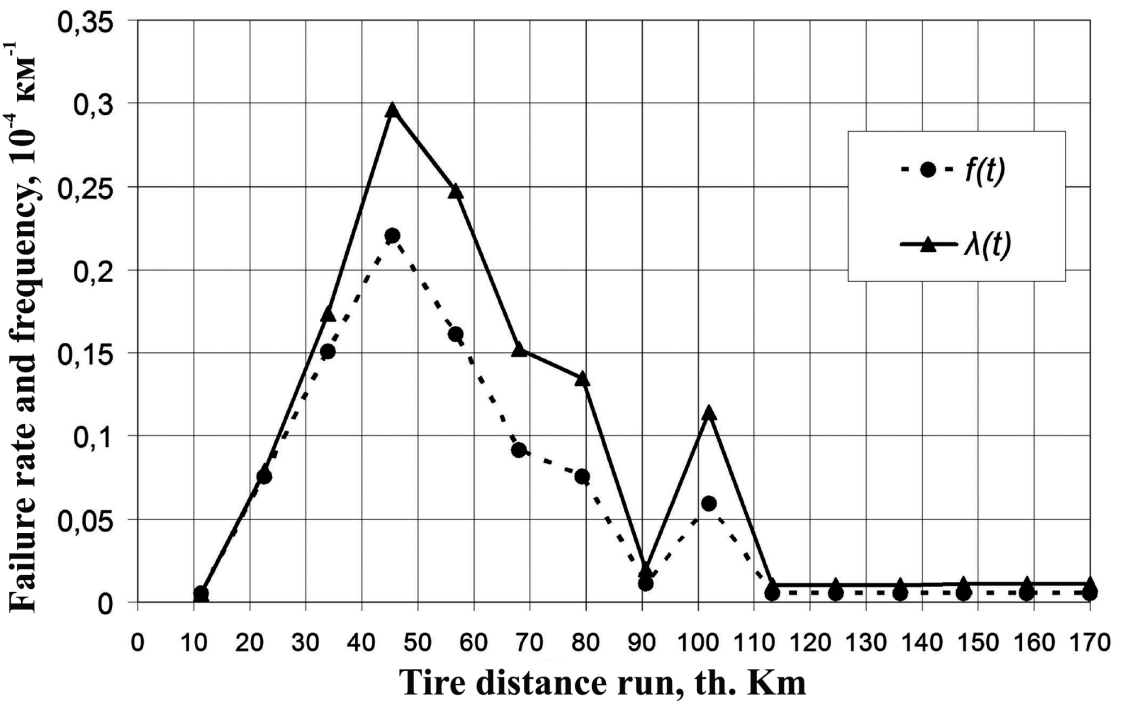


Fig. 3. Diagram of dependence of car tire failure density f(t) and rate λ(t) from the distance run

Average time (of operation) is calculated according to formula [3]:

$$T_1 \approx \frac{\sum_{i=1}^{m} n_i \cdot t_{cpi}}{N}, \quad (5)$$

where t_{cpi} is determined according to the formula: $t_{cpi} = (t_{i-1} + t_i)/2$.
where t_{i-1} is the time of the beginning of the *i*-interval; t_i is the time of the end of the *i*-interval.

Calculations according to formula (5) show that the average fault-less distance run by a tire is T_1 = 50790 km.

In general, the results of tire failure monitoring (Fig. 1) may follow a certain theoretical law of distribution. The verification of the theoretical distribution of monitoring results is performed using matching criteria χ^2. The identified theoretical distribution is confirmed if the following condition is true [5]:

$$\chi^2 < \chi^2_{\alpha}, \quad (6)$$

where χ^2 is the calculated parameter value; χ^2_{α} is the theoretical parameter value.

For a 10-percent significance and the number of the degrees of freedom equal to 6, the tabulated point χ^2_{α} = 10.645 [5]. The selection of theoretical distributions has provided the following results:

1. Normal distribution is χ^2 = 39.16.
2. Gamma distribution is χ^2 = 14.97.
3. Logarithmically normal distribution is χ^2 = 9.26.

The condition (6) is true only if the logarithmically normal distribution is 9.26<10.645.

Therefore, in order to identify the reliability of tires, the logarithmically normal distribution law is applied. Fig. 4 shows the theoretical distribution and experimental data curves.

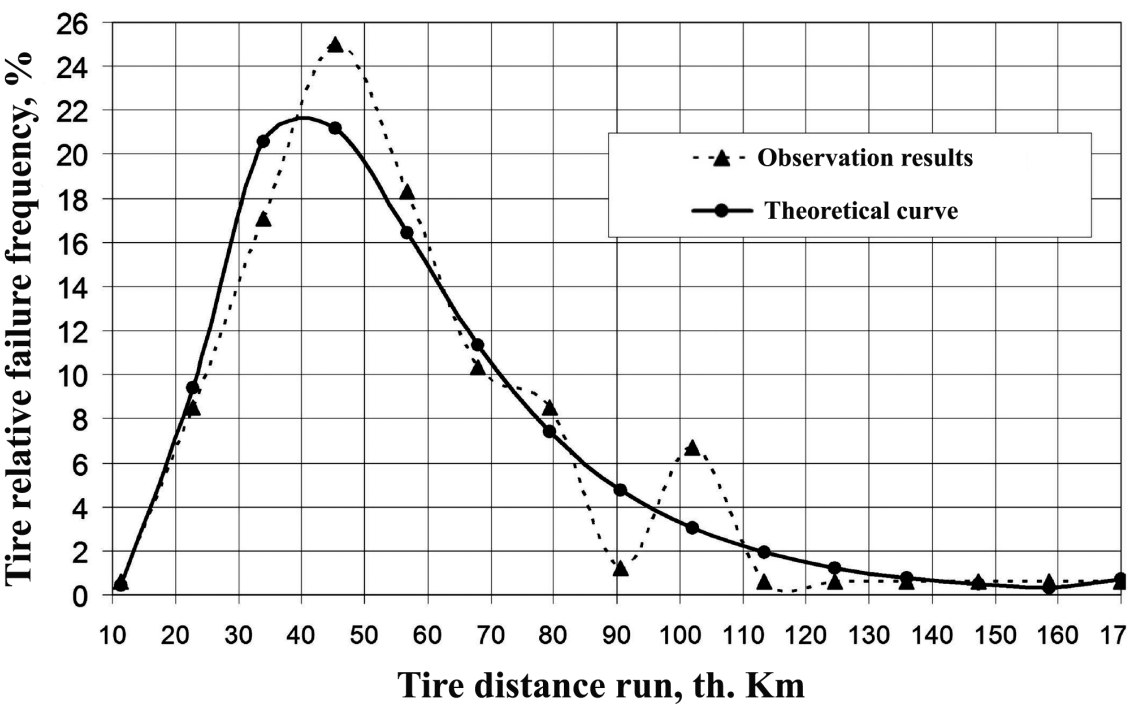


Fig. 4. Car tire failure theoretical distribution and experimental data curves

The conformity of experimental data with the logarithmically normal distribution law means that a random value (tire reliable operation) depends on a large number of unrelated factors [6]. In fact, a number of factors affect the reliability of car tires: quality of tires, condition of the road, car speed, driver's skill, tire pressure, wheel alignment, etc.

Based on the presented data, the following conclusions can be made. Statistical data of car tire operation match the logarithmically normal random distribution law. Furthermore, the theoretical operation time is somewhat lower than the actual one. As shown in the chart (Fig. 1), most of the tires (about 42%) fail at the 45-56 thousand kilometers of distance run. However, according to the theoretical law, most of the tires (41.5%) fail within the 34-45 thousand kilometer interval (Fig. 4). Then, the theoretical probability of reliable operation is 0.5-0.3, while the experimental probability of reliable operation is 0.74-0.5. The 10-percent probability of tire failure occurs after 23 thousand kilometers run. At the same time, the average reliable operation is 50790 kilometers. Maximum tire distance run reaches 170000 kilometers. Only 12% of tires reach distances run over 90000 kilometers, and their failure probability is 0.9. However, this shows a potential for increased car tire reliability by means of improvement of the quality of the factors that define their life.

References

1. **Tretiakov O.B.** Car tires. Design, mechanics, properties, operation. Tretiakov O.B., Gudkov V.A., Volnov A.A., Tarnovsky V.N. Moscow: KolosS, Khimia, 2007. – 432 p.

2. **Yevzovich V.E.** Recovery of worn pneumatic tires. Moscow: Avtopolis-plus, 2005. – 624 p.

3. **Korchagin A.B.** Dependability of technical systems and technology-related risk: study guide in two parts. Part 2. Praktikum. Korchagin A.B., Serdiuk V.S., Bokarev A.I. Omsk: Izdatelstvo OmGTU, 2011. – 140 p.

4. **Kurchatkin V.V.** Cars dependability and repair. Kurchatkin V.V., Telnov N.F., Achkasov K.A. and others; edited by V. V. Kurchatkin. Moscow: Kolos, 2000. – 776 p.

5. **Lvovsky E.N.** Statistical methods of empirical formula construction. Lvovsky E.N. study guide for technical colleges. – 2nd edition, revised and enlarged. Moscow: Vyshaya shkola, 1988. – 239 p.

6. **Aivazian S.A.** Applied statistics: Introduction to modelling and initial data processing. Reference book. Aivazian S.A., Yeniukov I.S., Meshalkin L.D. Moscow: Financy i statistika, 1983. – 471 p.

Перегуда А.И.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАДЕЖНОСТИ ИЗДЕЛИЯ, ПОДВЕРЖЕННОГО УДАРНЫМ НАГРУЗКАМ

Рассматривается математическая модель надежности, учитывающая кумулятивное накопление нагрузки изделием, вызванное воздействием циклических ударных нагрузок. Изучение процесса пересечения случайного уровня прочности накопленной нагрузкой при многократном воздействии ударных возмущений позволило получить математическую модель, которая дает возможность вычислять показатели надежности и долговечности. Полученные конечные соотношения для показателей надежности имеют простой вид, что позволяет их использовать при практических вычислениях.

Ключевые слова: *накопление повреждений, ударная нагрузка, распределение сумм случайных величин, показатель надежности, долговечность, оценка среднего значения, удар, пересечения уровня.*

Введение

В процессе эксплуатации изделий под воздействием таких факторов как повышенные температура и давление, циклические нагрузки, наличие коррозионной среды, которые приводят, например, к росту трещин усталости, и происходит старение материала. К настоящему времени в механике излома и механике материалов хорошо изучены физические процессы, приводящие к отказам оборудования.

В [1] отмечается, что к настоящему времени поведение конструкционных материалов в эксплуатационных условиях изучено не настолько хорошо, чтобы стать основой для обоснования модели кумулятивных повреждений на фундаментальных физических законах. Очевидно, что указанные задачи могут решаться без оценки количественной характеристики надежности, используя опыт эксплуатации подобных устройств в аналогичных или сходных производствах. Однако такое решение задачи без строгого математического анализа процессов функционирования и получения количественных оценок надежности и долговечности ни в коей мере нельзя считать достаточно обоснованным.

Рассматриваемый нами процесс функционирования изделия, на которое воздействуют ударные нагрузки, можно рассматривать как процесс со старением. В [2] введено понятие старения, основанное на поведении во времени функции интенсивности отказов. В частности, были определены возрастающая функция интенсивности ВФИ и убывающая функция интенсивности УФИ. Также было показано, что, если система состоит из независимых элементов с ВФИ распределением времени безотказной работы, то возникает распределение с возрастающей в среднем функцией интенсивности ВСФИ.

Часто можно получить сведения о нарастающем старении устройств, рассматривая динамику определенных параметров. Знание показателей процесса изменения параметра позволяет найти распределение наработок до отказа устройства, что, в свою очередь, дает возможность определения сроков остановки эксплуатации до его полного разрушения и последующего восстановления свойств устройства. Естественно, что при эксплуатации таких систем возникают задачи оценки количественных значений показателей их надежности и долговечности, а затем и планирование сроков остановки эксплуатации изделия [3].

К настоящему времени удовлетворительно развиты математические модели надежности изделий, к которым приложена статическая нагрузка и методы получения соответствующих показателей [4, 5]. В случае, когда кроме статической нагрузки, к изделию приложена нагрузка, имеющая случайную амплитуду и случайный период колебания, математические модели описания функционирования таких изделий становятся весьма громоздкими и получение из их анализа количественных значений для соответствующих показателей надежности и долговечности в общем случае не представляется возможным. Процесс функционирования таких изделий описывается стохастическим дифференциальным уравнением Ито с дискретной составляющей [6]. В [7] рассмотрен асимптотический метод вычисления показателей долговечности изделия, к которому прилагаются ударные нагрузки и показано, что такой процесс является процессом с независимыми приращениями.

Изучение процессов накопления нагрузки приведено в [8], где кроме этого рассмотрены вопросы оптимизации профилактического обслуживания по критерию минимума ожидаемой стоимости.

В данной работе будет изучаться математическая модель надежности функционирования изделия, на которое воздействуют ударные нагрузки при условии, что прочность является веерным случайным процессом.

Остановимся сразу на математической постановке задачи нахождения показателей надежности и долговечности, используя математическую модель эволюции изделия, основанной на теории случайных процессов накопления.

Постановка задачи

Рассмотрим изделие, подверженное износу из-за приложенного к нему ряда импульсных воздействий, это могут быть: толчки, удары, пульсации температуры и давления, вибрации и др. В дальнейшем, не уточняя физическую природу воздействий на изделие, будем импульсные воздействия называть ударными (циклическими) нагрузками. Пусть изменение параметров изделия вызвано ударными нагрузками (ударами, толчками импульсами), проявляющимися в моменты времени $t_0,\ t_1,\ t_2, \cdots,\ t_{k+1} \geq t_k,\quad k \geq 1$. Обозначим $\tau_i = t_{i+1} - t_i\ ,\ i > 0\ ,\ t_0 = 0$, где τ_i – случайные величины и соответствуют длинам интервалов времени между соседними приложениями к изделию ударных воздействий. Случайные величины $\tau_i\ ,\ i = 2, 3, 4, \cdots$ – независимы в совокупности и распределены с одной и той же функцией распределения $F(t)$, где $F_i(t) = P(\tau_i \leq t)$.

Заметим, если случайная величина равна $\tau_1 = t_1$, то возможно, что для нее будет выполняться $F_1(t) \neq F(t) = P(\tau_1 \leq t)$, следовательно, величина τ_1 распределена иначе, чем все остальные величины τ_i. Таким образом, последовательность неотрицательных взаимно независимых случайных величин $\{\tau_i, i \geq 1\}$ полностью характеризуется функциями распределения $F(t)$ и $F_1(t)$.

В моменты времени $t_i, i \geq 1$ к изделию прилагаются ударные воздействия (удары), и в эти же моменты происходит скачкообразное изменение повреждения, проявляющееся в скачкообразном росте нагрузки. Каждое такое изменение нагрузки будем обозначать через θ_i – случайную неотрицательную величину, равную приращению (увеличению) значения нагрузки (износу изделия) в результате воздействия i – го ударного возмущения, $i = 1, 2, 3, \cdots$.

Относительно случайных величин θ_i естественно предполагать, что они также независимы в совокупности, а также то, что они распределены с одной и той же функцией распределения $G(y)$, следовательно, для них будет выполняться условие $G_1(y) = G_2(y) = \cdots = G(y)$, где $G_i(y) = P(\theta_i \le y)$. Полагаем, что в промежутке между двумя соседними ударными воздействиями значение нагрузки, приложенной к изделию, не будет изменяться. Отметим, что величина θ_0 независима от последовательности случайных величин $\{\tau_i, i \ge 1\}$. В [3] отмечается, что описанный выше процесс функционирования изделия описывается ВСФИ-распределением, которое характеризуется возрастанием в среднем функции интенсивности.

Обозначим теперь через χ_t значение прочности в момент времени t. Случайный процесс $\{\chi_t\}_{t\ge 0}$ изменения прочности будем представлять монотонно убывающей линейной случайной функцией вида

$$\chi_t = \chi_0 - X_t,$$

где $\{\chi_t\}_{t\ge 0}$ – стохастический процесс, обладающий свойством $t = 0$, χ_0 – начальное значение, которое может быть и не случайным. Предположим, что $X_t = Vt$, V – скорость изменения прочности, тогда математическое ожидание и дисперсия линейной случайной функции χ_t будет определяться следующим образом

$$M\chi_t = M(\chi_0 - tV) = M\chi_0 - tMV,\ M(\chi_t - M\chi_t) = 0,$$

$$M(\chi_t - M\chi_t)^2 = D\chi_0 + t^2 DV - 2tM\chi_t MV,$$

$$M(\chi_t - M\chi_t)^3 = M(\chi_0 - M\chi_0)^3 + t^2 M(V - MV)^3,$$

где $M\chi_0$, MV, $D\chi_0$, DV – математические ожидания и дисперсии начального значения и скорости изменения прочности соответственно. Здесь и далее будем предполагать, что случайные величины χ_0 и V независимы. Одномерную функцию распределения процесса $\{\chi_t\}_{t\ge 0}$ будем обозначать

$$F_\chi^t(x) = P(\chi_t \le x).$$

Описанный выше случайный процесс называется веерным, и все его реализации имеют общую случайную точку $(M\chi_0, 0)$ [9]. Относительно функции $F_\chi(y)$ будем требовать, чтобы она удовлетворяла всем свойствам функции распределения.

Если рассматривать традиционную модель надежности “нагрузка – прочность”, то вероятность безотказной работы изделия не зависит от времени, т.к. предполагается, что изделие испытывает статическое воздействие в процессе эксплуатации.

Нашей задачей является получение показателей безотказности и долговечности изделия, к которому прилагаются случайные возмущения в процессе его эксплуатации, при случайной его прочности.

Формализация и решение задачи

Динамику определяющего параметра работоспособности изделия, функционирующего в условиях воздействия ударных нагрузок, можно представить графически (рис. 1). Предполагается, что изделие прекращает работать, как только накопленные повреждения превысили заданный уровень прочности, значение которого ограничено случайной функцией $\chi_t = \chi_0 - X_t$, (см. рис. 1).

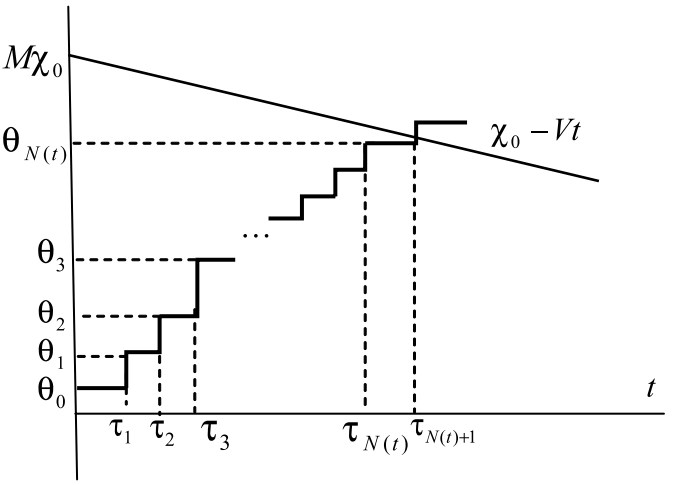


Рис.1. Графическое представление процесса функционирования в условиях воздействия ударных нагрузок

Именно учет случайных воздействий позволяет вводить в рассматриваемую модель зависимость от времени. В итоге традиционная статическая модель надежности "нагрузка – прочность" становится динамической моделью.

Нетрудно увидеть, что поскольку к изделию прикладывается все возрастающая нагрузка L_t, $t \geq 0$, то ее можно определить равенством

$$L_t = \begin{cases} \sum_{i=1}^{N_1(t)} \theta_i, & N_1(t) = 1, 2... \\ 0, & N_1(t) = 0 \end{cases}. \qquad (1)$$

Величина L_t имеет смысл полного накопленного повреждения изделием за время функционирования t. Определенный таким способом стохастический процесс $\{L_t\}_{t>0}$ называют кумулятивным. Суммирование здесь ведется по всем ударным воздействиям, которые случились до момента времени t включительно. Обозначим через $N_1(t) = N_t$ число восстановлений считающего процесса восстановления $\{N_1(t)\}_{t>0}$ соответствующего процессу $M\chi_t = M(\chi_0 + tV) = M\chi_0 + tMV$. Следовательно, $N_1(t) = N_t$ есть случайное число ударных воздействий за время $(0, t]$ или число циклов восстановления процесса $\{\tau_i, i \geq 1\}$, математическое ожидание от которого есть функция восстановления $H_1(t) = MN_1(t)$.

Ввиду того, что процесс $\{L_t\}_{t>0}$ – ступенчато возрастающий и его реализации – ступенчатые функции, то задавая допустимую границу (прочность), в нашем случае $\chi_t = \chi_0 - X_t$, можно вычислять соответствующие показатели надежности и долговечности.

Не останавливаясь более на описании процесса эволюции изделия, подверженного случайным периодическим воздействиям, введем дополнительные, но необходимые для дальнейшего изучения обозначения и определения.

Будем предполагать, что ударные возмущения имеют случайный характер, т.е. они прилагаются к изделию в случайные моменты времени и имеют случайную амплитуду. Каждое возмущение приводит к уменьшению прочности или можно утверждать, что каждое воздействие приводит к увеличению нагрузки на некоторую случайную величину, описываемую соответствующей функцией распределения. Таким образом, рассматривается случайный процесс накопления, в котором

изменение нагрузки является ступенчато возрастающим стохастическим процессом и отказ изделия наступает, как только указанный процесс пересечет границу (см. рис. 1), которая здесь является случайной величиной и, более того, случайным процессом (веерным).

При вычислении характеристик безотказности и долговечности изделия будем использовать результаты, полученные для случая детерминированной прочности изделия [10].

В дальнейшем будем учитывать то, что процесс $\{L_t\}_{t>0}$ есть простой процесс восстановления, порожденный функциями распределения $F_1(t)$, $F(t)$. Это упрощающее предположение легко обобщается на случай запаздывающего процесса восстановления. Нетрудно убедиться, что для получения вероятности безотказной работы изделия за время t, может быть использовано одно из записанных соотношений для вероятности $P(L_t \le \mathrm{x})$ [3]. Используя условие отказа изделия, а также формулу полной вероятности вычисляем условную вероятность того, что накопленная нагрузка не превосходит величину прочности изделия за время функционирования t, которую запишем так

$$P\left(L_t \le x\right) = MJ_{\sum_{i=1}^{N_1(t)} \theta_i \le x} = \sum_{k=0}^{\infty} \left(MJ_{\sum_{i=1}^{N_1(t)} \theta_i \le x} \Big|_{N_1(t)=k} \right) P(N_1(t)=k) = \sum_{k=0}^{\infty} \left(MJ_{\sum_{i=1}^{k} \theta_i \le x} \right) P(N_1(t)=k) =$$

$$= \sum_{k=0}^{\infty} G^{*(k)}(x) P(N_1(t)=k) = \sum_{k=0}^{\infty} G^{*(k)}(x) \left(F^{*(k)}(t) - F^{*(k+1)}(t) \right).$$

Поскольку в рассматриваемой модели прочность случайная величина, то используя формулу условного математического ожидания от случайной функции $P(L_t \le \mathrm{x})$, получаем вероятность безотказной работы изделия $P(t)$ за время t. Тогда

$$P(t) = \int_0^{\infty} P(L_t \le \mathrm{x}) dF_{\chi_t}(x) = \int_0^{\infty} \sum_{k=0}^{\infty} P(N_1(t)=k) G^{*(k)}(x) dF_{\chi_t}(x) =$$

$$= \sum_{k=0}^{\infty} P(N_1(t)=k) \int_0^{\infty} G^{*(k)}(x) dF_{\chi_t}(x) = \sum_{k=0}^{\infty} P(N_1(t)=k) C(k) = \sum_{k=0}^{\infty} C(k) P_k(t) = MC(N_1(t)), \quad (2)$$

где $C(k) = \int_0^{\infty} G^{*(k)}(x) dF_{\chi_t}(x) = MG^{*(k)}(\chi_t)$.

Отметим, что соотношение (2) – это функция распределения накопленной нагрузки за время t.

Аналогично введем второй процесс восстановления $\{Z_x\}_{x>0}$, связанный со временем функционирования изделия формулой (см. рис. 1)

$$Z_x = \begin{cases} \sum_{i=1}^{N_2(x)} \tau_i + \tau_t, & N_2(x) = 1, 2, \cdots \\ 0, & N_2(x) = 0 \end{cases},$$

где Z_x – случайная наработка при заданной допустимой нагрузке x. Здесь $N_2(x) = N_x$ – число циклов восстановления до исчерпания запаса прочности процессом накопления нагрузки. Математическое ожидание от случайной величины $N_2(x)$ также есть функция восстановления, обозначим её как $H_2(x) = MN_2(x)$. Величина $\sum_{i=0}^{N_2(x)} \tau_i + \tau_t$ – случайная наработка изделия до пересечения накопленной нагрузкой уровеня прочности χ_t, где τ_t – обратное остаточное время, это время в течение которого изделие функционировало исправно после последнего ударного воздействия. Условную функцию распределения наработки на отказ изделия запишем, используя формулу полной вероятности

$$P(Z_x \le t) = MJ_{\sum_{i=1}^{N_2(x)} \tau_i + \tau_t \le t} = \sum_{k=0}^{\infty} \left(MJ_{\sum_{i=1}^{N_2(x)} \tau_i + \tau_t \le t} \Big|_{N_2(x)=k} \right) P\left(N_2(x) = k\right) =$$

$$= \sum_{k=0}^{\infty} P\left(\sum_{i=1}^{N_2(x)} \tau_i + \tau_t \le t \Big|_{N_2(x)=k} \right) P\left(N_2(x) = k\right) = \sum_{k=0}^{\infty} F_t * F^{*(k)}(t) P\left(N_2(x) = k\right),$$

где $F_t(t)$ – функция распределения обратного остаточного времени τ_t [3].

Вычисляя математическое ожидание от записанного выше соотношения, получаем функцию распределения времени наработки на отказ изделия:

$$Q(t) = \int_0^{\infty} P(Z_x \le \mathrm{t}) dF_{\chi_t}(x) = \int_0^{\infty} \sum_{k=0}^{\infty} F_t * F^{*(k)}(t) P(N_2(x) = k) dF_{\chi_t}(x) =$$

$$= \sum_{k=0}^{\infty} F_t * F^{*(k)}(t) \int_0^{\infty} (G^{*(k)}(x) - G^{*(k+1)}(x)) dF_{\chi}(x). \qquad (3)$$

Функция $Q(t)$ является вероятностью отказа изделия за время функционирования t, следовательно $Q(t) + P(t) = 1$. Подынтегральное выражение (3) $G^{*(k)}(x) - G^{*(k+1)}(x) = P\left(\sum_{i=1}^{k} \theta_i < x < \sum_{i=1}^{k+1} \theta_i \right)$ – вероятность того, что отказ произошел между k и $k+1$-м ударным воздействием.

Нетрудно увидеть, что соотношения (3) и (2) есть смесь функций распределения $F^{*(k)}(t)$ и $G^{*(k)}(x)$ с весами $g_2(x) = G^{*(k)}(x) - G^{*(k+1)}(x)$ и $g_1(t) = F^{*(k)}(t) - F^{*(k+1)}(t)$ соответственно. Важным является то, что распределение наработки принадлежит классу ВСФИ при любой функции распределения $G(t)$.

Видно, что дальнейшие аналитические преобразования соотношения (2), (3) в общем виде не представляются возможными. При решении задач, в которых необходимо вычислять многочисленные свертки функций, обычно используются преобразования Лапласа или производящие функции, а затем возникает необходимость обращать полученное преобразование. Отметим, что задача обращения преобразования Лапласа, как правило, имеет тот же порядок трудности, что и решение исходной задачи. Трудность решения исходной задачи заключается в том, что для получе-

ния в удобном виде необходимых вероятностей требуется последовательно вычислить: во-первых, математическое ожидание от i –кратной свертки функции $G(x)$ или $F(t)$ в зависимости от рассматриваемой задачи, и во-вторых, повторно математическое ожидание от полученного результата.

Рассмотрим частный случай кумулятивного процесса – процесс ударных нагрузок, для этого предположим, что случайные величины τ и $\chi_t = \chi$ экспоненциально распределены, т.е. $F(t) = 1 - e^{-\lambda t}$ и $F_\chi(x) = 1 - e^{-\nu x}$, где λ – интенсивность потока ударных нагрузок, а $\nu = 1/M\chi$ – интенсивность изменения прочности. В таком предположении последовательность случайных величин τ_i образует пуассоновский поток событий, а из предположения $V = 0$ следует, что пересечение уровня прочности определяющим параметром происходит только в моменты воздействия ударных нагрузок. Поскольку случайные процессы $\{L_t\}_{t>0}$, $\{Z_x\}_{x>0}$ одновременно претерпевают изменения (см. рис. 1), то это позволяет их рассматривать как синхронные процессы.

Перепишем (2) с учетом сделанных предположений. Учитывая, что поток ударных воздействий образует пуассоновский процесс, для которого $P(N_t = k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}$, имеем

$$P(t) = \int_0^\infty P(L_t \le \mathrm{x}) dF_{\chi_t}(x) = \int_0^\infty \sum_{k=0}^\infty P(N_t = k) G^{*(k)}(x) dF_{\chi_t}(x) =$$

$$= \sum_{k=0}^\infty e^{-\lambda t} \frac{(\lambda t)^k}{k!} \int_0^\infty G^{*(k)}(x) dF_{\chi_t}(x) = 1 - \sum_{k=0}^\infty e^{-\lambda t} \frac{(\lambda t)^k}{k!} \int_0^\infty F_{\chi_t}(x) dG^{*(k)}(x) =$$

$$= \sum_{k=0}^\infty e^{-\lambda t} \frac{(\lambda t)^k}{k!} \int_0^\infty \overline{F}_{\chi_t}(x) dG^{*(k)}(x).$$

Замечая, что интеграл этого соотношения следует рассматривать как преобразование Лапласа–Стилтьеса $\tilde{G}(\nu) = \int_0^\infty e^{-\nu x} G(x) dx = M e^{-\nu\theta}$ функции $G^{*(k)}(x)$, поскольку $\overline{F}_{\chi_t}(x) = e^{-\nu x}$ при экспоненциальном законе распределения случайной величины χ_t, то

$$P(t) = \sum_{k=0}^\infty e^{-\lambda t} \frac{(\lambda t)^k}{k!} \int_0^\infty e^{-\nu x} dG^{*(k)}(x) = \sum_{k=0}^\infty e^{-\lambda t} \frac{(\lambda t)^k}{k!} \left(\tilde{G}(\nu)\right)^k =$$

$$= \sum_{k=0}^\infty e^{-\lambda t} \frac{\left(\lambda t \tilde{G}(\nu)\right)^k}{k!} = e^{-\lambda t (1 - M e^{-\nu\theta})}. \qquad (4)$$

Аналогично (2) вычислим функцию распределения накопленной нагрузки за время t, используя соотношение (3) в предположении, что процесс функционирования изделия есть процесс ударных нагрузок. При общих предположениях функция распределения накопленной нагрузки за время t определяется так

$$P(t) = \sum_{k=0}^\infty F' * F^{*(k)}(t) \int_0^\infty (G^{*(k)}(x) - G^{*(k+1)}(x)) dF_\chi(x),$$

где $F_t(x)$ – функция распределения обратного остаточного времени τ_t.

С целью дальнейшего упрощения полученного соотношения для $P(t)$ перепишем фигурирующий интеграл в этом соотношении так

$$\int_0^\infty (G^{*(k)}(x) - G^{*(k+1)}(x))dF_\chi(x) = \int_0^\infty \left(P\left(\sum_{i=1}^{k}\theta_i \le x\right) - P\left(\sum_{i=1}^{k+1}\theta_i \le x\right)\right)dF_\chi(x) =$$

$$= \int_0^\infty \overline{F}_\chi(x)d\left\{P\left(\sum_{i=1}^{k}\theta_i \le x\right) - P\left(\sum_{i=1}^{k+1}\theta_i \le x\right)\right\}.$$

Учитывая, что величина $\chi_t = \chi$ экспоненциально распределена с параметром ν, т.е. $F_\chi(x) = 1 - e^{-\nu x}$, и вычисляя преобразование Лапласа–Стилтьеса функции $P\left(\sum_{i=1}^{k}\theta_i \le x\right) - P\left(\sum_{i=1}^{k+1}\theta_i \le x\right)$ рассматриваемый интеграл перепишем еще раз:

$$\int_0^\infty (G^{*(k)}(x) - G^{*(k+1)}(x))dF_\chi(x) =$$

$$= \int_0^\infty e^{-\nu x}d\left\{P\left(\sum_{i=1}^{k}\theta_i \le x\right) - P\left(\sum_{i=1}^{k+1}\theta_i \le x\right)\right\} = Me^{-\nu k\theta} - Me^{-\nu(k+1)\theta} = Me^{-\nu k\theta}(1 - Me^{-\nu\theta}).$$

Поскольку процесс ударных воздействий является процессом Пуассона, который обладает свойством отсутствия последействия, то в силу этого замечательного свойства случайная величина τ_t имеет то же распределение, что и величина τ. Учитывая свертки функций $F(t)$, перепишем вероятность $P(t)$ следующим образом:

$$P(t) = \sum_{k=0}^{t} F^{*(k+1)}(t)Me^{-\nu k\theta}(1 - Me^{-\nu\theta}).$$

Выполняя преобразование Лапласа–Стилтьеса функции $F(t)$, перепишем

$$\tilde{P}(s) = \frac{(1 - Me^{-\nu\theta})\tilde{F}(s)}{1 - \tilde{F}(s)Me^{-\nu\theta}}.$$

Учитывая, что $\tilde{F}(s) = \int_0^\infty e^{-st}dF(t) = \frac{\lambda}{\lambda + s}$ для экспоненциального закона распределения случайной величины τ, $\tilde{P}(s)$ перепишем так

$$\tilde{P}(s) = \frac{1 - Me^{-\nu\theta})\frac{\lambda}{\lambda + s}}{1 - \frac{\lambda}{\lambda + s}Me^{-\nu\theta}} = \frac{\lambda(1 - Me^{-\nu\theta})}{s + \lambda(1 - Me^{-\nu\theta})}.$$

Отсюда получаем окончательное выражение для функции распределения накопленной нагрузки за время t, которое запишем, используя теорему о вычетах

$$Q(t) = 1 - e^{-\lambda t(1-Me^{-\nu\theta})} = 1 - e^{-\lambda t} e^{\lambda t M e^{-\nu\theta}} . \quad (5)$$

Если предположить, что функция $G(x) = 1 - e^{-\mu x}$, то $Q(t) = 1 - e^{-\lambda t \frac{\nu}{\mu+\nu}}$, а $P(t) = e^{-\lambda t \frac{\nu}{\mu+\nu}}$.

Вычислим теперь другие показатели надежности, например, интенсивность отказов изделия.

Интенсивность отказов изделия

Используя (2), получим соотношение для интенсивности отказов $\Lambda(t)$ изделия, на которое воздействует последовательность ударных нагрузок. Из определения интенсивности отказов $\Lambda(t)$ запишем так

$$\Lambda(t) = \frac{\sum_{k=0}^{\infty} f^{*(k+1)}(t) \int_0^{\infty} (G^{*(k)}(x) - G^{*(k+1)}(x)) dF_{\chi}(x)}{\sum_{k=0}^{\infty} \int_0^{\infty} G^{*(k)}(x) dF_{\chi}(x) (F^{*(k)}(t) - F^{*(k+1)}(t))},$$

где плотность распределения $f^{*(k+1)}(t)$ определяется последовательным интегрированием $f^{*(k+1)}(t) = \int_0^t f^{*(k)}(t-x) f(x) dx$, где $f(t) = \frac{dF(t)}{dt}$.

Ввиду того, что дальнейшие аналитические упрощения записанного соотношения интенсивности отказов $\Lambda(t)$ невозможны, то опять предполагаем, что имеет место процесс ударных нагрузок, для которого величины τ и $\chi_t = \chi$ являются экспоненциально распределенными случайными величинами, тогда

$$f^{*(k+1)}(t) = \lambda \frac{(\lambda t)^k}{k!} e^{-\lambda t} .$$

Учитывая сделанные предположения и подставляя плотность распределения $f^{*(k+1)}(t)$ в соотношение для интенсивности отказов $\Lambda(t)$ изделия, имеем

$$\Lambda(t) = \frac{\sum_{k=0}^{\infty} \lambda \frac{(\lambda t)^k}{k!} e^{-\lambda t} \left(\tilde{G}(\nu)\right)^k (1 - \tilde{G}(\nu))}{\sum_{k=0}^{\infty} \left(\tilde{G}(\nu)\right)^k e^{-\lambda t} \frac{(\lambda t)^k}{k!}} = \lambda(1 - \tilde{G}(\nu)). \quad (6)$$

Соотношение (6) можно получить непосредственно из (5) и (4). Таким образом, получен несколько неожиданный результат – интенсивность отказов «стареющего» изделия не зависит от времени.

Поскольку траектории процесса функционирования изделия – это ступенчатая функция, то и время до отказа является дискретной случайной величиной, поэтому для оценки интенсивности отказов изделия можно использовать ее дискретный аналог ([2] с. 35). Используя ранее полученное, имеем

$$\lambda_{k+1} = \frac{MG^{*(k+1)}(\chi_t)}{\sum_{i=k}^{\infty} MG^{*(i+1)}(\chi_t)} = \frac{\left(\tilde{G}(\nu)\right)^{k+1}(1-\tilde{G}(\nu))}{\sum_{i=k}^{\infty}\left(\tilde{G}(\nu)\right)^{i+1}(1-\tilde{G}(\nu))} = \frac{\left(\tilde{G}(\nu)\right)^{k+1}}{\sum_{i=k}^{\infty}\left(\tilde{G}(\nu)\right)^{i+1}} = 1-\tilde{G}(\nu),$$

где λ_{k+1} представляет вероятность того, что изделие, исправное после k -го удара, откажет после $k+1$ -го. В случае, когда $G(x) = 1-e^{-\mu x}$, тогда $\lambda_{k+1} = \frac{\nu}{\nu+\mu}$, $\lambda_{k+1} \le 1$.

Таким образом, предположения об экспоненциальных распределениях потока ударных нагрузок и величины прочности позволили, исходя из математической модели надежности изделия, функционирующего в условиях многократных воздействий ударных возмущений, получить в явном виде количественные показатели надежности изделия, необходимые для инженерной практики. Конечные соотношения показателей надежности просты, что делает их привлекательными для практического использования.

Литература

1. **Богданофф Дж., Козин Ф.** Вероятностные модели накопления повреждений: Пер. с англ. – М.: Мир, 1989. – 334 с.

2. **Барлоу Р., Прошан Ф.** Математическая теория надежности: Пер. с англ. – М.: Сов. Радио, 1969.– 488 с.

3. **Байхельт Ф., Франкен П.** Надежность и техническое обслуживание. Математический подход: Пер. с нем. – М.: Радио и связь, 1988. – 392 с.

4. **Капур К., Ламберсон Л.** Надежность и проектирование систем: Пер. с англ. – М.: Мир, 1980. – 604 с.

5. **Дилон Б., Сингх Ч.** Инженерные методы обеспечения надежности систем: Пер. с англ. – М.: Мир, 1984. – 318 с.

6. **Гихман И.И., Скороход А.В.** Теория случайных процессов. – М.: Наука, 1973, том. 2. С. 398 -399.-640 с.

7. **Перегуда А.И., Андреев А.Г.** Асимптотический метод вычисления показателей надежности и долговечности изделий, функционирующих в условиях ударных нагрузок. – Надежность, 2007, №3 (22) – С. 45-53.

8. **Toshio Nakagawa.** Shock and damage models in reliability theory. – Springer – Verlag London Limited 2007. – 191

9. **Дружинин Г.В.** Надежность автоматизированных систем. – М.: Энергия, 1977. – 535 с.

10. **Перегуда А.И., Соборова И.А., Андреев А.Г.** Об одном методе построения двухсторонних оценок показателей надежности и долговечности изделий, функционирующих в условиях ударных нагрузок. – Надежность, 2005, №2 (13) – С. 14-24.

Pereguda A.I.

MATHEMATICAL MODEL OF THE RELIABILITY OF A PRODUCT SUBJECT TO IMPACT STRESS

The paper considers a mathematical model of reliability in view of a product's load accumulation caused by cyclic impact loads. Study of the process when accumulated stress crosses a random level of endurance under repeated impact disturbances allowed us to obtain a mathematical model that makes it possible to calculate reliability and durability parameters. The obtained final relations for reliability parameters have a simple form, which can be used in practical calculations.

Keywords: *damage accumulation, impact load, distribution of sums of random variables, reliability parameter, durability, estimated mean, impact, crossings of the level.*

Introduction

During the process of maintenance of products, aging of material occurs under the influence of factors such as increased temperature and pressure, cyclic loads, presence of corrosive environment, which leads, for example, to fatigue crack growth. By now, physical processes leading to equipment failure has been well studied by fracture mechanics and mechanics of materials.

[1] states that so far the behavior of structural materials under operating conditions has not been studied well enough to provide the basis for model justification of cumulative damages according to the fundamental physical laws. Obviously, these problems can be solved without quantitative assessment of reliability using the experience of maintenance of such devices in the same or similar production areas. However, such solution of the task without a rigorous mathematical analysis of operation processes and quantitative estimates of reliability and durability by no means can be considered well founded.

A product's operation process in question, which is affected by impact loads, can be regarded as a process with aging. [2] introduced the concept of aging based on time behavior of a failure rate function. In particular, it identified an increasing rate function IRF and a decreasing rate function DRF. It was also shown that if a system consists of independent elements with IRF time-to-failure distribution, then a distribution emerges that has a rate function increasing in the mean RFIM.

Often one can get information about a growing aging of devices considering the dynamics of certain parameters. Knowledge of indicators of the parameter changing process allows us to find the distribution of a device's MTBF, which in turn makes it possible to determine the time to stop a device's maintenance

until its complete destruction and recovery of its properties. Naturally, during operation of such systems, the issues of quantitatively assessing reliability and durability parameters and afterwards the task of scheduling the time to stop a product's maintenance arise [3].

To date, mathematical models of the reliability of products, which are opposed to static loads, and the methods of obtaining relevant indicators have been satisfactorily developed [4, 5]. If, in addition to static loads, the product is opposed to the load, which has a random amplitude and random oscillation period, mathematical models for describing the operation of such products are very cumbersome, and to obtain quantitative values for corresponding reliability and durability parameters based on their analysis is generally impossible. The process of operation of such products is described by Ito's stochastic differential equation with a discrete constituent [6]. [7] considered the asymptotic method for calculating life indicators of a product, which is opposed to impact loads and showed that such process is a process with independent increments.

Studies of processes of load accumulation are given in [8], where also the optimization of preventive maintenance according to the criterion of minimum expected cost is analyzed.

This paper will study the mathematical model of operation reliability of a product, which is affected by impact loads provided that endurance is a fan random process.

Let us immediately come to the definition of the mathematical problem of determining dependability and durability parameters, using a mathematical model of a product's evolution based on the theory of random processes of accumulation.

Problem definition

We shall consider a product subject to wear due to a number of applied pulse impacts. These can be jolts, shocks, temperature and pressure pulsations, vibrations, etc. From now on, without specifying the physical nature of impacts on a product, we will call pulse actions as impact (cyclic) loads. Let the change in parameters of a product be caused by impact loads (jolts, shocks, pulses), occurred at times t_0, t_1, $t_2, \cdots$, $t_{k+1} \geq t_k$, $k \geq 1$. Denote $\tau_i = t_{i+1} - t_i$, $i > 0$, $t_0 = 0$, where τ_i is random variables equal to the length of time intervals between successive impact applications to a product. Random variables τ_i, $i = 2, 3, 4, \cdots$ are independent and distributed with the same distribution function $F(t)$, where $F_i(t) = P(\tau_i \leq t)$.

It should be noted that if a random variable is equal to $\tau_1 = t_1$, it is possible that $F_1(t) \neq F(t) = P(\tau_1 \leq t)$ will be true for it, therefore, the quantity τ_1 I is distributed differently than all other values τ_i. Thus, the sequence of non-negative mutually independent random variables $\{\tau_i, i \geq 1\}$ is completely characterized by distribution functions $F(t)$ and $F_1(t)$.

As at time points $t_i, i \geq 1$ the product is opposed to shock effects (impacts), at the same moments there is a stepwise change of damage manifested in the abrupt increase of load. Each such change will be denoted as θ_i, a non-negative random variable equal to increment (increase) of load value (product wear) as a result of the effect of the *i*-th impact disturbance, $i = 1, 2, 3, \cdots$.

As regards the random variables θ_i, it is natural to assume that they are also independent, as well as they are distributed with the same distribution function $G(y)$, and therefore, we have the following condition for them $G_1(y) = G_2(y) = \cdots = G(y)$, where $G_i(y) = P(\theta_i \leq y)$. We suppose that between times of two successive shocks the value of the load applied to the product will not change. Note that the value θ_0 is independent on the sequence of random variables $\{\tau_i, i \geq 1\}$. The study [3] notes that the process of product operation described above is defined by RFIM distribution, which is characterized by a rate function increasing in the mean.

Now let us denote the endurance value at time point t as χ_t. We shall represent the random process $\{\chi_t\}_{t\geq 0}$ of endurance changing as a monotonically decreasing linear random function in the following form

$$\chi_t = \chi_0 - X_t,$$

where $\{\chi_t\}_{t\geq 0}$ is a stochastic process with the property $t = 0$, χ_0 is the initial value, which may be not random. Suppose that $X_t = Vt$, V is the speed of endurance changing, then the expectation and the dispersion of a linear random function will be defined as follows

$$M\chi_t = M(\chi_0 - tV) = M\chi_0 - tMV,\ M(\chi_t - M\chi_t) = 0,$$

$$M(\chi_t - M\chi_t)^2 = D\chi_0 + t^2 DV - 2tM\chi_t MV,$$

$$M(\chi_t - M\chi_t)^3 = M(\chi_0 - M\chi_0)^3 + t^2 M(V - MV)^3,$$

where $M\chi_0$, MV, $D\chi_0$, DV are expectations and dispersions of the initial value and the speed of endurance changing, respectively. Hereafter, we will assume that the random variables are independent. A one-dimensional distribution function of the process $\{\chi_t\}_{t\geq 0}$ will be denoted as

$$F_\chi^t(x) = P(\chi_t \leq x).$$

The random process described above is called as a fan process, and all its implementations have a common random point $(M\chi_0, 0)$ [9]. Regarding the function $F_\chi(y)$, we shall require that it should meet all of the properties of a distribution function.

If we consider the traditional model of reliability "load – endurance", then the probability of failure-free operation of a product is independent from time, since it is assumed that the product is subject to static impacts in the process of operation.

Our objective is to obtain reliability and durability parameters of a product, which is opposed to random disturbances during its operation, with its random endurance.

Formalization and solution of the problem

The dynamics of a key parameter of product availability operating under conditions of impact loads can be represented graphically (Fig. 1). It is assumed that a product stops working as soon as the accumulated damages exceed the specified level of endurance, the value of which is limited by the random function $\chi_t = \chi_0 - X_t$, (see Fig. 1).

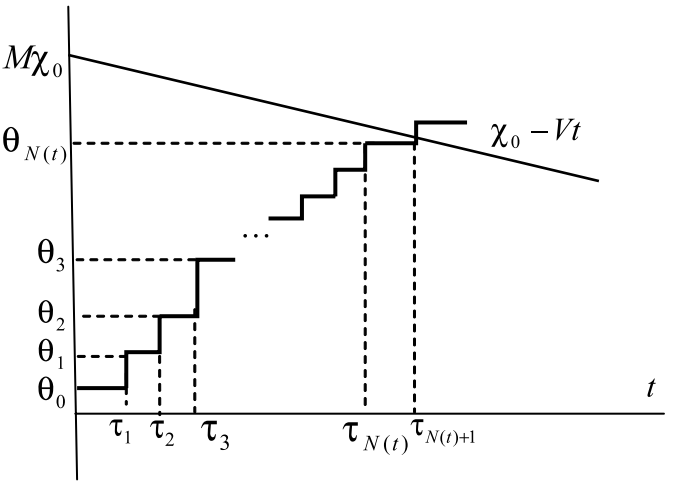


Fig.1. Graphical representation of operation process under conditions of impact loads

It is the accounting of random actions that allows us to introduce time dependence in this model. As a result, a traditional static model of reliability "load – endurance" becomes a dynamic model.

It is easy to see that since a product is opposed to an increasing load $L_t \;\; t \geq 0$, it can be defined by the following equality

$$L_t = \begin{cases} \sum_{i=1}^{N_1(t)} \theta_i, & N_1(t) = 1, 2... \\ 0, & N_1(t) = 0 \end{cases}. \qquad (1)$$

The value L_t means the accumulated damage to a product during operation *t*. A stochastic process defined in this way is called cumulative. Here, the summing is made for all impact loads, which have occurred up to the time *t* inclusive. We shall denote as $N_1(t) = N_t$ the number of renewals of recovery counting process $\{N_1(t)\}_{t>0}$, corresponding to the process $M\chi_t = M(\chi_0 + tV) = M\chi_0 + tMV$. Therefore, $N_1(t) = N_t$ is a random number of impact loads over time $(0, t]$ or is the number of cycles of recovery process $\{\tau_i, i \geq 1\}$, the expectation of which is a function of recovery $H_1(t) = MN_1(t)$.

In view of the fact that the process $\{L_t\}_{t>0}$ is stepwise increasing and its implementations are stepwise functions, then specifying the acceptable limit (endurance), in our case $\chi_t = \chi_0 - X_t$, we can calculate the appropriate reliability and durability indices.

Then we shall introduce additional, but necessary notations and definitions for a further study without going over description of the evolution of a product subject to periodic random effects.

We shall assume that impact disturbances are random, i.e. they are applied to a product at random time points and have random amplitude. Each disturbance leads to decrease in endurance, or it can be assumed that every action leads to increase of load on some random value described by a relevant distribution function. Thus, the random process of accumulation, in which load change is a stepwise increasing stochastic process, and a product's failure occurs only when this process crosses the border (see Fig. 1), which is a random variable, and moreover, a random process (fan shaped).

We shall use the results obtained for the case of deterministic endurance of a product in the calculation of the characteristics of product reliability and durability [10].

Further we shall consider that the process $\{L_t\}_{t>0}$ is a simple process of recovery generated by distribution functions $F(t)$, $F_1(t)$. This simplifying assumption is easily generalized to the case of a delayed recovery. It is easy to receive evidence that to obtain the probability of failure-free operation of a product over time *t*, one of the recorded relations for the probability $P(L_t \le \mathrm{x})$ can be used [3]. Using the condition of a product failure, and the total probability formula we shall calculate the conditional probability that the cumulative load does not exceed the endurance of the product during operation, which we write as

$$P\left(L_t \le x\right) = MJ_{\sum_{i=1}^{N_1(t)} \theta_i \le x} = \sum_{k=0}^{\infty} \left(MJ_{\sum_{i=1}^{N_1(t)} \theta_i \le x} \Big|_{N_1(t)=k} \right) P(N_1(t)=k) = \sum_{k=0}^{\infty} \left(MJ_{\sum_{i=1}^{k} \theta_i \le x} \right) P(N_1(t)=k) =$$

$$= \sum_{k=0}^{\infty} G^{*(k)}(x) P(N_1(t)=k) = \sum_{k=0}^{\infty} G^{*(k)}(x) \left(F^{*(k)}(t) - F^{*(k+1)}(t) \right).$$

Since the endurance is a random variable in the considered model, then using the formula of conditional expectation of a random function $P(L_t \le \mathrm{x})$, we obtain the probability of failure-free operation of a product over time. Then

$$P(t) = \int_0^{\infty} P(L_t \le \mathrm{x}) dF_{\chi_t}(x) = \int_0^{\infty} \sum_{k=0}^{\infty} P(N_1(t)=k) G^{*(k)}(x) dF_{\chi_t}(x) =$$

$$= \sum_{k=0}^{\infty} P(N_1(t)=k) \int_0^{\infty} G^{*(k)}(x) dF_{\chi_t}(x) = \sum_{k=0}^{\infty} P(N_1(t)=k) C(k) = \sum_{k=0}^{\infty} C(k) P_k(t) = MC(N_1(t)), \quad (2)$$

where $C(k) = \int_0^{\infty} G^{*(k)}(x) dF_{\chi_t}(x) = MG^{*(k)}(\chi_t)$.

It should be noted that relation (2) is a distribution function of the accumulated load over time *t*.

Similarly, we introduce the second recovery process $\{Z_x\}_{x>0}$ associated with the time function of a product by the following formula (see Fig. 1)

$$Z_x = \begin{cases} \sum_{i=1}^{N_2(x)} \tau_i + \tau_t, & N_2(x) = 1, 2, \cdots \\ 0, & N_2(x) = 0 \end{cases}$$

where Z_x is a random time to failure for a given acceptable load *x*. Here $N_2(x) = N_x$ is the number of cycles of recovery until the exhaustion of endurance resources by the process of load accumulation. The expectation of a random variable $N_2(x)$ is also a function of recovery, which we denote as $H_2(x) = MN_2(x)$. The quantity $\sum_{i=0}^{N_2(x)} \tau_i + \tau_t$ is a random mean time between failures of a product before crossing the endurance level χ_t by accumulated load, where τ_t is the reverse residual time, that is the time during which a product operates properly after the last impact. A conditional distribution function of a product's MTBF can be written using the formula of total probability

$$P(Z_x \le t) = MJ_{\sum_{i=1}^{N_2(x)} \tau_i + \tau_t \le t} = \sum_{k=0}^{\infty} \left(MJ_{\sum_{i=1}^{N_2(x)} \tau_i + \tau_t \le t} \Big|_{N_2(x)=k} \right) P\left(N_2(x) = k\right) =$$

$$= \sum_{k=0}^{\infty} P\left(\sum_{i=1}^{N_2(x)} \tau_i + \tau_t \le t \Big|_{N_2(x)=k} \right) P\left(N_2(x) = k\right) = \sum_{k=0}^{\infty} F_t * F^{*(k)}(t) P\left(N_2(x) = k\right).$$

where $F_t(t)$ is the distribution function of the reverse residual time τ_t [3].

Calculating the expectation from a recorded above relation, we obtain the distribution function of a product's MTBF and the distribution of time to a first failure.

$$Q(t) = \int_0^{\infty} P(Z_x \le \mathrm{t}) dF_{\chi_t}(x) = \int_0^{\infty} \sum_{k=0}^{\infty} F_t * F^{*(k)}(t) P(N_2(x) = k) dF_{\chi_t}(x) =$$

$$= \sum_{k=0}^{\infty} F_t * F^{*(k)}(t) \int_0^{\infty} (G^{*(k)}(x) - G^{*(k+1)}(x)) dF_{\chi}(x). \qquad ((3)$$

The function $Q(t)$ is the probability of a product's failure during its operation time *t,* therefore, $Q(t) + P(t) = 1$. The integrand (3) $G^{*(k)}(x) - G^{*(k+1)}(x) = P\left(\sum_{i=1}^{k} \theta_i < x < \sum_{i=1}^{k+1} \theta_i \right)$ is the probability that a failure has occurred between the *k*-th and the *k +1*-th impacts.

It is evident that (3) and (2) are a mixture of distribution functions $F^{*(k)}(t)$ and $G^{*(k)}(x)$ with weights $g_2(x) = G^{*(k)}(x) - G^{*(k+1)}(x)$ and $g_1(t) = F^{*(k)}(t) - F^{*(k+1)}(t)$, respectively. It is important that the distribution of MTBF belongs a class of RFIM with any distribution function $G(t)$.

It is evident that further analytical transformations of (2), (3) in general form are not possible. In solving problems, where it is necessary to calculate numerous convoluted functions, Laplace transforms or generating functions are commonly used, and then there is a need to convert the resulting transformation. It should be noted that the problem of the conversion of a Laplace transform, as a rule, is of the same order of difficulty as the initial problem. The difficulty of solving the initial problem consists in the fact that to get required probabilities in convenient form it is necessary to calculate successively: first, the expectation of time of the i-th convolution function $G(x)$ or $F(t)$, depending on the problem under consideration, and second, the re-calculation of the expectation from the obtained result.

Let us consider the special case of the cumulative process, i.e. the process of impact loads. Let us assume for this that the random variables τ and $\chi_t = \chi$ are exponentially distributed, i.e. $F(t) = 1 - e^{-\lambda t}$ and $F_{\chi}(x) = 1 - e^{-\nu x}$, where λ is the rate of impact loads, and $\nu = 1/M\chi$ is the rate of endurance changes. Under this assumption, the sequence of random variables forms a Poisson flow of events, and from the assumption that $V = 0$ it follows that the crossing of the endurance level by the determining parameter occurs only at moments of impact loads. Since the random processes $\{L_t\}_{t>0}$, $\{Z_x\}_{x>0}$ are changing simultaneously (see Fig. 1), it allows them to be considered as synchronous processes.

Now we rewrite (2) in view of the assumptions made. Taking into account that the rate of impact loads forms a Poisson process, for which $P(N_t = k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}$, we have

$$P(t)=\int_0^\infty P(L_t\le \mathrm{x})dF_{\chi_t}(x)=\int_0^\infty\sum_{k=0}^\infty P(N_t=k)G^{*(k)}(x)dF_{\chi_t}(x)=$$

$$=\sum_{k=0}^\infty e^{-\lambda t}\frac{(\lambda t)^k}{k!}\int_0^\infty G^{*(k)}(x)dF_{\chi_t}(x)=1-\sum_{k=0}^\infty e^{-\lambda t}\frac{(\lambda t)^k}{k!}\int_0^\infty F_{\chi_t}(x)dG^{*(k)}(x)=$$

$$=\sum_{k=0}^\infty e^{-\lambda t}\frac{(\lambda t)^k}{k!}\int_0^\infty \overline{F}_{\chi_t}(x)dG^{*(k)}(x).$$

Noting that the integral of this relationship should be considered as the Laplace-Stieltjes transform $\tilde{G}(\nu)=\int_0^\infty e^{-\nu x}G(x)dx=Me^{-\nu\theta}$ of the function $G^{*(k)}(x)$, since $\overline{F}_{\chi_t}(x)=e^{-\nu x}$ for the exponential distribution of the random variable χ_t, then we have

$$P(t)=\sum_{k=0}^\infty e^{-\lambda t}\frac{(\lambda t)^k}{k!}\int_0^\infty e^{-\nu x}dG^{*(k)}(x)=\sum_{k=0}^\infty e^{-\lambda t}\frac{(\lambda t)^k}{k!})\left(\tilde{G}(\nu)\right)^k=$$

$$=\sum_{k=0}^\infty e^{-\lambda t}\frac{\left(\lambda t\tilde{G}(\nu)\right)^k}{k!}=e^{-\lambda t(1-Me^{-\nu\theta})}. \qquad (4)$$

Similarly to (2), let us calculate the distribution function of the cumulative load for the time *t* using relation (3), assuming that the process of a product's operation is the process of impact loads. Under general assumptions, the distribution function of cumulative load for the time *t* is defined as follows

$$P(t)=\sum_{k=0}^\infty F'*F^{*(k)}(t)\int_0^\infty (G^{*(k)}(x)-G^{*(k+1)}(x))dF_\chi(x),$$

where $F_t(x)$ is the distribution function of the inverse residual time τ_t.

To further simplify the obtained relation for $P(t)$, we shall rewrite the integral appearing in this equation as

$$\int_0^\infty (G^{*(k)}(x)-G^{*(k+1)}(x))dF_\chi(x)=\int_0^\infty\left(P\left(\sum_{i=1}^k\theta_i\le x\right)-P\left(\sum_{i=1}^{k+1}\theta_i\le x\right)\right)dF_\chi(x)=$$

$$=\int_0^\infty \overline{F}_\chi(x)d\left\{P\left(\sum_{i=1}^k\theta_i\le x\right)-P\left(\sum_{i=1}^{k+1}\theta_i\le x\right)\right\}.$$

Given that the quantity $\chi_t=\chi$ is exponentially distributed with the parameter ν, i.e. $F_\chi(x)=1-e^{-\nu x}$ and calculating the Laplace-Stieltjes transform of the function $P\left(\sum_{i=1}^k\theta_i\le x\right)-P\left(\sum_{i=1}^{k+1}\theta_i\le x\right)$, then the integral under consideration can be rewritten again

$$\int_0^{\infty}(G^{*(k)}(x)-G^{*(k+1)}(x))dF_{\chi}(x)=$$

$$=\int_0^{\infty}e^{-\nu x}d\left\{P\left(\sum_{i=1}^{k}\theta_i\le x\right)-P\left(\sum_{i=1}^{k+1}\theta_i\le x\right)\right\}=Me^{-\nu k\theta}-Me^{-\nu(k+1)\theta}=Me^{-\nu k\theta}(1-Me^{-\nu\theta}).$$

Since the process of impacts is a Poisson process, which has the property of no-aftereffect, then in view of this remarkable property the random variable τ_t has the same distribution as the variable τ. Taking into account the convolution functions $F(t)$, we rewrite the probability as follows

$$P(t)=\sum_{k=0}^{t}F^{*(k+1)}(t)Me^{-\nu k\theta}(1-Me^{-\nu\theta}).$$

Performing the Laplace-Stieltjes transform of the function $F(t)$, we shall rewrite

$$\tilde{P}(s)=\frac{(1-Me^{-\nu\theta})\tilde{F}(s)}{1-\tilde{F}(s)Me^{-\nu\theta}}.$$

Taking into consideration that $\tilde{F}(s)=\int_0^{\infty}e^{-st}dF(t)=\frac{\lambda}{\lambda+s}$ for the exponential law of random variable distribution τ, we can rewrite $\tilde{P}(s)$ as

$$\tilde{P}(s)=\frac{1-Me^{-\nu\theta})\frac{\lambda}{\lambda+s}}{1-\frac{\lambda}{\lambda+s}Me^{-\nu\theta}}=\frac{\lambda(1-Me^{-\nu\theta})}{s+\lambda(1-Me^{-\nu\theta})}.$$

Hence, we obtain the final expression for the distribution function of the cumulative load for the time *t*, which we write, using the theorem of residues

$$Q(t)=1-e^{-\lambda t(1-Me^{-\nu\theta})}=1-e^{-\lambda t}e^{\lambda tMe^{-\nu\theta}}. \quad (5)$$

If we assume that the function $G(x)=1-e^{-\mu x}$, then $Q(t)=1-e^{-\lambda t\frac{\nu}{\mu+\nu}}$ and $P(t)=e^{-\lambda t\frac{\nu}{\mu+\nu}}$.

Now we shall calculate other indices of reliability, such as a failure rate of a product.

Failure rate of a product

Using (2), we obtain the relation for the failure rate $\Lambda(t)$ of a product, which is opposed to a sequence of impact loads. $\Lambda(t)$ can be written according to the definition of a failure rate as

$$\Lambda(t) = \frac{\sum_{k=0}^{\infty} f^{*(k+1)}(t) \int_0^{\infty} (G^{*(k)}(x) - G^{*(k+1)}(x)) dF_{\chi}(x)}{\sum_{k=0}^{\infty} \int_0^{\infty} G^{*(k)}(x) dF_{\chi}(x) (F^{*(k)}(t) - F^{*(k+1)}(t))},$$

where the density of distribution $f^{*(k+1)}(t)$ is determined by successive integration of $f^{*(k+1)}(t) = \int_0^t f^{*(k)}(t-x) f(x) dx$, where $f(t) = \frac{dF(t)}{dt}$.

In view of the fact that further analytical simplifications of the written relation of the failure rate $\Lambda(t)$ are not possible, then again, we assume that there is a process of impact loads, for which the quantities τ and $\chi_t = \chi$ are exponentially distributed random variables, then we have

$$f^{*(k+1)}(t) = \lambda \frac{(\lambda t)^k}{k!} e^{-\lambda t}.$$

Considering these assumptions and substituting the density of distribution $f^{*(k+1)}(t)$ in relation to the product failure rate $\Lambda(t)$, we have

$$\Lambda(t) = \frac{\sum_{k=0}^{\infty} \lambda \frac{(\lambda t)^k}{k!} e^{-\lambda t} \left(\tilde{G}(\nu)\right)^k (1 - \tilde{G}(\nu))}{\sum_{k=0}^{\infty} \left(\tilde{G}(\nu)\right)^k e^{-\lambda t} \frac{(\lambda t)^k}{k!}} = \lambda (1 - \tilde{G}(\nu)). \quad (6)$$

Equation (6) can be obtained directly from (5) and (4). Thus, we obtain a somewhat unexpected result: the failure rate of an "aging" product does not depend on time.

Since the trajectories of a product operation process is a stepwise function, then the time to failure is a discrete random variable, so to estimate the failure rate of a product, you can use a discrete analog ([2], p. 35). Using the above obtained, we have

$$\lambda_{k+1} = \frac{MG^{*(k+1)}(\chi_t)}{\sum_{i=k}^{\infty} MG^{*(i+1)}(\chi_t)} = \frac{\left(\tilde{G}(\nu)\right)^{k+1} (1 - \tilde{G}(\nu))}{\sum_{i=k}^{\infty} \left(\tilde{G}(\nu)\right)^{i+1} (1 - \tilde{G}(\nu))} = \frac{\left(\tilde{G}(\nu)\right)^{k+1}}{\sum_{i=k}^{\infty} \left(\tilde{G}(\nu)\right)^{i+1}} = 1 - \tilde{G}(\nu),$$

where λ_{k+1} is the probability that the product is in good order after the *k*-th impact, but it fails after the $k+1$-th impact. In case if $G(x) = 1 - e^{-\mu x}$, then $\lambda_{k+1} = \frac{\nu}{\nu + \mu}$, $\lambda_{k+1} \le 1$.

Thus, the assumptions about exponential distributions of rates of impact loads and magnitude of endurance allowed us to obtain explicit quantitative indices of a product's reliability necessary for engineer-

ing practice, from the mathematical model of a product's reliability, operating under multiple effects of impact disturbance. Final relations of reliability indices are simple, which makes them attractive for practical use.

References

1. **Bogdanoff J., Kozin F.** Probabilistic models of damage accumulation: Transl. from English. – Academic Press, 1989. –334 p.

2. **Barlow R., Proschan F.** The mathematical theory of reliability: Transl. from English. – Sov. Radio, 1969. – 488 p.

3. **Bayhelt F., Franken P.** The reliability and maintenance. Mathematical approach: Transl. from German. – M.: Radio and communication, 1988. – 392 p.

4. **Kapoor K., Lamberson L.** Reliability and system engineering: Transl. from English. – Academic Press, 1980. – 604 p.

5. **Dillon B., Singh Ch.** Engineering methods to ensure system reliability: Transl. from English. – Academic Press, 1984. – 318 p.

6. **Gihman I.I., Skorokhod A.V.** The theory of stochastic processes. – Moscow: Nauka, 1973, vol. 2. Pp. 398-399.-640.

7. **Pereguda A.I., Andreev A.G.** Asymptotic method for calculating reliability and durability parameters of products operating under impact loads. – Dependability, 2007, # 3 (22) -p. 45-53.

8. **Toshio Nakagawa.** Shock and damage models in reliability theory. – Springer – Verlag London Limited 2007. – 191

9. **Druzhinin G.V.** The reliability of automated systems. – Moscow: Energy, 1977. – p.535.

10. **Pereguda A.I., Soborov I.A., Andreev A.G.** A method for constructing bilateral assessments of reliability and durability of products operating under impact loads. – Dependability, 2005, #2 (13) – p. 14-24

Володарский В.А.

К ВОПРОСУ ТОЧНОСТИ ЗАДАНИЯ ИНФОРМАЦИИ ПРИ ОПТИМИЗАЦИИ ПРЕДУПРЕДИТЕЛЬНЫХ ЗАМЕН

Предложен метод исследования устойчивости и чувствительности моделей оптимизации предупредительных замен, позволяющий обосновать точность задания исходной экономической информации.

Ключевые слова: *модель, оптимизация, устойчивость, чувствительность, точность.*

1. Состояние вопроса

В настоящее время оптимизационные расчеты параметров предупредительных замен (ПЗ) технических устройств (ТУ) проводятся, как правило, в предположении о строгой достоверности и однозначности используемой исходной информации и, следовательно, о строгой однозначности получаемых решений. При решении практических задач оптимизации ПЗ неизбежна большая или меньшая неопределенность исходной информации, которая проявляется в недостоверном знании численных значений исходных показателей или их вероятностного описания. Исходную информацию в задачах оптимизации ПЗ можно разделить на три вида:

1) детерминированную;

2) вероятностно-определенную, когда известны функции и параметры распределения случайных величин;

3) вероятностно-неопределенную, когда функции распределения случайных величин не известны.

К детерминированной относится информация о стоимости ПЗ, среднее значение которой однозначно определено нормативными документами. Информацию о стоимости аварийного восстановления можно считать вероятностно-определенной, поскольку она не может быть определена однозначно из-за зависимости от ряда случайных факторов (внезапность отказов ТУ, квалификация обслуживающего персонала и т.п.). В зависимости от полноты исходных данных, информацию об ущербе из-за отказов ТУ в силу случайного, а иногда недостаточно определенного характера, можно отнести к вероятностно-определенной или вероятностно-неопределенной.

Особые трудности на практике возникают при выборе функции распределения вероятности безотказной работы (ВБР) из-за малого объема статистического материала об отказах ТУ. Определить функцию распределения существующим методом математической статистики можно при количестве отказов более ста. В этом случае информация будет вероятностно-определенной, а в

противном случае – вероятностно-неопределенной, так как при этом можно получить несколько возможных функций распределения.

Неопределенность исходной информации приводит к методическим и практическим трудностям оптимизации ПЗ. При этом значительно повышается размерность решаемой задачи, так как появляется большое число возможных сочетаний информации о функции распределения вероятности безотказной работы и стоимостных показателях. Это приводит к неоднозначности решения оптимизационной задачи, поскольку каждая периодичность ПЗ при тех или иных сочетаниях исходной информации будет условно оптимальной.

Поэтому проблема исследования влияния точности определения исходной информации о функциях распределения вероятности безотказной работы и стоимостных показателях при оптимизации ПЗ остается весьма актуальной.

В статье [1] автором впервые применительно к моделям оптимизации предупредительных замен введены понятия экономической устойчивости решений и чувствительности к вариации исходных данных функции удельных эксплуатационных затрат. Проведены исследования устойчивости и чувствительности известных в теории надежности моделей оптимизации ПЗ по наработке и групповых замен [2]. При заданной точности расчетов определены зоны равноэкономичной периодичности и оценены диапазоны допустимых отклонений параметров моделей в зоне экономической устойчивости. Как продолжение этой работы, в статье [3] с целью обоснования точности задания исходных экономических данных проведены аналогичные исследования функции удельных эксплуатационных затрат известной в теории надежности модели оптимизации ПЗ с минимальным ремонтом при отказе для функции распределения Вейбулла [2].

В связи с актуальностью, в дальнейшем появился ряд публикаций по этой проблеме. Так, в [4] рассматривается случай, когда установлен вид закона распределения времени безотказной работы и оценены значения его параметров. Здесь исследуется только влияние отклонений параметров распределения на выбор периода профилактического обслуживания. В качестве критерия используется максимальное значение коэффициента готовности, а средние длительности предупредительных профилактик и аварийно-профилактических работ при этом считаются детерминированными. Необходимо отметить, что приведенный пример определения периода профилактики при экспоненциальном законе распределения является некорректным. Этот закон описывает отказы нестареющих систем, для которых проведение профилактического обслуживания нецелесообразно [2].

Аналогично в [5] приведены результаты исследования влияния отклонений оценочных значений параметра формы распределения Вейбулла (параметр масштаба при этом принимается детерминированным) на оптимальные значения сроков замен и на оптимальные значения эксплуатационных затрат при стратегии ПЗ по наработке. Здесь функция распределения считается определенной, а информация о стоимости предупредительных и аварийных замен принимается детерминированной.

В статье [6] сделана попытка обоснования требований к точности оценок показателей безотказности для решения задач продления срока службы РЭС. Авторы ссылаются только на публикацию [1], хотя полностью используют результаты ранее выполненных исследований [3], заменив только обозначения параметров формул. Если в [3] по результатам исследования устойчивости и чувствительности эксплуатационных затрат дана оценка допустимой точности определения исходных экономических данных, то в публикации [6] фактически повторяется исследование устойчивости известной модели ПЗ с минимальным ремонтом при отказе для функции распределения Вейбулла, и не дается решение поставленной в статье задачи.

Таким образом, из приведенного анализа публикаций очевидно, что вопросы исследования и обоснования требований к точности исходной информации при оптимизации предупредительных замен до настоящего времени остаются незавершенными.

В предыдущей публикации автора [7] представлены результаты выполненных исследований экономической устойчивости моделей оптимизации ПЗ в условиях вероятностно-неопределенной информации о функции распределения ВБР. В этом случае при оцененном значении коэффициента вариации задано семейство функций распределения и показана эквивалентность получаемых решений в отношении определения диапазона оптимальных значений периодичности ПЗ.

Цель статьи – исследования устойчивости и чувствительности моделей оптимизации предупредительных замен для обоснования точности задания исходной экономической информации.

2. Обоснования точности задания исходной экономической информации

При оптимизации периодичности проведения ПЗ технических устройств, как правило, ориентируются на средние значения исходных экономических данных. На практике часто стоимость аварийного ремонта с учетом ущерба от простоя устройств имеет значительные отклонения от среднего значения. При этом параметры математических моделей не могут быть заданы однозначно. В этих условиях при решении задачи каждому сочетанию значений параметров соответствует свое оптимальное значение периодичности ПЗ.

Основываясь на ранее полученных результатах [1], задачу обоснования точности, с которой должны определяться исходные данные, предлагается решать в два этапа.

Во-первых, необходимо провести исследование экономической устойчивости функции удельных эксплуатационных затрат и при заданной точности расчетов определить допустимые отклонения периодичности ПЗ в зоне оптимальных значений.

Во-вторых, необходимо исследовать чувствительность функции удельных эксплуатационных затрат к изменению её параметров и, используя диапазон допустимого отклонения периодичности ПЗ, обосновать точность определения исходных экономических данных.

Решение этой задачи покажем на примере стратегии предупредительных замен с минимальным ремонтом при отказе, когда удельные эксплуатационные затраты (если наработка между отказами имеет распределение Вейбулла) определяется согласно [2]

$$C(\tau) = [B+A(k_b\ \tau T^{-1})^b]\ \tau\ ^{-1}], \qquad (1)$$

где B – стоимость предупредительной замены; A – стоимость аварийного ремонта при отказе с учетом ущерба; b – параметр формы распределения Вейбулла; $k_b=\Gamma(1-b^{-1})$. Здесь Γ – гамма-функция; T - наработка на отказ; τ - периодичность ПЗ.

Разделив выражение (1) на A/T, получим значение относительных удельных затрат в безразмерном виде

$$y = C(\tau)A^{-1} = \eta x^{-1}+k_b{}^b x^{b-1}, \qquad (2)$$

где $\eta = B/A$ – коэффициент стоимости; $x = \tau/T$ – относительная периодичность предупредительных замен в долях наработки на отказ.

Оптимальное значение x_0 при минимуме относительных удельных эксплуатационных затрат y_0 определяется из условия $dx/dy = 0$ по формулам:

$$X_0=k_b^{-1}(\eta(b-1)^{-1})^{1/b}; \qquad (3)$$

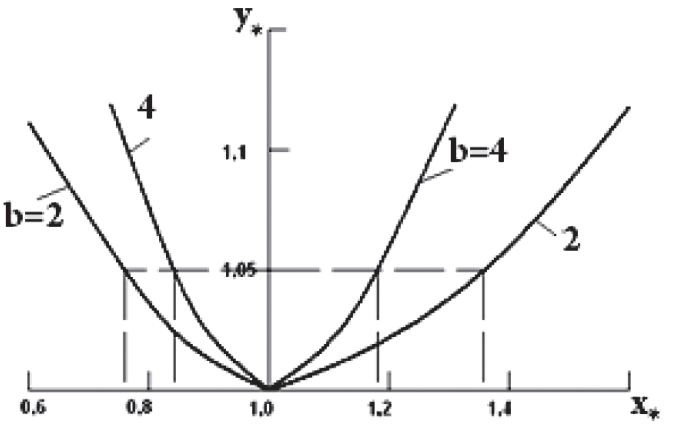


Рис. 1. Результаты исследования экономической устойчивости

$$y_0 = bk_b{}^b x_0{}^{b-1}. \quad (4)$$

Преобразовав (2) через (3) и (4), получим уравнение вида

$$y_x = (b - 1 + x_x{}^b)(bx_x)^{-1}, \quad (5)$$

где $y_x = y/y_0$; $x_x = x/x_0$ – относительные отклонения, соответственно, удельных эксплуатационных затрат и периодичности предупредительных замен от их оптимальных значений.

Уравнение (5) носит обобщенный характер, не зависит от параметров η, x и k_b исходной математической модели (2) и позволяет исследовать экономическую устойчивость удельных эксплуатационных затрат. Задаваясь значением $y_x = 1+\delta$, можно определить допустимые относительные отклонения оптимальной периодичности предупредительных замен, соответствующие принятой точности расчетов относительных удельных эксплуатационных затрат.

Графики зависимости y_x от x_x при разных значениях b представлены на рис.1, из которого видно следующее. С ростом параметра формы распределения Вейбулла b (уменьшением коэффициента вариации) экономическая устойчивость функции удельных эксплуатационных затрат

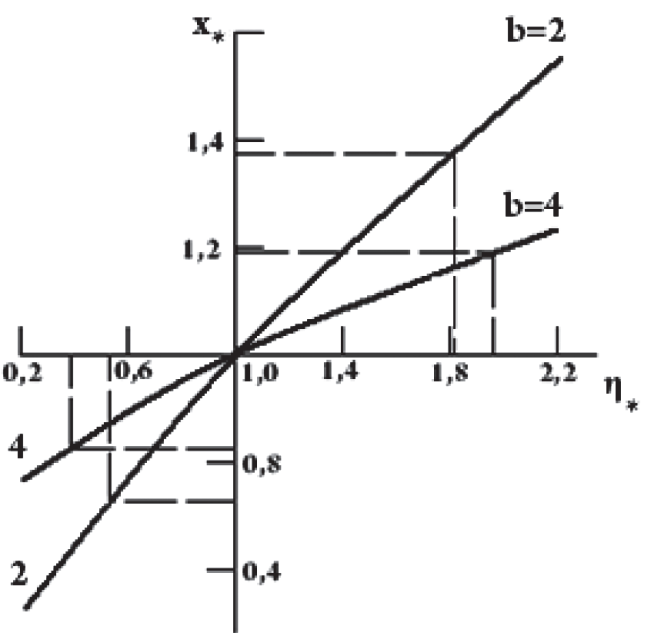


Рис. 2. Результаты исследования чувствительности

снижается. Если задать, например, δ = 0,05 (см. пунктир на рис.1), то получим следующие допустимые отклонения периодичности предупредительных замен: при *b*=2 от нижнего $\underline{x_x}$ = 0,73 до верхнего $\overline{x_x}$ =1,37; при *b*=4 – от $\underline{x_x}$ = 0,82 до $\overline{x_x}$ =1,19. Тогда оптимальное τ_0, допустимые нижнее $\underline{\tau_0}$ и верхнее $\overline{\tau_0}$ значения периодичности предупредительных замен определяются как $\tau_0=x_0T$, $\underline{\tau_0}=\underline{x_x}\tau_0$, $\overline{\tau_0}=\overline{x_x}\tau_0$.

Определение чувствительности функции удельных эксплуатационных затрат к изменению коэффициента стоимости η проводится с использованием уравнения (3). Исследование чувствительности не требует знания численных значений коэффициента стоимости, так как выполняется в относительных единицах $\eta_x = \eta/\eta_o$, где η_o – базовое значение коэффициента стоимости, соответствующее оптимальной периодичности предупредительных замен.

Результаты исследования чувствительности представлены на рис.2, из которого видно, что с увеличением параметра формы *b* чувствительность к изменению η_x снижается, и исходные экономические данные могут определяться с большей погрешностью. Например, в зоне экономической устойчивости функции удельных эксплуатационных затрат при δ=0,05 (см. пунктир на рис. 2) допустимы следующие относительные отклонения коэффициента стоимости: при *b*=2 – от 0,52 до 1,84, а при *b*=4 – от 0,46 до 2,0 от его базового значения.

Заключение

В результате исследования чувствительности установлено, что в зоне экономической устойчивости функции удельных эксплуатационных затрат исходные экономические данные могут определяться с большой погрешностью. Например, при точности расчетов 5% удельных эксплуатационных затрат в случае стратегии замен с минимальным ремонтом при отказах допустимы относительные отклонения коэффициента стоимости в случае распределения Вейбулла с коэффициентом формы равным двум – от 0,52 до 1,84, а с коэффициентом формы равным четырем – от 0,46 до 2,0 от его базового значения. В рассматриваемых случаях эти значения могут быть приняты в качестве допустимой точности определения исходных экономических данных.

Литература

1. **Володарский В.А.** Оптимизация периодичности предупредительных замен в условиях неопределенности исходной информации // Надежность и контроль качества. – 1984. – №8. – С. 39-44.

2. **Барлоу Р., Прошан Ф.** Математическая теория надежности. – М.: Советское радио, 1969.- 488 с.

3. **Володарский В.А.** Обоснование точности определения исходных экономических данных при оптимизации периодичности предупредительных замен // Надежность и контроль качества. – 1986. – №4. – С. 36-39.

4. **Голиков В.Ф.** О влиянии точности определения характеристик надежности на выбор периода профилактического обслуживания // Известия АН ССР. Техническая кибернетика. 1986. – №1. – С. 66-69.

5. **Байхельт Ф., Франкен П.** Надежность и техническое обслуживание. Математический подход. – М.: Советское радио, 1988.- 392 с.

6. **Ланецкий Б.Н., Кобзев В.В.** Обоснование требований к точности оценок показателей безотказности РЭС эксплуатируемых ЗРК для решения задач продления назначенных сроков службы (ресурсов) // Системи обробки информації.- 2006.- Випуск 4 (53).- С.110-117.

7. **Володарский В.А.** Исследования экономической устойчивости моделей оптимизации предупредительных замен // Надежность. – 2012. – №1(40). – С. 36-43.

Volodarsky V.A.

THE ISSUE OF ACCURACY OF INFORMATION ASSIGNMENT FOR OPTIMIZATION OF PREVENTIVE REPLACEMENTS

The paper offers a method for researching the stability and sensitivity of models of preventive replacement optimization that allows for justification of the accuracy of initial economic information assignment.

Keywords: *model, optimization, replacement, stability, sensibility, accuracy.*

1. State of the art

Currently, optimization calculations for parameters of preventive replacements (PR) of technical devices (TD) are usually carried out under the assumption of strict reliability and unambiguity of raw information and, consequently, strong unambiguity of the solutions obtained. When solving practical optimization problems of PR, it is inevitable to face greater or lesser uncertainty of source information that presents itself in unreliable knowledge of numerical values of initial indicators or their probabilistic description. Initial information in optimization problems of PR can be divided into four types:

1. deterministic;
2. probabilistically certain, when functions and parameters of the distribution of random variables are known;
3. probabilistically uncertain, when the distribution functions of random variables are not known.

Deterministic initial information includes information about the cost of PR, the average value of which is unambiguously defined by regulations. Information about the cost of emergency recovery can be considered as probabilistically certain, because it cannot be unambiguously determined due to the dependence from the number of random factors (device sudden failure, qualification of maintenance personnel, etc.). Depending on the completeness of source data, information about the damage due to TD failures because of the random and sometimes not sufficiently certain nature can be attributed to the probabilistically certain or probabilistically uncertain information.

Particular difficulties arise in practice when selecting a reliability function (RF) because of the small amount of statistic data about TD failures. The distribution function can be determined by existing methods of mathematical statistics when the number of failures is more than one hundred. In this case, the information will be probabilistically certain, and otherwise it will be probabilistically uncertain, because several possible distribution functions can be obtained.

The uncertainty of initial information leads to methodological and practical difficulties of PR optimization. In this case, the dimension of the problem increases significantly, since there is a large number of possible combinations of information about the reliability function and cost parameters. This leads to the ambiguity of the optimization problem solution, because each interval of PR under various combinations of initial information is conditionally optimal.

Therefore, the problem of investigating the influence of the accuracy in determining the initial information about the reliability function (probability distribution function) and cost parameters while optimizing the PR remains relevant.

In the paper [1], the author for the first time introduced the concept of economic solutions' stability and variation sensitivity of the initial data functions of operational cost per unit in relation to the optimization model of preventive replacements. The research of stability and sensitivity of PR optimization models for mean time between failures and group replacements known in the reliability theory has been carried out [2]. For a specified accuracy of calculations, the areas of equally economic intervals have been defined and the region of admissible deviation of models' parameters in the area of economic sustainability assessed. The paper [3] as a continuation of this work in order to substantiate the accuracy of assignments of initial economic data presents similar research of operational cost per unit function of PR optimization models known in the reliability theory with minimal repair at failure for the Weibull distribution function [2].

Later due to the urgency of this issue, a number of publications on this problem have been offered. Thus, the paper [4] considers the case where the type of time-to-failure distribution law has been set and its parameters evaluated. It examines only the effect of deviations of the distribution parameters to choose the cycle of preventive maintenance. In this case, the maximum value of availability factor is used as a criterion, and the average duration of preventive and emergency maintenance works are considered as deterministic. It should be noted that the above example of determining the period of preventive maintenance with an exponential distribution law is incorrect. This law describes failures of ageing-resistant systems for which preventive maintenance is not appropriate [2].

Similarly, the paper [5] shows the results of researches as regards the effect of deviations of the shape parameter estimated values in Weibull distribution (in this case, the scale parameter is accepted as deterministic) on the optimal values of replacement ages and on the optimal values of operating costs using the strategy of PR according to mean time between failures. Here, the distribution function is considered specified, and information on the cost of preventive and emergency replacements is accepted as deterministic.

The paper [6] attempted to justify requirements for the accuracy of reliability factor estimates to meet the challenges of extending the lifetime of radio electronic systems life. The authors refer only to publication [1], although fully utilize the results of previous studies [3] by replacing the designation parameters in formulas. While the paper [3] gives the assessment of allowable accuracy of initial economic data based on the obtained results of stability and sensitivity operating costs, publication [6] actually repeats the study of stability of the known model for PR with minimal repair at failure for the Weibull distribution function, but there is no any solution of the stated problem in [6].

Thus, from the above analysis of publications, it is evident that the research issues and justification of the accuracy requirements for the initial information in the optimization of preventive replacements have not been completed so far. In previous publication [7], the author presented the results of the research of economic stability optimization models of PR under probabilistically uncertain information about the reliability function (RF as a function of time). In this case, for the estimated value of the variation coefficient, a family of distribution functions is specified and the equivalence of the solutions obtained is shown in relation to determination of the range of optimal values of PR periodicity.

The purpose of the present paper is to study stability and sensitivity optimization models of preventive replacements to justify the accuracy of the initial economic information assignment.

2. Justification of the accuracy of the initial economic information assignment

When optimizing the PR periodicity of technical devices, the average values of the initial economic data are considered as a guiding line. In practice, the cost of emergency repair taking into account the damage owing to repair downtime of devices has significant deviations from the average value. In this case, the parameters of mathematical models cannot be defined unambiguously. Under these conditions, when solving the problem, its own optimal values of PR periodicity correspond to each combination of parameter values.

Based on the results obtained previously in [1], the problem of justifying the accuracy by which the initial data should be determined should be solved in two stages. First, it is necessary to carry out a study of economic stability of the operational cost per unit function and for a given accuracy of calculations to determine the acceptable deviations of PR periodicity in the area of optimal values.

Second, it is necessary to investigate the sensitivity of the operational cost per unit to alteration of its parameters and using an acceptable deviation range of PR periodicity to justify the determination accuracy of the initial economic data.

We shall show the solution of this problem using the example of preventive replacements strategy with minimal repair at failure when the operational cost per unit (if operating time between failures has the Weibull distribution) is determined according to [2]

$$C(\tau) = [B+A(k_b\, \tau T^{-1})^b]\, \tau^{-1}], \quad (1)$$

where B is the cost of preventive replacement; A is the cost of emergency repair in case of failure, with the damage taken into account; b is the shape parameter of the Weibull distribution; $k_b = G(1- b^{-1})$. Here G is the gamma function, and T is mean time between failures (MTBF); ϕ is the periodicity of PR.

Dividing equation (1) by A/T, we will obtain the value of the relative cost per unit in the dimensionless form

$$y = C(\tau)A^{-1} = \eta x^{-1} + k_b^{\,b} x^{b-1}, \quad (2)$$

where $з = B/A$ is a cost factor, $x = ϕ /T$ is the relative periodicity of preventive replacements in fractions of MTBF.

The optimal value x_0 at minimum relative operating costs per unit is determined from the condition $dx/dy = 0$ by the following formulas:

$$X_0 = k_b^{-1}(\eta(b-1)^{-1})^{1/b}; \quad (3)$$

$$y_0 = bk_b^{\,b} x_0^{\,b-1}. \quad (4)$$

Transforming (2) through (3) and (4), we shall obtain an equation of the following form:

$$y_x = (b - 1 + x_x^{\,b})(bx_x)^{-1}, \quad (5)$$

where $y_x = y/y_0$; $x_x = x/x_0$ are relative deviations of operating costs per unit and periodicity of preventive replacements from their optimal values respectively.

Equation (5) has a generalized character, does not depend on the parameters η, *x* and k_b of initial mathematical model (2) and allows to explore the economic sustainability of the operating costs per unit. Assuming the value $y_x = 1+\delta$, it is possible to determine the permissible relative deviations of optimal periodicity of preventive replacements corresponding to the accepted accuracy of calculations of relative operating costs per unit.

The diagrams of dependence y_x on x_x for different values of *b* are presented in Fig. 1, which shows the following. With the growth of the shape parameter of the Weibull distribution *b* (decreasing coefficient of variation), economic sustainability of the function of operating costs per unit decreases. If we specify, for example, д = 0,05 (see a dashed line in Fig. 1), it is possible to obtain the following admissible deviations of preventive replacements: for *b* =2 from the lower $\underline{x_x} = 0.73$ to the upper $\overline{x_x} = 1.37$, for *b* = 4 from the lower $\underline{x_x} = 0.82$ to the upper $\overline{x_x} = 1.19$. Then the optimal τ_0, the permissible lower $\underline{\tau_0}$ and the upper $\overline{\tau_0}$ values of the periodicity of preventive replacements are defined as follows

$$\tau_0 = x_0 T,\ \underline{\tau_0} = \underline{x_x}\tau_0,\ \overline{\tau_0} = \overline{x_x}\tau_0.$$

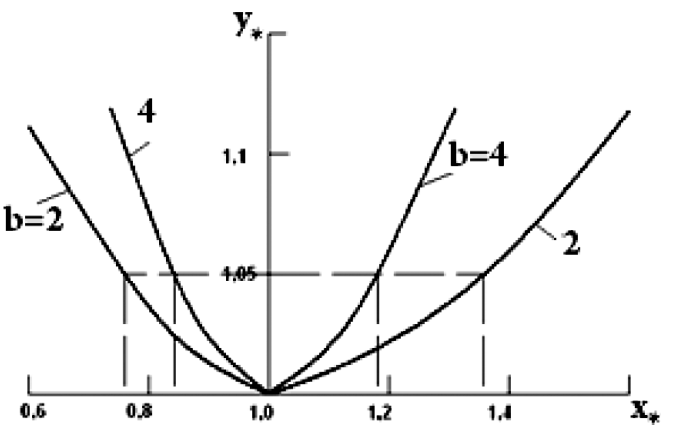


Fig.1. Results of the economic stability study

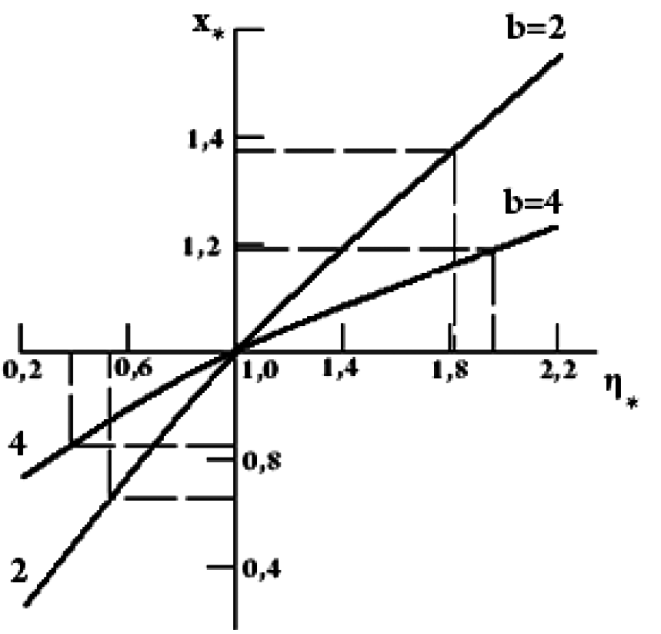


Fig. 2. Results of the sensitivity study

Determination of the sensitivity function of operating costs per unit for change of the cost coefficient з is carried out using equation (3). Sensitivity analysis does not require knowledge of the numerical values of the cost coefficient, as it is executed in relative units $\eta_x = \eta/\eta_o$, where η_o is the basic value of the cost coefficient corresponding to the optimum periodicity of preventive replacements.

The results of sensitivity analysis are presented in Fig. 2, which shows that with the increase of the shape parameter *b* the sensitivity to changes of η_x decreases, and initial economic data can be determined with lower accuracy.

For example, in the area of economic stability function of operating costs per unit at д = 0,05 (see a dashed line in Fig. 2) the following relative deviations of cost coefficient: for *b* = 2 – from 0.52 to 1.84, and for *b* = 4 – from 0.46 to 2.0 of its baseline value.

Conclusion

As a result of sensitivity analysis, it has been found that in the area of economic stability of the function of operating costs per unit the initial economic data can be determined with lower accuracy. For example, if the calculation accuracy makes up 5% of operating costs per unit in case of the replacements strategy with minimal repairs at failures, permissible relative deviations of the coefficient cost in t case of the Weibull distribution with a shape factor equal to 2 from 0.52 to 1.84, and with a shape factor equal to 4 from 0.46 to 2.0 of its basic value. In considered cases, these values can be taken as acceptable accuracy of determining initial economic data.

References

1. **Volodarsky V.A.** Optimizing the periodicity of preventive replacements under uncertainty initial information // Dependability and quality control. – 1984. – # 8. – pp. 39-44.

2. **Barlow R., Proschan F.** Mathematical theory of reliability. – Moscow: Soviet Radio, 1969. – 488 p.

3. **Volodarsky V.A.** Justification of initial economic data accuracy for optimizing the periodicity of preventive replacements // Dependability and quality control. – 1986. – # 4. – pp. 36-39

4. **Golikov V.F.** About the influence of determining the accuracy of dependability characteristics to choose the period of preventive maintenance // News of the USSR Academy of Sciences. Engineering Cybernetics. 1986. – # 1. – pp. 66-69.

5. **Bayhelt F., Franken P.** Dependability and Maintenance. Mathematical approach. – Moscow: Soviet Radio, 1988. – p. 392.

6. **Lanetsky B.N., Kobzev V.V.** Justification of requirements for the accuracy of estimates of radio electronics' reliability factor in exploited surface-to-air missile systems for solving the problem of assigned service life extension (of resources) // Information processing systems – 2006. – Issue 4 (53). – pp.110-117.

7. **Volodarsky V.A.** Studies of economic stability optimization models for preventive replacements / / Reliability. – 2012. – № 1 (40). – S. 36-43.

Абрамова Н.А., Коврига С.В., Макаренко Д.И.

ПРИНЦИПЫ УПРАВЛЕНИЯ КАЧЕСТВОМ ПРОЕКТИРОВАНИЯ СЛОЖНЫХ ПРОГРАММНО-ТЕХНИЧЕСКИХ КОМПЛЕКСОВ С УЧЕТОМ ОЦЕНКИ РИСКОВ ОШИБОК ЧЕЛОВЕКА

Для снижения влияния человеческих факторов при проектировании программно-технических комплексов, связанных с безопасностью, на риски возникновения опасных ситуаций в ходе их эксплуатации, предложены некоторые новые принципы, направленные на повышение качества проектирования таких комплексов. Представленные результаты основаны, с одной стороны, на психологических и междисциплинарных исследованиях, а с другой, – на анализе практики проектирования сложных программно-технических комплексов в атомной энергетике.

***Ключевые слова**: потенциально опасный объект, безопасность, программно-технический комплекс, достоверность, риски из-за человеческого фактора, управление качеством проектирования.*

Введение

Сегодня имеет место существенное усложнение потенциально опасных объектов, для которых создаются методы и системы управления или поддержки принятия решений на основе формальных методов. В понятие сложности объектов (систем, комплексов), наряду с более традиционными признаками (такими как количественная сложность, структурная сложность, сложность математических моделей – «organized complexity»), включается человеческий аспект сложности, когда интеллектуально сложным этапом решения задач управления и обеспечения безопасности является первичная структуризация и формализация знаний о проектируемых объектах и предъявляемых к ним требованиях.

В силу неизбежного участия людей, применяемые методы структуризации и формализации знаний при проектировании сложных объектов в принципе не могут обеспечить достоверности конечных результатов. Другими словами, они являются рискованными в отношении достоверности результатов[1]. Таким образом, поиск решений проблемы рисков, обусловленных человеческим фактором, должен охватывать не только сами объекты, но и процесс их создания, в котором также

[1] Здесь достоверность понимается в широком смысле, как возможность полагаться на результаты применения таких методов.

участвуют люди. Это означает, что человеческие факторы риска могут быть связаны не только с людьми, участвующими в процессе управления объектом, но и с разработчиками методов и систем управления и информационных технологий, и учеными, которые теоретически обосновывают методы управления.

Целью данной работы является разработка подходов и принципов управления качеством проектирования сложных программно-технических комплексов (ПТК), связанных с безопасностью, для снижения влияния человеческих факторов при проектировании таких ПТК на риски возникновения опасных ситуаций в ходе их эксплуатации.

Серьезным свидетельством практической значимости рассматриваемых рисков при решении задач управления сложными объектами являются экспериментальные исследования мышления субъекта управления в сложных проблемных ситуациях и анализ причин мыслительных ошибок, порождаемых в ходе их разрешения [1].

В статье представлена типология рисков по характеру их влияния на безопасность потенциально опасного объекта при эксплуатации ПТК, предложены некоторые новые принципы и подходы, направленные на повышение качества проектирования ПТК. Представленные результаты основаны, с одной стороны, на психологических и междисциплинарных исследованиях, а с другой, – на анализе практики проектирования сложных ПТК для АЭС.

1. Разнообразие косвенных источников риска возникновения опасных ситуаций в ходе эксплуатации программно-технических комплексов, связанных с безопасностью

С целью выявления и систематизации человеческих факторов и механизмов риска, (1) действующих в жизненном цикле создания, внедрения и применения ПТК и (2) практически значимых для управления качеством, проведен выборочный анализ практики проектирования сложных ПТК, связанных с безопасностью (применительно к АЭС).

Изучение практической деятельности по обеспечению качества ПТК для потенциально опасных объектов показывает, что в условиях возрастающей интеллектуальной сложности ПТК традиционный подход к обеспечению качества не охватывает широкого спектра разнородных косвенных рисков для безопасности, действующих на практике и не поддающихся количественной оценке. Прежде всего, это относится к рискам из-за человеческого фактора в ходе проектирования и испытаний ПТК. При этом в качестве традиционного подхода к обеспечению качества ПТК, связанных с безопасностью, рассматривается поэтапная верификация и валидация вкупе с организационными методами и ограниченным применением формальных методов, возможности которых в условиях возрастающей сложности ПТК существенно ограничены.

Выделены следующие типы рисков по характеру их влияния на безопасность потенциально опасного объекта при эксплуатации ПТК:

- риски, явно связанные с безопасностью при эксплуатации ПТК (т.е. порождающие риск возникновения опасных ситуаций на объекте),
- косвенные риски, в которых явная связь с опасными ситуациями не прослеживается.

К косвенным рискам относятся:

- технические риски – риски, связанные с принятием технических решений при создании ПТК;

• организационно-управленческие риски, включая риски, связанные

– с уровнем зрелости производственного процесса создания ПТК в терминах модели зрелости SW-CMM [2];

– с компетентностью субъектов производственной и управленческой деятельности;

• субъективные риски – риски, связанные с когнитивными и иными особенностями субъектов производственной и управленческой деятельности (согласно современным данным когнитивных наук).

На рис. 1 представлены типовые риски и причинно-следственные связи между этими типами рисков (знак «+» на связи означает положительное влияние («чем больше…, тем больше…»), а знак «–» – отрицательное влияние («чем больше…, тем меньше…»); серые стрелки указывают на другие возможные типы рисков).

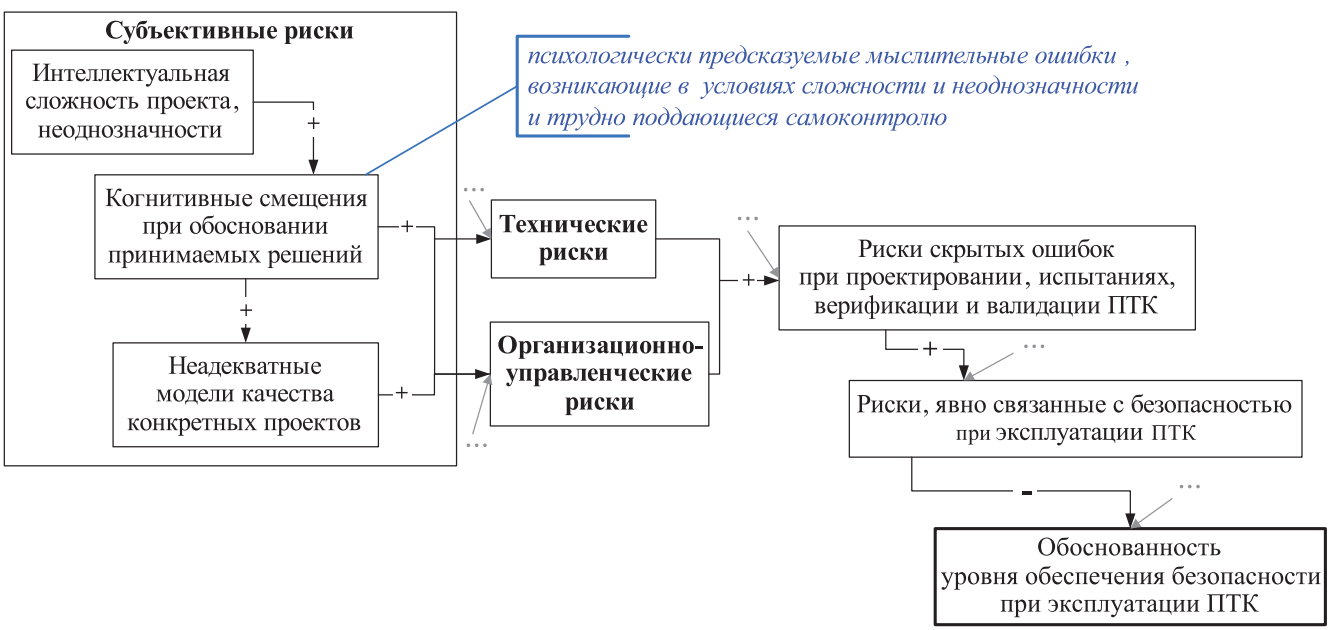


Рис. 1. Риски из-за человеческого фактора при создании ПТК, связанных с безопасностью, и их причинно-следственные связи

В ходе анализа и систематизации рисков по характеру их влияния на безопасность потенциально опасного объекта при эксплуатации ПТК (1) нашла свое подтверждение гипотеза о зависимости рисков из-за человеческого фактора при проектировании ПТК, связанных с безопасностью, от функциональных ролей человека в жизненном цикле ПТК; (2) а также выдвинута и прошла проверку гипотеза о зависимости неадекватных моделей качества конкретных проектов у ответственных исполнителей от известных в психологии факторов риска, называемых когнитивными смещениями (психологически предсказуемых мыслительных ошибок, возникающих в условиях сложности и неоднозначности и трудно поддающихся самоконтролю). К ним относятся стереотипы применения устаревших технологий, систематическая недооценка значимости непривычных требований.

Разнородность выделенных практически значимых рисков при проектировании сложных ПТК, связанных с безопасностью, при существенной роли человеческого фактора в них в сочетании с практической невозможностью достоверной количественной оценки такого рода рисков свидетельствуют о необходимости разработки новых теоретических подходов к решению исследуемой задачи управления качеством проектирования сложных ПТК.

2. Общие принципы косвенного управления качеством программно-технических комплексов, связанных с безопасностью

Известный принцип поэтапной верификации в ходе создания ПТК, связанных с безопасностью, может рассматриваться как принцип косвенного управления качеством таких ПТК. При этом стандартным подходом считается верификация по предопределенным критериям качества, которые предъявляются к промежуточным продуктам проектирования, представленным соответствующей документацией.

Для расширения возможности раннего обнаружения косвенных рисков из-за человеческого фактора (по сравнению с типовым подходом к верификации) предложен ряд новых принципов:

• *более широкий охват разнородных косвенных факторов риска и их причинно-следственных связей*, прежде всего человеческих факторов, в ситуациях обнаружения ошибок или рисков неадекватных технических и управленческих решений, с целью повышения эффективности управления качеством ПТК и расширения состава механизмов управления;

• *принцип расширенной верификации*, включая верификацию не только технических решений, но и используемых методов оценки, в том числе моделей качества проектов (в рамках имеющихся суммарных ресурсов);

• *ограниченное применение формальных методов комплексного оценивания*, используемых при управлении качеством проектирования и испытаний ПТК, связанных с безопасностью, во избежание рисков недостоверного оценивания в сочетании с верификацией самих методов оценивания. Обоснованиями принципа ограниченного применения формальных методов комплексного оценивания в сочетании с верификацией самих методов оценивания служат (1) найденные ранее теоретическим анализом и подтвержденные на практике возможности манипулирования оценками качества в условиях невозможности достоверной количественной оценки рисков или иных показателей качества проектирования; (2) найденные риски в самих методах оценивания, которые предлагаются теорией и стандартами для решения задач комплексного оценивания, связанных с безопасностью [3];

• *рефлексивный подход к анализу обоснований* принимаемых технических и управленческих решений, учитывающий не только собственно объективные обоснования принимаемых решений, но и зависимость представлений и оценок ответственных исполнителей от субъективных факторов риска, функциональных ролей и интересов. Обоснованием рефлексивного подхода служит наличие ряда практических ситуаций, в которых выявление необоснованных решений невозможно или затруднительно без учета субъективных факторов (например, ошибочное занижение уровня требований к проектированию ПТК по сравнению с уровнем требований, который мотивирован классом безопасности);

• *экспертная верификация без предопределенных критериев* в дополнение к традиционной верификации по предопределенным критериям качества. Обоснованиями принципа экспертной верификации без предопределенных критериев служат:

– анализ опыта верификации и перекрестных анализов проектных решений соисполнителями конкретного проекта ПТК;

– междисциплинарное исследование психологических механизмов, лежащих в основе экспертной верификации, начиная с таких как «детекторы ошибок» [4], «когнитивный диссонанс» [5].

Для повышения качества процесса обнаружения ошибок и рисков экспертами-верификаторами разработана оригинальная междисциплинарная модель когнитивного процесса экспертной верификации без предопределенных критериев. Она сопоставима с широко известной моделью двух когнитивных систем, отражающей внутренние возможности человека к обнаружению ошибок в обоснованиях [6].

2.1. Модель когнитивного процесса экспертной верификации без предопределенных критериев

Принципиальное различие традиционной верификации по предопределенным критериям от экспертного анализа как метода верификации состоит в том, что в первом случае выбор критерия и выбор (идентификация) верифицируемого фрагмента предшествуют оценке соответствия, тогда как при экспертном анализе некоторый анализируемый материал сразу идентифицируется как несоответствующий тем или иным представлениям эксперта-верификатора. «Сразу» здесь означает, что оценка появляется в результате внутренних, необязательно осознаваемых когнитивных процессов.

Предлагаемая модель экспертной верификации без предопределенных критериев опирается на принципиальное свойство – свойство самопроизвольной идентификации (локализации) несоответствий. При этом учитывается, что, как показывают наблюдения, типичны два вида определения несоответствий. В одних случаях идентифицированный экспертом-верификатором фрагмент анализируемого материала (или его свойство) может сразу оцениваться им как несоответствующий некоторому объявляемому (но не выбранному заранее) критерию, требованию. В других случаях оценка дается в самых общих словах типа «некорректно», «так не может быть», «сомнительно», «что-то тут не то», «непонятно», «какая-то странность (или аномалия)».

Далее последующим «самоизвлечением знаний» даются объяснения оценки, так что, в конечном счете, либо выявляется нарушенный критерий соответствия, либо устанавливается необходимость

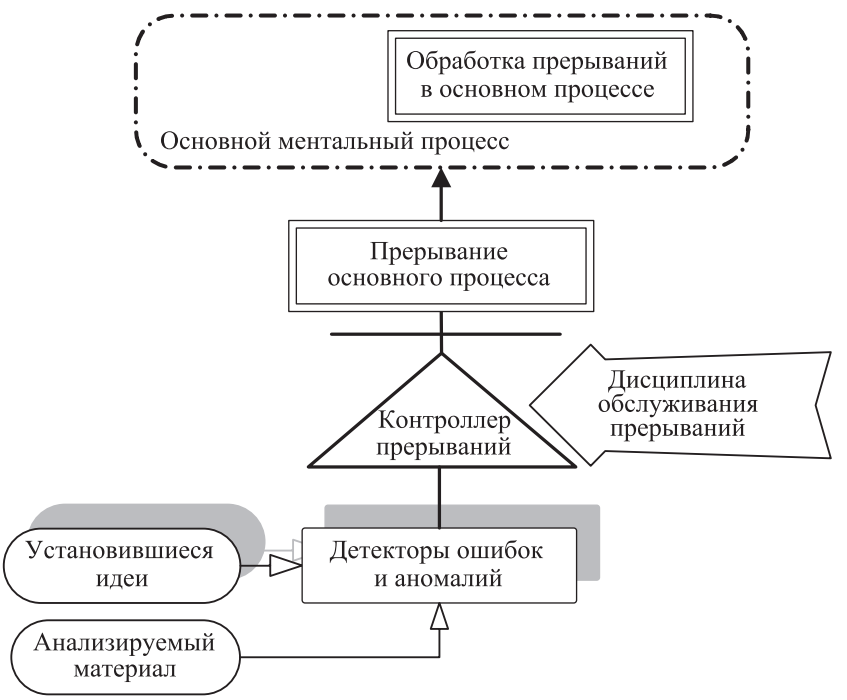


Рис. 2. Структурная организация обработки экспертного знания с прерываниями при обнаружении ошибок и аномалий

дальнейшего анализа для объяснения идентифицированной странности или аномалии. В последнем случае можно говорить об идентификации рискованного фрагмента или общего свойства.

Объяснение когнитивных процессов, дающих такого рода реакцию эксперта-верификатора, может быть дано с использованием знаний когнитивных наук в таких терминах как «когнитивный диссонанс», «когнитивный контроль», «детектор ошибок», «функциональный орган».

Однако более четкое и целостное представление получается дополнительным привлечением компьютерной метафоры с использованием понятия «системы прерываний» и родственных понятий таких как «источник прерываний», «основной (прерываемый) процесс», «механизм прерываний», «дисциплина обслуживания прерываний» для увязывания. Структурная организация обработки экспертного знания с прерываниями при обнаружении ошибок и аномалий представлена на рис. 2.

Идентификацию несоответствия представляется уместным рассматривать как частный случай проявления когнитивного диссонанса – психологического дискомфорта, который, по теории Л. Фестингера [5], может вызываться противоречием между имеющимся устоявшимся представлением и свежей поступающей информацией, фактами.

Акт идентификации несоответствия может трактоваться как срабатывание «системы прерываний», которая осуществляет когнитивные контроли над знаниями, извлекаемыми экспертом из объекта верификации.

Система прерываний выявляет несоответствия посредством совокупности релевантных детекторов ошибок. Эти детекторы отражают стереотипные, или, по крайней мере, хорошо усвоенные активные знания, относящиеся к сфере анализа. Обнаружение несоответствия тем или иным детектором может приводить к прерыванию основного процесса в соответствии с той или иной «дисциплиной обслуживания прерываний», так что несоответствие, по крайней мере, регистрируется экспертом-верификатором, и, возможно, проводится его первичный анализ (прерывание «обслуживается»). С учетом наблюдений по идентификации рискованных фрагментов предполагается, что детекторы могут обнаруживать не только ошибки, но и рискованные и сомнительные ситуации.

Согласно нейрофизиологическим экспериментам Н.П. Бехтеревой [4], действие механизма, который она назвала «детектором ошибок», происходит через эмоции, которые могут рассматриваться как «механизм прерывания».

Из предложенной модели экспертной верификации с двумя видами знаний, порождающих когнитивный диссонанс, можно сделать довольно нетривиальный вывод. Для срабатывания теоретических знаний в качестве элемента диссонанса у эксперта-верификатора должны сформироваться надлежащие детекторы ошибок или, по крайней мере, детекторы риска, рискованных свойств, способные в силу высокой активности вызвать когнитивный диссонанс и самопроизвольные прерывания основного когнитивного процесса в случае несоответствий.

Анализ практики верификации ПТК, связанных с безопасностью, в области атомной энергетики, показал, что предложенная модель не только обладает сравнительно большими объяснительными возможностями, но и открывает пути для повышения качества процесса обнаружения ошибок и рисков экспертами-верификаторами и для его компьютерной поддержки.

2.2. Модифицированная модель управления качеством программно-технических комплексов, связанных с безопасностью

На основе предлагаемых принципов модифицирована модель управления качеством ПТК, которая включает, в дополнение к традиционной модели управления качеством посредством поэтапной верификации, выделение и оценку в конкретном процессе проектирования, верификации и испытаний ПТК разнородных косвенных факторов риска, действующих в жизненном цикле ПТК и их

причинно-следственных влияний на управление качеством. Обобщенная схема модифицированной модели управления качеством проектирования ПТК, связанных с безопасностью, представлена на рис. 3.

Рис. 3. Обобщенная схема модифицированной модели управления качеством проектирования ПТК, связанных с безопасностью

Предлагаемый подход с расширением традиционной модели управления качеством проектирования в ходе верификации прошел частичную эмпирическую проверку применительно к созданию конкретного ПТК, связанного с безопасностью, для АЭС «Куданкулам». В процессе верификации проекта ПТК был выявлен ряд значимых разнородных факторов риска, выходящих за рамки ошибочных или рискованных технических решений (например, несогласованность системы понятий в неоднородном коллективе участников и руководства международного проекта, сложность (непрозрачность) ролевой структуры взаимоотношений между участниками проекта, недостаточный опыт разработчиков по созданию ПТК, связанных с безопасностью). Это позволило уточнить первоначальную модель управления качеством проекта в виде соответствующей причинно-следственной схемы косвенного влияния найденных факторов на риск скрытых ошибок проектирования, а значит, и на уровень обеспечения безопасности при эксплуатации ПТК. Модифицированная модель позволила выделить дополнительные точки приложения управляющих воздействий по повышению качества проектирования. В том числе была подтверждена целесообразность ее применения для согласования и обоснования различных представлений в условиях сложной ролевой структуры взаимоотношений между участниками международного проекта.

Заключение

Практическая роль предложенных новых принципов косвенного управления качеством ПТК состоит в расширении возможностей управления качеством проектирования таких комплексов благодаря выявлению и учету рисков из-за человеческого фактора при разработке объектов с повышенными требованиями надежности и безопасности функционирования.

Работоспособность модифицированной модели управления качеством ПТК подтверждена в ходе создания конкретного ПТК, связанного с безопасностью, для АЭС «Куданкулам», что обусловливает целесообразность разработки методического обеспечения для внедрения данного подхода в практику управления качеством проектирования потенциально опасных объектов.

Оригинальная междисциплинарная модель когнитивного процесса экспертной верификации открывает возможности:

– для целенаправленного управления процессами обнаружения ошибок и аномалий, не охватываемых традиционным методом поэтапной верификации по предопределенным критериям;

– для комплексного развития теоретических и инструментальных средств поддержки экспертного анализа, активизирующих когнитивные ресурсы экспертов-верификаторов на разных этапах проектирования ПТК.

Литература

1. **Дёрнер Д.** Логика неудачи. Стратегическое мышление в сложных ситуациях. – М.: Смысл, 1997. – 243 с.

2. **Paulk M. and others.** Capability Maturity Model for Software. (CMU/SEI-93-TR-24). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

3. **Абрамова Н.А.** О некоторых мифах в оценке качества программного обеспечения // Надежность, №1, 2004. − С. 38-63.

4. **Бехтерева Н.П.** Мозг человека. Сверхвозможности и запреты. // Доклад на Всемирном Конгрессе «Итоги тысячелетия». – Санкт-Петербург, 2000.

5. **Фестингер Л.** Теория когнитивного диссонанса: Пер. с англ. СПб.: Ювента, 1999. – 318 с.

6. **Kahneman D., Frederick S.** Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin & D. Kahneman (Eds.), Heuristics and Biases Heuristics and biases: The psychology of intuitive judgment (pp. 49-81). New York: Cambridge University Press, 2002.

Abramova N.A., Kovriga S.V., Makarenko D.I.

PRINCIPLES OF QUALITY MANAGEMENT OF COMPLEX HARDWARE AND SOFTWARE SYSTEMS PRIORITIZING MITIGATION OF RISKS CAUSED BY HUMAN FACTOR

In order to reduce the impact of human factor on risks of hazard in operation for the design of safety-critical hardware and software systems, several new principles have been suggested to increase the quality of such systems' design. The findings presented in this paper are based, on the one hand, on psychological and interdisciplinary researches and, on the other hand, on the analysis of the designing practice of complex hardware and software systems of the atomic energy industry.

***Keywords**: hazardous facility, safety, hardware and software system, reliability, human factor-related risks, design quality management.*

Introduction

Today there is a progressive complication of potentially hazardous facilities that use management or decision support methods and systems based on formal methods. The concept of facility (system) complexity, along with more conventional characteristics (quantitative complexity, structural complexity, mathematical models complexity – «organized complexity»), includes the human aspect of complexity when the intellectually complex stage of control and safety ensurance is the initial structuring and formalization of knowledge regarding the designed facilities and the specified requirements.

[1]Because of the inevitable human involvement, the currently used knowledge structuring and formalization methods in the design of complex facilities are generally unable to ensure the reliability of final results. In other words, the results bear reliability risks. Thus, the search for the solution for the problem of human factor-related risks must cover not only the facilities themselves, but also the design process that also involves people. That means that human factors of risk may be related not only with people involved in the facility operation process, but also the developers of management and information technology methods and systems as well as the scientists providing theoretical justification of management methods.

The practical significance of the risks in question with regards to the management of complex facilities is largely confirmed by experimental research of the control subject's thinking process in complex problem situations and analysis of the causes of cognitive errors made during their resolution [1].

[1] Here the reliability is interpreted broadly as the reliability of the results of such methods' application.

The article presents a classification of risks depending on the nature of their influence on the safety of potentially hazardous facilities operating HSSs, proposes several new principles and methods aimed at improving the quality of HSS design. The presented results are based, on the one hand, on psychological and interdisciplinary research and, on the other hand, on the analysis of the design practice of HSS for nuclear power plants.

1. Variety of indirect sources of risk during operation of safety critical hardware and software systems

In order to identify and classify the human factors and risk mechanisms (1) manifesting themselves within the HSS development, deployment and application lifecycle and (2) practically significant to quality management, a selective analysis of complex safety critical HSSs design practice has been conducted (as regards nuclear power plants).

The analysis of the potentially hazardous facilities' HSSs quality assurance practice shows that due to the increasing intellectual complexity of HSSs the conventional methods of quality assurance do not cover the wide range of various indirect safety risks that manifest themselves in practice and cannot be evaluated quantitatively. That primarily pertains to human factor-related risks during HSS design and testing. It is assumed that the conventional approach to safety critical HSS quality assurance is the stage-by-stage verification and validation along with relevant organizational methods and limited use of formal methods whose capabilities amidst the increasing HSS complexity are significantly limited.

Below is the classification of risks depending on the nature of their influence on the safety of potentially hazardous facilities during HSS operation:

- HSS operation-related obviously safety critical risks (i.e. entailing the risk of hazardous situations at the facility),
- indirect risks that do not show obvious connection with hazardous situations.

The indirect risks include:

- technical risks related to the engineering decisions taken during HSS development;
- organizational and managerial risks including those related to the

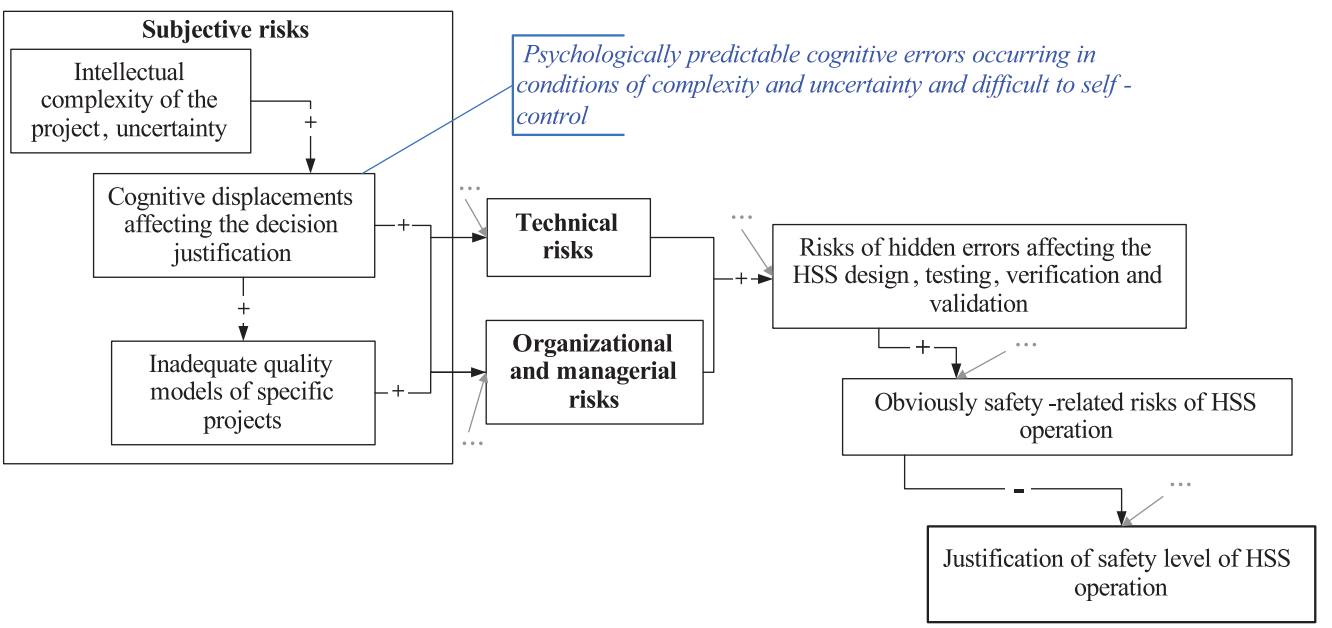


Fig. 1. Human factor-related risks during safety-critical HSS development and their causal relationships

– maturity of the HSS development process in terms of the SW-CMM maturity model [2];
– competence of the parties involved in the manufacturing and managerial processes;
• subjective risks related to cognitive and other particular properties of the parties involved in the manufacturing and managerial processes (according to present-day cognitive science knowledge).

Fig. 1 shows generic risks and causal relationships between those generic risks (the sign «+» indicates a positive influence («the more…, the more…»), while the sign «–» indicates a negative influence («the more…, the less…»); the grey arrows indicate other possible types of risks).

As a result of analysis and classification of risks depending on their influence on the safety of potentially hazardous facilities during HSS operation (1), confirmation was found for the hypothesis of the dependence of human factor-related risks during the design of safety-critical HSS on the functional roles of people in the HSS lifecycle; (2) a hypothesis was developed and tested of the dependence of inadequate quality model of specific projects used by executive managers from well known psychological risk factors called cognitive displacements (psychologically predictable cognitive errors occurring under conditions of complexity and uncertainty that are difficult to self-control). Those include stereotypes of obsolete technology application, systematic underestimation of the significance of unusual requirements.

The diversity of the identified practically significant risks affecting the design of complex safety critical HSS considering the significant role of the human factor along with the practical impossibility of reliable quantitative evaluation of such risks indicate the development of new theoretical approaches to the solution of the problem of complex HSS design quality management.

2. General principles of indirect quality management of safety critical hardware and software systems

The well-known principle of stage-by-stage verification during safety critical HSS development can be considered as an indirect HSS quality management principle. The standard approach involves the verification based on preventive quality criteria of intermediate design products represented in appropriate documentation.

In order to boost the capability of early identification of indirect human factor-related risks (compared to the standard approach to verification), a number of new principles were proposed:

• *wider coverage of diverse indirect risk factors and their causal relationships*, most notably human factors in situations of identification of errors or risks of inadequate technical or managerial decisions in order to improve the efficiency of HSS quality management and to extend the number of control mechanisms;

• *principles of extended verification*, including the verification of not only technical solutions, but the used evaluation methods, namely project quality models (within the available total resources);

• *limited use of formal methods of comprehensive assessment*, specific to safety critical HSS design and testing quality management in order to avoid the risk of inaccurate assessment combined with the verification of the assessment methods themselves. The principle of limited use of formal methods of comprehensive assessment combined with the verification of the methods of assessment is justified by (1) previously found by means of theoretical analysis and practically confirmed possibilities of quality assessment manipulations in conditions of impossibility of reliable quantitative evaluation of risks or other design quality indicators; (2) uncovered risks in the assessment methods themselves suggested by the theory and standards for the purpose of comprehensive assessment of safety critical HSSs;

• *reflexive method of justification analysis* of the technical and managerial decisions that takes into consideration not only the objective justifications of the decisions taken, but also the dependence of the notions of the executive managers from the subjective factors of risk, functional roles and interests. The reflexive method is justified by the existence of a number of practical situations when the identification of unjustified decisions is impossible or complicated if subjective factors are not taken into consideration (e.g. erroneous understatement of requirements to the design of HSS compared to the level of requirements based on the safety class);

• *expert verification without predefined criteria* in addition to conventional verification based on predefined criteria. The method of expert verification without predefined criteria is justified by the

– analysis of the experience of verification and cross analysis of design decisions taken by co-contractors of a specific HSS project;

– interdisciplinary research of psychological mechanisms at the foundation of expert verification, beginning with «error detector» [4], «cognitive dissonance», etc. [5].

In order to increase the quality of the error and risk identification process, verification experts have developed an original interdisciplinary model of the cognitive process of expert verification without predefined criteria. It is comparable with the well-known model of two cognitive systems reflecting the intrinsic human capability to identify errors in justifications [6].

2.1. Model of cognitive process of expert verification without predefined criteria

The fundamental difference between the conventional verification based on predefined criteria from the expert analysis as a verification method is that in the first case the selection of the criteria and the selection (identification) of the verified fragment precede the consistency assessment, while in the case of expert analysis the analyzed material is immediately identified as inconsistent with certain notions of the verification expert. «Immediately» means that the evaluation is the result of intrinsic, not necessarily conscious cognitive processes.

The proposed model of expert verification without predefined criteria is based on a fundamental property of spontaneous identification (localization) if inconsistencies. Furthermore, it is taken into account that, as observations have shown, there are two typical kinds of inconsistence identification. In some cases a fragment of analyzed material (or its property) identified by a verification expert may be immediately assessed as inconsistent with a declared (but not chosen in advance) criterion or requirement. In other cases the assessment is given in the most general expressions like «incorrect», «it can't be», «questionable», «something is wrong», «unclear», «strange» or «anomaly».

By means of subsequent «self-extraction of knowledge» the assessment is explained in such a way that, ultimately, either the inconsistent criterion is identified, or the necessity of further analysis in order to explain the identified irregularity or anomaly is established. In the latter case it is safe to say that we deal with the identification of a risky fragment or general property.

The explanation of cognitive processes resulting in such reaction of the verification expert can be given using the knowledge of cognitive sciences in terms of «cognitive dissonance», «cognitive control», «error detector», «functional body».

However, a more clear and comprehensive notion can result from the use of the computational metaphor and the terms «interrupt system» and related concepts such as «interrupt source», «primary (interrupted) process», «interrupt mechanism», «interrupt service discipline» for connection. The structural organization of expert knowledge processing with interruptions in case of identification of errors and anomalies is shown in Fig. 2.

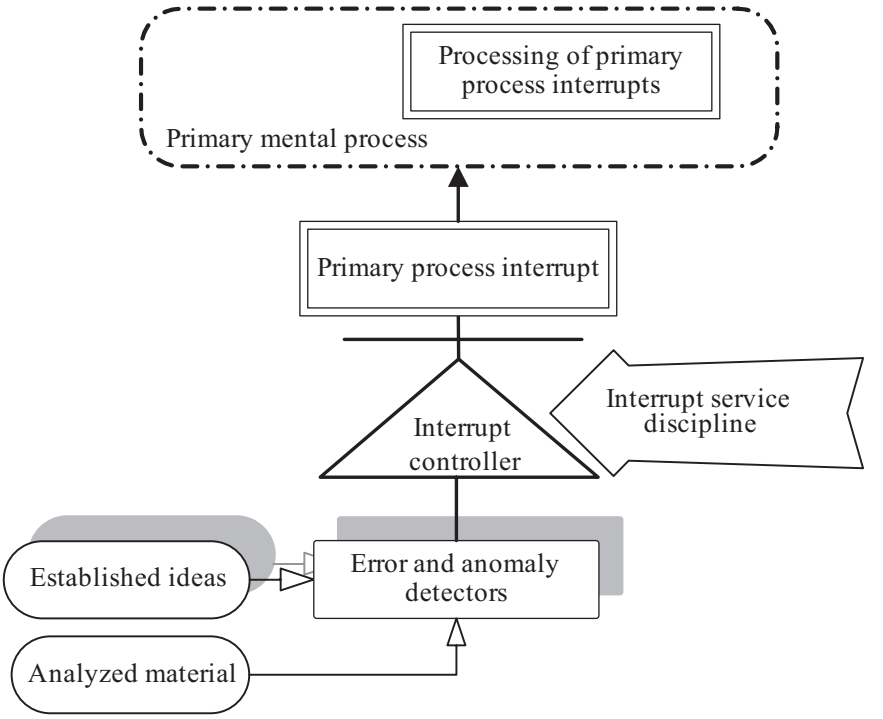


Fig. 2. Structural organization of expert knowledge processing with interruptions in case of identification of errors and anomalies

It appears to be reasonable to consider the identification of inconsistencies as a special case of cognitive dissonance, a psychological discomfort that according to L. Festinger [5] may be caused by the contradiction between the established notions and new information, facts.

The act of inconsistency identification can be interpreted as an operation of an «interrupt system» that carries out cognitive control of the knowledge extracted by the expert from the verification object.

The interrupt system identifies inconsistencies by means of the total of relevant error detectors. Those detectors reflect the stereotypical or at least well assimilated active knowledge in the analyzed area. The identification of an inconsistency by a detector may cause an interruption of the primary process in accordance with an «interrupt service discipline», thus the inconsistency is at least registered by the verification expert and an initial analysis is probably conducted (interruption of the «service»). Given the observation of the identification of risky fragments it is assumed that the detectors can detect not only errors, but also risky and controversial situations.

According to neurophysiologic experiments of N.P. Bekhtereva [4], the action of the mechanism that she called the «error detector» is exercised through emotions that may be considered to be the «interrupt mechanism».

The proposed model of expert verification with two types of knowledge causing a cognitive dissonance allows us to make quite an uncommon conclusion. For the theoretical knowledge to operate as an element of dissonance, the verification expert must have well formed error detectors or at least risk or risky properties detectors that due to their high activity may cause cognitive dissonance and spontaneous interruptions of the primary cognitive process in case of inconsistencies.

The analysis of the practice of safety critical HSS verification in the area of nuclear energy has shown that the proposed model does not only have comparatively significant explanatory capabilities, but also enables the improvement of errors and risks detection process by verification experts, as well as its computer support.

2.2. Modified model of safety critical hardware and software systems quality management

Using the proposed principles, a modified HSS quality management model has been developed that includes, in addition to conventional quality management model with stage-by-stage verification, the identification and assessment within a specific process of HSS design, verification and testing of diverse indirect risk factors active within the HSS lifecycle and their causal relationships with the quality control operations. The general diagram of the modified safety critical HSS quality management model is shown in Fig. 3.

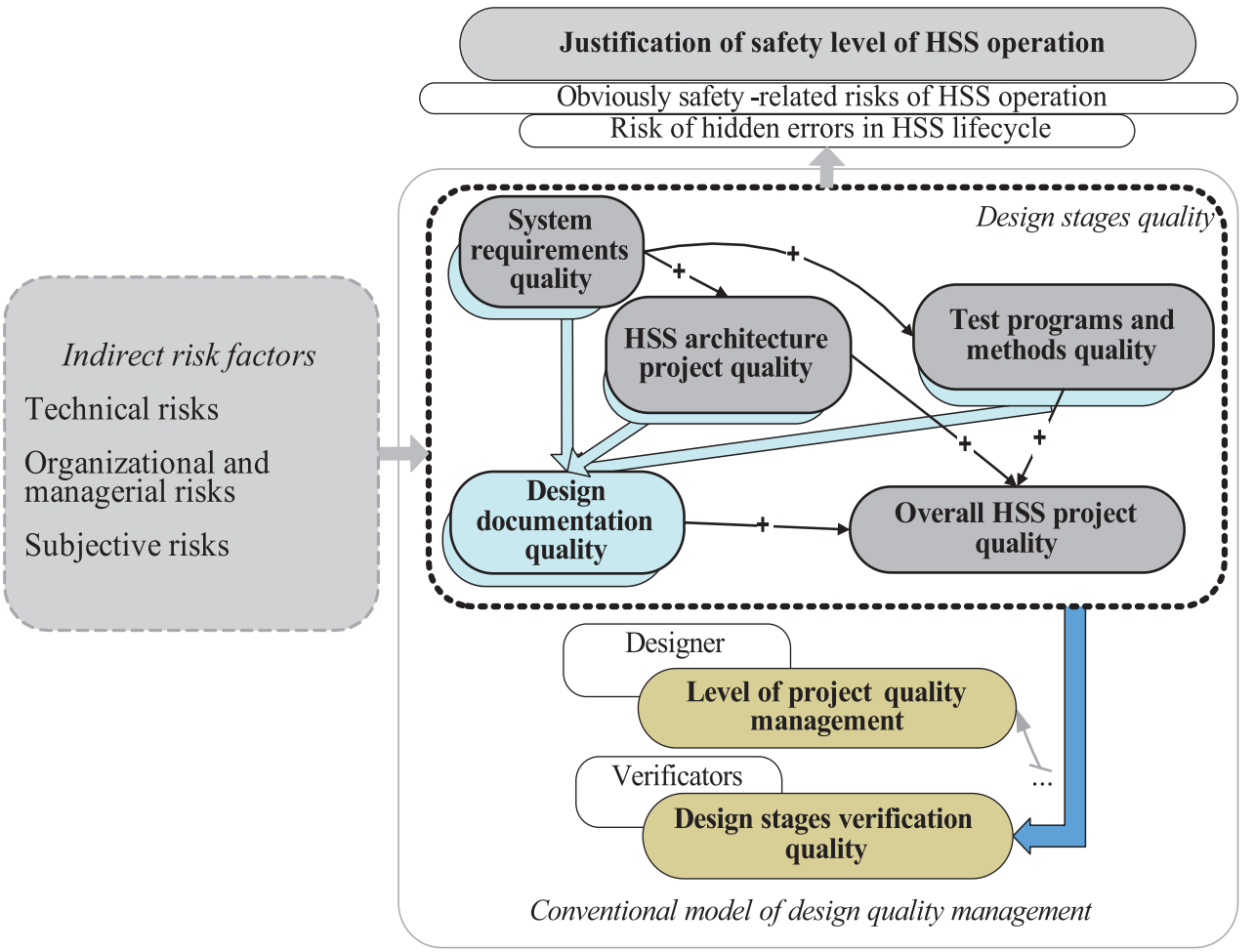


Fig. 3. General diagram of the modified safety critical HSS quality management model

The proposed method that involves the extension of the conventional design quality management model has undergone partial empirical verification as part of the development of a specific safety critical HSS for the Kudankulam nuclear power plant. As part of the HSS project verification a number of significant diverse risk factors were identified beyond erroneous or risky technical decisions (e.g. inconsistency of the system of concepts in the diverse team of an international project, complexity (non-transparency) of the role structure of relationships among project participants, insufficient experience of the developers in the creation of safety critical HSSs). That allowed us to refine the initial quality management model of the project in the form of a cause and effect diagram of indirect influence of the identified factors on the risk of hidden design errors and consequently on the safety level of HSS operation. The modification

enabled the identification of additional control points in order to improve the quality of design. Among other things, it has been confirmed that its application helps coordinate and justify various concepts and notions within a complex role structure of an international project team.

Conclusion

The practical significance of the proposed new principles of indirect HSS quality management consists in the improved capability to manage the quality of such systems' design through identification and recording of human factor-related risks as part of the development of facilities with increased safety and reliability requirements.

The efficiency of the modified model of HSS quality management has been confirmed during the development of a specific safety critical HSS for the Kudankulam nuclear power plant, thus defining the requirement to develop procedural guidelines for its practical application in potentially hazardous facilities design quality management.

The original interdisciplinary model of the cognitive process of expert verification enables

– dedicated management of errors and anomalies identification process management not covered by the conventional method of stage-by-stage verification based on predefined criteria;

– integrated development of theoretical facilities and tools in order to support expert analysis involving more active use of cognitive resources of verification experts at various stages of HSS design.

References

1. **Doerner D.** The logic of failure Strategic thinking in complex situations. Moscow, Smysl, 1997. – 243 p.

2. **Paulk M. and others.** Capability Maturity Model for Software. (CMU/SEI-93-TR-24). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

3. **Abramova N.A.** On some of the myths regarding the quality assessment of software // Dependability, No. 1, 2004. − P. 38-63.

4. **Bekhtereva N.P.** Human brain. Superpowers and Prohibitions. Proceedings of World Congress "Results of the Millennium". – Saint-Petersburg, 2000.

5. **Festinger L.** A Theory of Cognitive Dissonance: Translated from English. Saint-Petersburg: Yuventa, 1999. – 318 p.

6. **Kahneman D., Frederick S.** Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin & D. Kahneman (Eds.), Heuristics and Biases Heuristics and biases: The psychology of intuitive judgment (pp. 49-81). New York: Cambridge University Press, 2002.

Гапанович В.А., Розенберг Е.Н., Шубинский И.Б.

НЕКОТОРЫЕ ПОЛОЖЕНИЯ ОТКАЗОБЕЗОПАСНОСТИ И КИБЕРЗАЩИЩЕННОСТИ СИСТЕМ УПРАВЛЕНИЯ

Приводятся определения опасного отказа и отказобезопасности, обсуждается взаимосвязь и принципиальные различия между функциональной надежностью и функциональной безопасностью, анализируются альтернативы обеспечения отказобезопасности систем управления.
Рассматриваются основные угрозы киберзащищенности, способы реализации кибератак, предлагается концепция обеспечения гарантированного уровня киберзащищенности системы управления.

Ключевые слова: *надежность, отказ, опасный отказ, функциональная безопасность, отказобезопасность, кибератака, киберпространство, киберзащищенность.*

1. Отказобезопасность

Согласно [1] «опасность – ситуация, потенциально оказывающая вред человеку». Это, конечно, относится не только к человеку, но и к ущербам, которые могут быть причинены материальным ценностям или окружающей среде. Не каждая опасность всегда переходит в угрозу. Для этого необходимо, чтобы случилось инициирующее событие. Потом из угрозы может развиваться цепочка нежелательных событий, которая, в конечном счете, сведет к опасному событию, к аварии. Опасное состояние (событие) – это неисправное состояние объектов информационной системы, при котором возникают превышающие допустимые уровни риски причинения вреда жизни и здоровью граждан, имуществу физических и юридических лиц, государственному и муниципальному имуществу, окружающей среде, жизни и здоровью животных и растений.

Итак, безопасность – отсутствие неприемлемого риска. Риск – это комбинация ущерба и вероятности возникновения [2]. В зависимости от последствий можно отдельно рассматривать:

а) функциональную надежность системы, если она выполняет свою функцию (т.е. не теряет определенных свойств) в цепочке всех тех систем, которые участвуют в реализации данной функции;

б) функциональную безопасность, если последствия не сведут к неприемлемым рискам.

Рис. 1 показывает, что со стороны последствий функциональная надежность плавно переходит в функциональную безопасность, если критичность последствий возрастает. Отсюда и понятно, что информационные системы управления, у которых интенсивность отказов в выполнении функ-

ции должна быть не выше 10^{-6} 1 / час, можно толковать с позиций функциональной безопасности [3]. Такие системы часто называют потенциально опасными системами. Для них *опасный отказ* определяется как событие, в результате которого система переходит из исправного, работоспособного или частично работоспособного в опасное состояние.

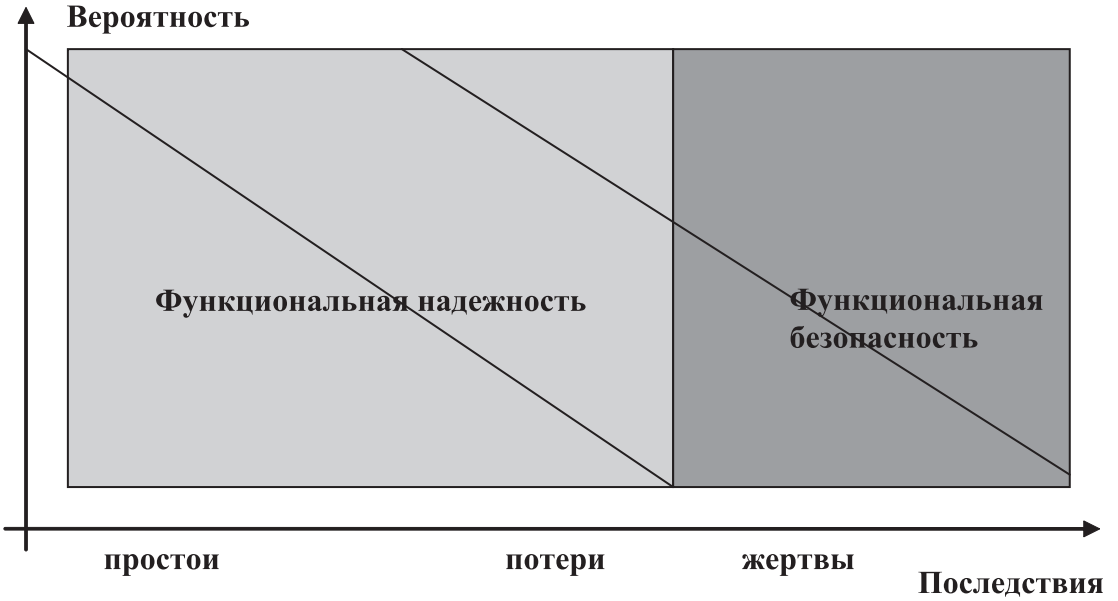


Рис. 1. Функциональная надежность и функциональная безопасность

Отказобезопасность – способность системы управления сохранять безопасное состояние и (или) обеспечивать безопасность управления подчиненными объектами в случае опасных отказов самой системы или ее составных частей.

Проблема обеспечения функциональной безопасности систем управления состоит в исключении влияния их отказов и ошибок в функционировании на объекты управления и окружающую среду, т.е. в исключении так называемых опасных отказов (рис. 2). В результате выдачи неправильных команд управления возможны столкновения поездов, разгерметизация цистерн, пожары, взрывы и т.д. В итоге возникают экономические и экологические ущербы, человеческие жертвы и даже катастрофы.

Полностью исключить влияние отказов и ошибок систем на окружающую среду принципиально невозможно – всегда существует некоторая вероятность возникновения подобных событий. Задача заключается в достижении минимально допустимых значений этих вероятностей. Одним из ключевых направлений в достижении этих целей остается обеспечение высокого уровня надежности систем. Однако возможности резкого повышения надежности известными технологическими, алгоритмическими, структурными и др. методами ограничены, главным образом из-за неприемлемых экономических потерь.

С позиций безопасности не может быть другой альтернативы кроме как прекратить функционирование системы или понизить до предусмотренных пределов ее производительность при недопустимой вероятности возникновения в ней опасного отказа. Отсюда следует необходимость создания технологий гарантированного и достоверного обнаружения отказов в системах. Если правильно реализована технология обеспечения функциональной безопасности, то обеспечивается своевременное обнаружение и блокирование опасных состояний системы.

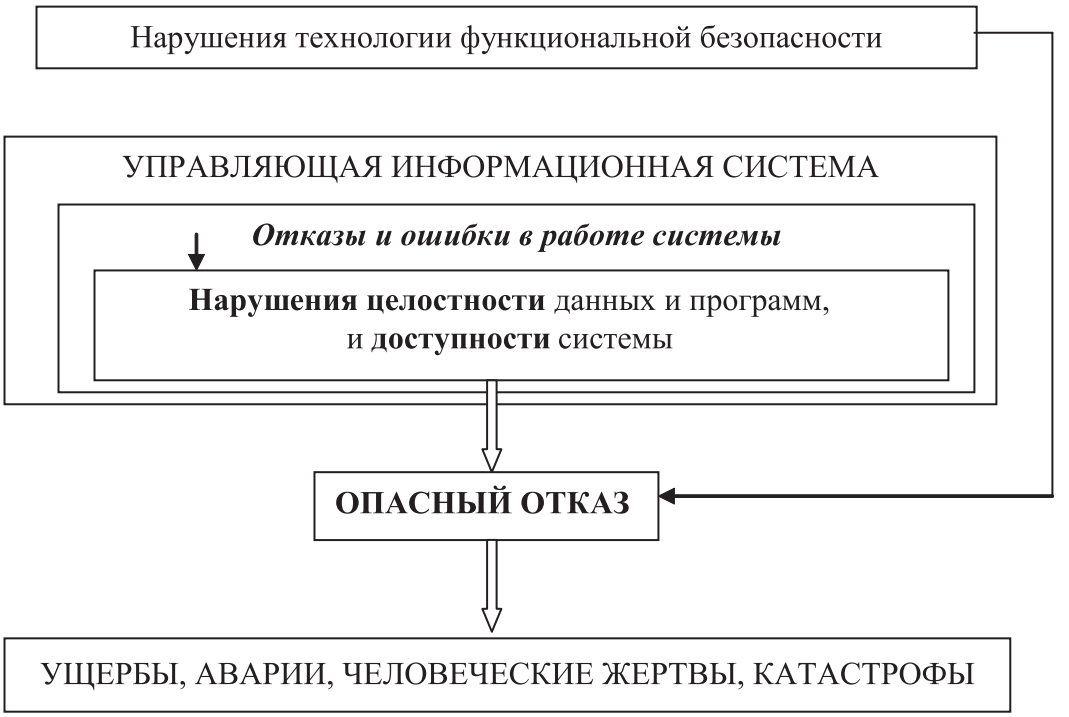


Рис. 2. Угрозы безопасности в управляющих информационных системах

Высокая эффективность обнаружения опасных состояний в ИС достигается с помощью технологий обнаружения отказов, основанных на построении двух, трех и более параллельных каналов управления. Параллельное формирование и сравнение выдаваемых команд управления обеспечивает уверенность в обнаружении опасных состояний при условии построения безопасных алгоритмов или устройств сравнения (так называемых компараторов), обеспечения независимости каналов и данных, несимметричности отказов каналов и при выполнении целого ряда других условий. Вместе с тем, для реализации указанной технологии обнаружения отказов дополнительно требуется включение в состав системы значительного объема аппаратных и программных средств, что приводит к снижению ее надежности.

Из указанных положений следует:

– между содержанием безопасности и надежности систем имеют место принципиальные различия – если ненадежность приводит к неприемлемым уровням готовности, технического использования, безотказности и стоимости технического обслуживания, то недостаточная безопасность приводит к авариям и человеческим жертвам;

– между целями обеспечения надежности и функциональной безопасности систем существуют противоречия, устранение которых возможно на основе компромисса, требования к надежности и функциональной безопасности должны быть между собой сбалансированы;

– в критически важных, потенциально опасных объектах, или объектах, представляющих повышенную опасность, приоритеты отдаются задачам обеспечения безопасности, а требуемые уровни надежности должны задаваться с учетом ограничений по стоимости после выполнения требований по безопасности.

Для обеспечения отказобезопасности систем нужно проделать тот же путь, что и для обеспечения отказоустойчивости, т.е. создать условия для наблюдаемости и управляемости системы. На основе принципа приемлемости остаточного риска при имеющихся ограничениях в затратах средств необходимо в полной мере реализовать возможности по обеспечению отказоустойчивости и функциональной безопасности.

2. Киберзащищенность

Проблема обеспечения отказобезопасности в системах управления неразрывно связана с вопросами обеспечения их информационной защищенности, в первую очередь, от кибератак. Термин *кибер* определяется как «имеющий отношение к информационным технологиям» [4]. Информационные технологии реализуются в так называемом *киберпространстве*, под которым понимается «среда, созданная при помощи физических и не физических компонентов, характеризуемая использованием компьютеров и электромагнитного диапазона для хранения, изменения и обмена данными при помощи компьютерных сетей» [4]. Использование кибернетических возможностей, с целью достижения задач в киберпространстве или при помощи использования киберпространства определяется как «кибероперация». Теперь мы вплотную подошли к определению понятия *кибератака* – это кибероперация как наступательная, так и оборонительная, которая приводит к телесным повреждениям или человеческим потерям, или нанесению ущерба, или разрушению объектов.

Опираясь на приведенные выше понятия, можно определить **киберзащищенность, как способность системы управления успешно выполнять предусмотренные задачи при сохранении безопасного состояния в условиях кибератак, направленных на нанесение ущерба критически важным или потенциально опасным объектам, или объектам, представляющим повышенную опасность для жизни и здоровья граждан, имуществу физических или юридических лиц, экономике, окружающей среде.**

Основными угрозами нарушения киберзащищенности в информационно-управляющих системах являются (рис. 3):

- Информационные атаки (в первую очередь кибератаки);
- Недекларированные возможности в программах и устройствах систем;
- Отказы и ошибки в работе систем, в том числе аппаратные и программные сбои и ошибки, ошибки операторов, ошибки данных.

На рис. 2. показано, что киберзащищенность системы зависит как от возможностей несанкционированного доступа к системе (НСД) вероятного противника, так и от недекларированных возможностей (НДВ), которые имеют место в программных и аппаратных средствах. Несанкционированный доступ реализуется путем информационных атак (кибератак) на систему.

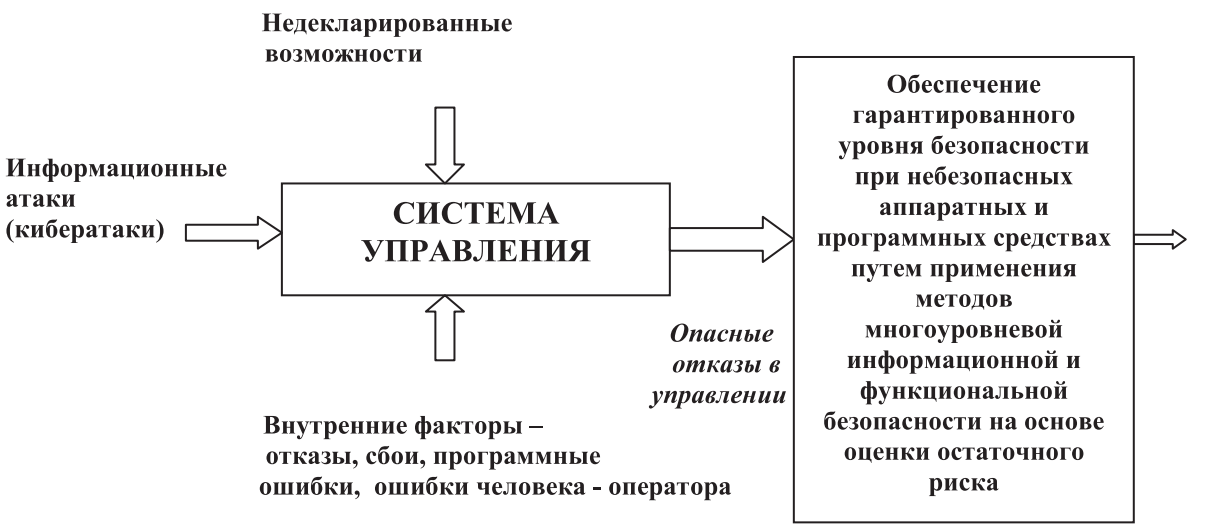


Рис. 3. Концепция обеспечения гарантированного уровня киберзащищенности системы управления

Полное устранение опасных отказов в управлении теоретически возможно, но практически неосуществимо, поскольку потребует экономических затрат, заведомо больших, чем ожидаемый ущерб от воздействия опасных отказов. Реальный путь – это определение допустимого уровня риска от кибератак и создание эффективной защиты от опасных отказов.

Рассмотрим более подробно перечисленные угрозы.

Результатом успешной кибератаки может стать нарушение целостности или доступности информации. В качестве целей атаки могут рассматриваться серверы, рабочие станции пользователей или коммуникационное оборудование информационной системы. При организации кибератак злоумышленники часто используют специализированное ПО, позволяющее автоматизировать действия, выполняемые на различных стадиях атаки.

В общем случае в любой кибератаке можно выделить четыре стадии:

Рекогносцировка. На этой стадии нарушитель старается получить как можно больше информации об объекте атаки, чтобы на ее основе спланировать дальнейшие этапы вторжения. Этим целям может служить, например, информация о типе и версии операционной системы; список пользователей, зарегистрированных в системе; сведения об используемом прикладном ПО и т.д.

Вторжение. На этом этапе нарушитель получает несанкционированный доступ к тем ресурсам, на которые совершается атака.

Атакующее воздействие. На данной стадии реализуются те цели, ради которых и предпринималась атака, – например, нарушение работоспособности системы, удаление или модификация данных и т.д. При этом атакующий часто выполняет операции, направленные на удаление следов его присутствия в системе. Всякая атака основана на наличии в системе управления уязвимостей и «правильное» использование хотя бы одной из них открывает злоумышленнику вход в систему.

Развитие атаки. После атакующего воздействия нарушитель стремится перевести атаку в фазу дальнейшего развития. Для этого в систему обычно внедряется вредоносная программа, с помощью которой можно организовать атаку на другие средства системы. Основные угрозы киберзащищенности информационным системам (ИС) создают следующие группы вредоносных программ: ***DoS-атака*** (от англ. Denial of Service, отказ в обслуживании) – атака на информационную систему, с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён. Отказ «вражеской» системы может быть одним из шагов к овладению системой (если во внештатной ситуации ПО выдаёт какую-либо критическую информацию – например, версию, часть программного кода и т. д.); ***троянские программы –*** после внедрения в систему нарушают целостность данных и программ или рассаживают вирусы в системе. Они также могут собрать сведения о хранящихся на компьютере профилях пользователей, паролях и другую конфиденциальную информацию и затем переслать ее в руки злоумышленников; ***программы несанкционированного управления компьютерами ИС (****загрузочные вирусы, программные вирусы, сетевые черви и др.)*

Недекларированные возможности – функциональные возможности программных или аппаратных средств, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение доступности, целостности, а также конфиденциальности обрабатываемой информации. Реализацией недекларированных возможностей, в частности, являются программные или аппаратные закладки.

В результате реализации указанных угроз возникают опасные отказы, которые приводят к недопустимым ущербам объектам, которые для хозяйствующего субъекта относятся к категории объектов с повышенной опасностью или к категории потенциально опасных объектов, а на уровне

государственных или региональных органов опасные отказы могут приводить к недопустимым ущербам критически важных объектов. Последнее обстоятельство объясняется тем, что ответственность за защиту критически важных объектов возлагается на государственные или региональные органы.

Угрозы нарушения киберзащищенности систем управления аналогичны угрозам нарушения отказобезопасности. Принципиальное различие в том, что кибератаки – это специфический класс информационных атак, направленный на нанесение ущерба или разрушение объекта управления, который относится к одной из отмеченных выше трех групп важных объектов.

В вопросах обеспечения киберзащищенности, также как и в вопросах обеспечения отказоустойчивости и отказобезопасности, целесообразно опираться на следующие основные **постулаты***:*

1. Не существует абсолютной киберзащищенности (отказоустойчивости, отказобезопасности) систем управления.

2. Чем более сложная система, чем больше задач она выполняет, тем ниже ее киберзащищенность.

3. Необходимым условием повышения киберзащищенности системы является введение избыточности в сочетании с организацией эффективного контроля.

4. Киберзащищенность системы управления должна обеспечиваться на всех этапах жизненного цикла.

5. Уровень киберзащищенности системы ограничен экономическими рисками заказчика и эксплуатирующей организации.

Абсолютной киберзащищенности невозможно достичь, поскольку устранение одних уязвимостей в системе не исключает возможности появления новых. Проблема обеспечения киберзащищенности – это проблема совершенствования щита от нападения меча. Одновременно с повышением уровня защиты совершенствуются средства нападения и не факт, что эффективность средств защиты в определенные отрезки времени сколь угодно выше эффективности средств нападения.

Кардинальное решение задачи состоит в том, чтобы обеспечить **гарантированный уровень киберзащищенности при небезопасных аппаратных и программных средствах путем применения многоуровневой информационной и функциональной системы защиты на основе оценки остаточного риска** (рис. 3).

Примерами реализации принципов многоуровневой безопасности на железнодорожном транспорте могут быть [5]:

● ***многоуровневое обеспечение безопасности каждого автономного устройства управления.*** Пусть в этом программно-аппаратном устройстве предусматривается *несколько* функций безопасности. Одна или одновременно несколько функций безопасности в случае возникновения отказа выполняют задачу перевода устройства в неопасное состояние, – это могут быть состояния допустимых пониженных функциональных возможностей или защитные состояния, когда блокируется выдача управляющих воздействий;

● ***многоканальная безопасная многоуровневая система (МС) из разнотипных устройств или систем.*** Суть в том, что два или более устройств (систем) управления выполняют на определенном участке дороги аналогичные функции управления, которые реализуются разными способами и алгоритмами. Результаты каждого управления проверяются на непротиворечивость. Если это условие выполняется, то осуществляется управление. В противном случае осуществляется дополнительная проверка и принимается решение о введении защитного отказа одного из устройств или о продолжении его работы в составе МС, но с пониженной производительностью. Если в произвольный момент времени функции управления не противоречивы, то МС продолжает выполнять функции управления с заданной производительностью.

● ***система с выбором более запрещающего сигнала.*** В многоуровневую систему вводится устройство принятия решения, которое реализует следующее правило: если функции управления не противоречивы, но не совпадают по уровням градации опасности управления, то выбирается менее опасное управление. Например, если на выходе первого устройства железнодорожной автоматики и телемеханики сформировано управление светофором *«красный»*, а на выходе второго устройства – «*красно-желтый*», то на выходе системы формируется сигнал управления светофором *«красный»*.

● ***создание системных функций безопасности в развивающихся многоуровневых системах.*** Развивающаяся многоуровневая система – это система, которая обладает возможностями и способностями формировать новые свойства управления и/или новые функции безопасности. В дальнейшем будем рассматривать развивающуюся систему, которая формирует только новые функции безопасности. Суть принципа в следующем: в системе вместе с устройством принятия решения (или вместо него) вводится подсистема поддержки принятия решения (ППР). Кроме того, для каждого составного устройства или составной системы железнодорожной автоматики и телемеханики вводится дополнительный логический контроль состояний безопасности, который осуществляется путем запоминания, анализа, корреляции с указаниями составных устройств логических последовательностей смены состояний напольного оборудования автоматики и телемеханики. Путем совместной обработки в ППР команд управления с выходов этих устройств или систем и данных логического контроля формируются их дополнительные функции безопасности.

3. Заключение

Для обеспечения отказобезопасности систем управления нужно создать условия для наблюдаемости и управляемости системы.

На основе принципа приемлемости остаточного риска при имеющихся ограничениях в затратах средств необходимо в полной мере реализовать возможности по обеспечению отказоустойчивости и функциональной безопасности.

Для обеспечения киберзащищенности системы управления целесообразно комплексно реализовать меры по обеспечению информационной защищенности, надежности, и, особенно, функциональной безопасности. Кардинальное решение задачи состоит в том, чтобы обеспечить гарантированный уровень киберзащищенности при небезопасных аппаратных и программных средствах путем применения многоуровневой информационной и функциональной безопасности на основе оценки остаточного риска.

Литература

1. ИСО 9126 ГОСТ Р ИСО/МЭК 9126-93, Оценка программной продукции, характеристика качества и руководства по их применению, 28.12.93

2. ГОСТ Р/МЭК 61508. Функциональная безопасность электрических/ электронных/ программируемых электронных систем безопасности. – 2010.

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

4. Таллиннский справочник по международному праву, применимому к кибернетическим способам ведения военных действий. – 2013.

5. **Rozenberg E.N, Shubinskiy I.B.** Functional Safety of RailwayAutomation Systems: Methods and Models. Moscow: VNIIAS MPS UIC, 2005.- 155 p.

Gapanovich V.A., Rozenberg E.N., Shubinsky I.B.

SOME CONCEPTS OF FAIL-SAFETY AND CYBER PROTECTION OF CONTROL SYSTEMS

The paper provides some definition of a hazardous failure and fail-safety, discusses relations and principal differences between functional reliability and functional safety, and analyzes alternatives for ensuring fail-safety of control systems.
The paper considers major threats to cyber protection, ways of implementing cyber attacks, offers a concept of ensuring a guaranteed cyber protection level of control systems.

Keywords: *reliability, failure, hazardous failure, functional safety, fail-safety, cyber attack, cyber space, cyber protection.*

1. Fail-safety

According to [1], "a hazardous event is a situation potentially causing damage for a human being". Of course, it applies not only to a human being but also to damages that can be caused for material assets or environment. Not every hazard always brings a threat. For that to happen, a causing event should take place. Afterward a threat can result in a chain of undesirable events that ultimately will lead to a hazardous event, to an accident. A hazardous state (event) is failed state of IT system objects when there occur unacceptably high risks of damages for the life and health of citizens, assets of persons and companies, state and municipal assets, environment, the life and health of animals and vegetation.

Therefore, safety is an absence of unacceptable risk. The risk is a combination of damage and probability of occurrence [2]. With consequences taken into account, we can separately consider:

a) functional reliability of a system if it performs its function (i.e. does not lose certain properties) in a chain of all those systems that are involved in implementing that function;

b) functional safety if consequences will not lead to unacceptable risks.

Fig. 1 shows that in terms of consequences functional reliability smoothly transits into functional safety if criticality of consequences increases. Hence it is clear that IT control systems whose failure rate in implementation of a function should not be higher than 10^{-6} 1 / hour can be treated in terms of functional safety [3]. Such systems are often called potentially hazardous systems. For such systems *a hazardous failure* is defined as an event resulting in transit of a system from good, operating or partially operating state into hazardous state.

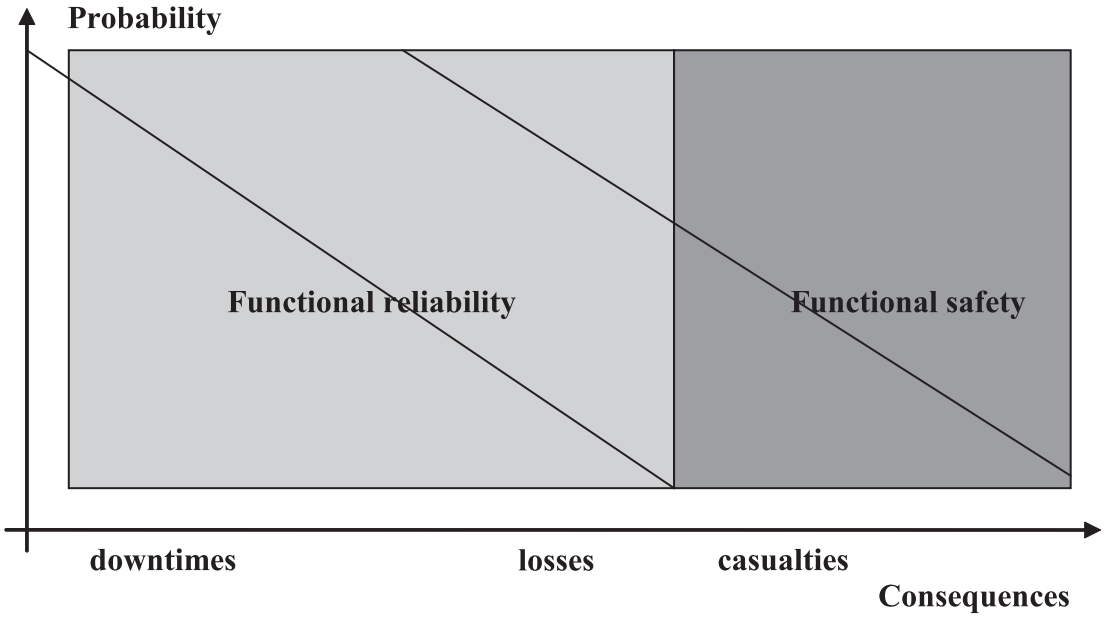


Fig. 1. Functional reliability and functional safety

Fail-safety is a control system's ability to retain safe state and (or) to ensure the safety of controlling subordinate objects in case of hazardous failures of a system itself or its components.

The issue of ensuring the functional safety of control systems consists in eliminating the influence of their failures and faults on controlled objects and environment, i.e. eliminating the so-called hazardous failures (Fig. 2). Giving wrong commands can bring train crashes, tank leakage, explosions etc. It results to economical and ecological damages, casualties and even disasters.

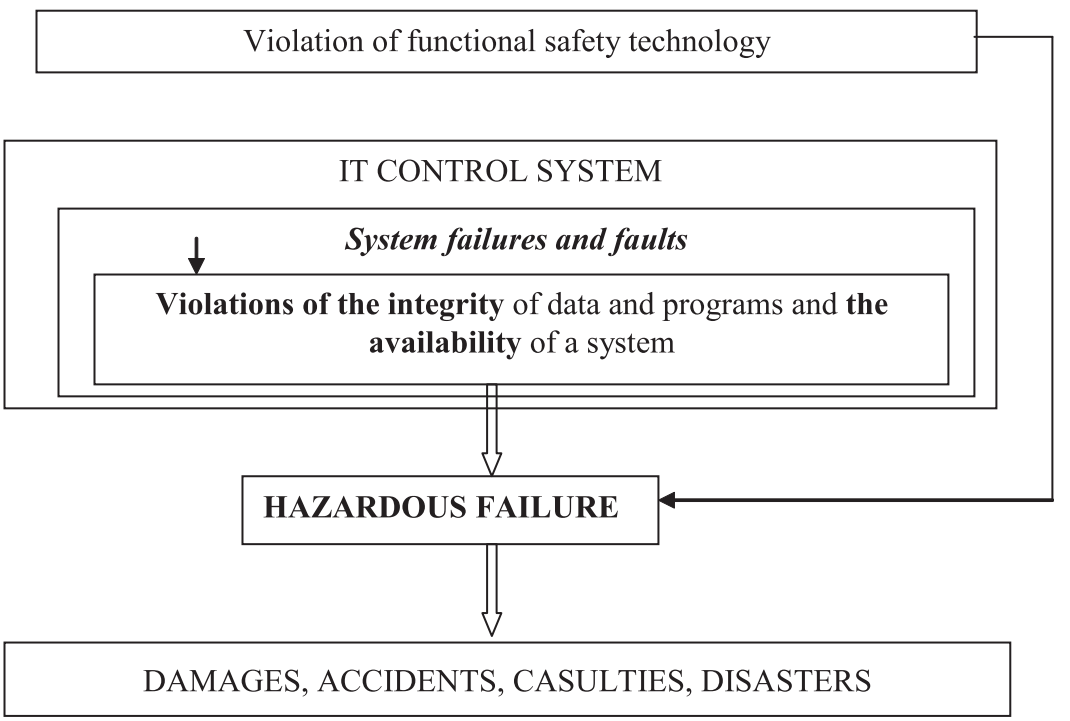


Fig. 2. Threats to safety of IT control systems

In principle, we cannot entirely rule out the influence if failures and faults of systems on the environment since there is always some probability of such events happening. Our task is to achieve minimum

values of such probabilities. One of the ways to achieve them is to ensure a high level of system reliability. However, the possibilities of radically increasing the reliability by means of technological, algorithmical, structural and other methods are limited, mainly due to unacceptable economical losses.

In terms of safety, there can be no other alternative than to stop a system's functioning or to decrease its capacity to predefined levels in case of unacceptable probabilities of a hazardous failure occurring in it. Hence, it is necessary to develop technologies of guaranteed and confident detection of system failures. If functional safety is ensured in a right way, then system hazardous states are duly identified and eliminated.

Hazardous states are effectively identified in IT systems by using detection technologies based on development of two, three and more control channels working in parallel. Parallel generation and comparison of commands secure detection of hazardous states provided that there are safe algorithms or comparing devices (so-called comparator circuits), independence of channels and data, unsymmetrical failures of channels ensured and other conditions satisfied. Yet, to implement this technology of failure detection, it is required to introduce an extra considerable amount of HW and SW into systems, thus reducing its reliability.

The above said leads to the following:

– the safety and the reliability of systems have principal differences: if unreliability leads to unaccepted levels of availability, maintenance, non-failure operation and maintenance costs, then insufficient safety leads to accidents and casualties;

– the objectives of ensuring the reliability and the functional safety of systems have contradictions that can be eliminated on the basis of some compromise, so the requirements for reliability and functional safety should be well balanced together;

– in safety critical, potentially hazardous objects, or objects presenting increased hazards, the tasks of safety ensuring are prioritized, while required level of reliability should specified with cost limits taken into account, after safety requirements have been implemented.

In order to ensure system fail-safety, we should go the same way that we go to ensure fault-tolerance, i.e. create conditions when a system is observable and controllable. Based on the principle of acceptability of a residual risk with existing financial limits taken into account, it is necessary to fully realize the possibilities of ensuring fault-tolerance and functional safety.

2. Cyber protection

The issue of fail-safety in control systems is closely related to the issues of their IT protection, above all, against cyber attacks. The term *cyber* is defined as "bearing a relation to IT technologies" [4]. IT technologies are implemented in the so-called *cyber space* that is understood as "environment created by means of physical and nonphysical components characterized by use of personal computers and electromagnetic band to store, change and exchange data via computer networks" [4]. Use of cybernetic capabilities aiming to implement some goals in cyber space or by means of cyber space is defined as *cyber operation*. Now we have come close to the definition of the term cyber attack. This is *cyber operation*, either offensive or defensive one that causes human damages or casualties, or damage to or destruction of objects.

Based on the above definitions, we can define **cyber protection as the ability of a system to successfully perform specified tasks under the conditions of cyber attacks aiming to make damage to safety critical or potentially hazardous objects, or objects presenting an increased threat for the life and health of citizens, assets of persons and companies, economy, environment.**

The main threats to cyber protection in IT control systems are as follows (Fig. 3):
- IT attacks (cyber attacks in the first place);
- Undocumented features of SW/HW;
- Failures and faults, including HW/SW errors and glitches, operator mistakes, data errors.

Fig. 2 shows that a system's cyber protection depends on unauthorized access capabilities of a potential attacker as well as on undocumented features that occur in HW and SW means. Unauthorized access is realized by means of information attacks (cyber attacks) at a system.

In theory, full elimination of hazardous failures in control systems is possible but in practice, it is not feasible as it will take expenditures much higher than expected damages due to hazardous failures. The most realistic way is to define an acceptable level of risks due to cyber attacks and to develop efficient protection against hazardous failures.

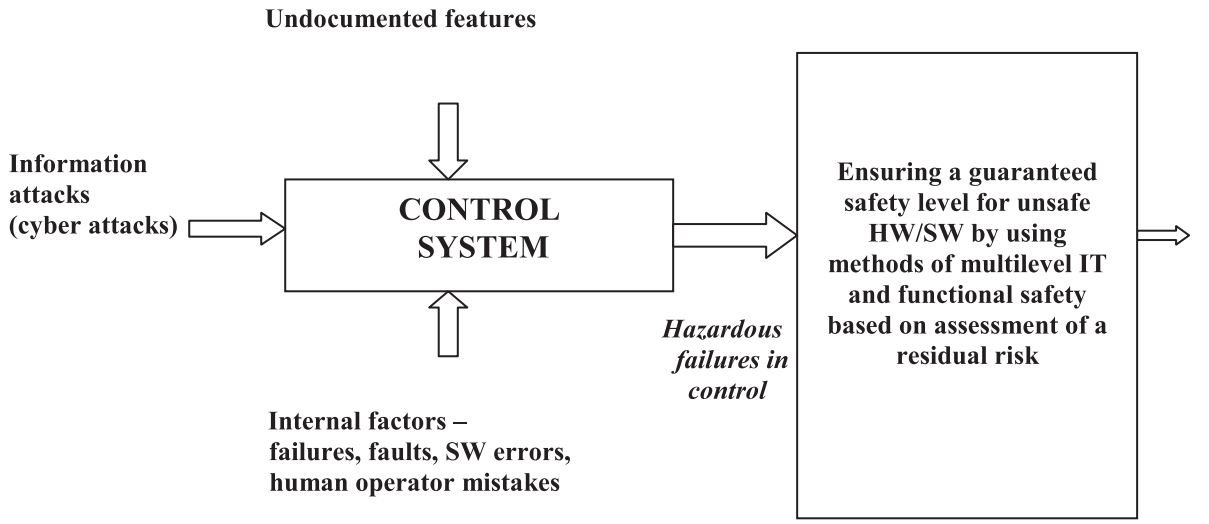


Fig. 3. The Concept of ensuring a guaranteed safety level of control systems

Let us consider the above listed threats in more detail.

A successful cyber attack can result in violations of information integrity or availability. An attack can target servers, personal. For implementation of cyber attacks, intruders often use specialized SW that provides automation for actions performed at different stages of an attack.

Generally, four stages can be identified in any cyber attack:

Reconnaissance. At this stage an introduer attempts to get as much information as possible about an attack object in order to plan further stages of intrusion on its basis. To this end he can target, for example, information about the type and version of an operating system, a list of users registered in the system, data about applied SW used in the system etc.

Intrusion. At this stage an intruder get an unauthorized access to those resources that are under attack.

Attack perpetration. At this stage an intruder realizes the goals that motivated the attacker, for example, violation of IT system operation, deletion or change of data etc. while doing this, an intruder often performs actions aiming at deletion of the traces of his presence in the system. Each attack is based on the fact that a control system has some vulnerabilities, and the "right" use of at least one of them opens the door for an intruder to the system.

Attack progression. After attack perpetration, an intruder aims to go to the stage of its further progression. To that end, he usually implants into a system some malicious program that helps to arrange an attack at some other nodes of an IT system. Major threats for IT system cyber protection are presented by the following groups of malicious programs: ***DoS attack*** (Denial of Service) that is an attack at an

IT system aiming at its failure, i.e. creating such conditions when legitimate (authorized) users cannot get an access to resources (servers) provided by the system or this access gets complicated. An "enemy" system's failure can be one of the steps to get hold of a system (if SW generates some critical information in emergency – for example, version, part of a program code etc.); ***Trojan programs*** *when implemented into a system disrupt the integrity of information and programs or generate viruses in the system*. They can also collect information about user profiles stored on a PC, passwords and other confidential data with further sending it to intruders; ***programs of unauthorized control of information system PCs (****boot viruses, SW viruses, network viruses etc.)*

Undocumented features are HW and SW functional features not specified or not compliant with those described in specifications, whose application can cause violation of availability, integrity as well as confidentiality of processed information. For example, SW and HW bugs belong to undocumented features.

Implementation of the above listed threats results in hazardous failures that lead to unacceptable damages of objects, which in terms of an operating company belong to the category of objects with increased hazards or to the category of potentially hazardous objects, and in terms of state or regional authorities hazardous failures can cause unacceptable damages for critical infrastructure. The latter is explained by the fact that responsibility for critical infrastructure protection is put on state or regional authorities.

Threats of cyber protection violations are similar to threats of fail-safety violations. A principal difference is that cyber attacks are a specific class of information attacks aiming at damaging or destructing a control object that belong to one of the three groups of critical objects.

When dealing with the issues of cyber protection, as well as fail-safety and fault-tolerance, it is reasonable to rely on the following **postulates**:

1. There is no absolute cyber protection (fail-tolerance, fail-safety) of control systems.
2. The more complicated a system is, the more number of tasks it performs, the lower its cyber protection is.
3. A prerequisite for enhancing the cyber protection of a system is redundancy in combination with organization of efficient control.
4. The cyber protection of a control system should be ensured at all stages of its life cycle.
5. The level of cyber protection is restricted by economical risks of a customer and operating company.

Absolute cyber protection cannot be reached since elimination of vulnerabilities of one type does not rule out the possibility of new vulnerabilities appearing. The problem of ensuring cyber protection is the problem of improving a shield against a sword's attacks. Along with the increase of a protection level, attack means are improved, and one cannot guarantee that the efficiency of protection means at certain times is much higher than the efficiency of attack means.

The radical solution of the task consists in **ensuring a guaranteed level of cyber protection for unsafe HW/SW by using multilevel IT and functional safety based on assessment of residual risk** (Fig. 3).

The implementation of multilevel safety principles on railway transport can be exemplified as follows:

Multilevel safety ensuring for each standalone control device. Let this HW/SW complex provide for *several* safety functions. One or several safety functions simultaneously performs the task of switching the device into safe state in case of failure, which can be states of acceptable decreased functionality or states of protection when generation of commands is blocked;

Multichannel safe multilevel system made of devices or systems of different types. The point is that on a certain railway section two or more control devices (systems) perform analogous control functions that are implemented by different ways and algorithms. The results of each controlling action are checked

for consistency. If the condition is satisfied, then controlling is realized. Otherwise, an additional check is done and a decision is made on introducing a safe failure of one of the devices or its further operating as part of a multilevel system, but with decreased performance. If at some random moment of time control functions are not contradictory, then a multilevel system keeps on performing control functions with predefined efficiency.

System of choosing a more restrictive aspect. A decision making device is introduced into a multilevel system. This device realizes the following rule: if control functions are not contradictory, then a less hazardous control is chosen. For example, if the output of the first device of railway signalling and remote control generates "at danger" light signal, and the output of the second one generates "red and yellow" signal, then the output of the system generates "at danger" control signal.

Development of system functions of safety in developing multilevel systems. A developing multilevel system is a system that has possibilities and abilities to generate new controlling properties and/or new safety functions. Further on we'll consider a developing system that only generates new safety functions. The essence of the principle is as follows: a decision making support subsystem is introduced into a system along with (or instead of) a decision making device. Also, for each composite device or composite system of railway signalling and remote control, an additional logical control of safety states is introduced. This control is realized by means of memorization, analysis, correlation with indication of composite devices of logical consequences as regards changes of states of trackside signalling and remote control equipment. By jointly processing control commands from the outputs of these devices or systems and data of logical control in decision making support systems, their additional safety functions are generated.

3. Conclusion

In order to ensure the fail-safety of control systems, it is necessary to create conditions when a system is observable and controllable.

Based on the principle of acceptability of a residual risk under the existing limits of financial resources, it is needed to fully realize possibilities in ensuring fail-safety and functional safety.

To ensure the cyber protection of a control system, a complex of measures for ensuring IT protection, reliability and, in particular, functional safety should be implemented. A radical solution of the task is in ensuring a guaranteed cyber protection level for unsafe HW/SW by using multilevel IT and functional safety based on assessment of residual risk.

References

1. ISO 9126 GOST R ISO/IEC 9126-93 Information technology. Software product evaluation. Quality characteristics and guidelines for their use, 28.12.93

2. GOST R/IEC 61508. Functional safety of electrical, electronic, programmable electronic safety-related systems, 2010.

3. **Shubinsky I., Schäbe H.** On the definition of functional reliability. Dependability, 2012. – №4, pp. 74-84.

4. Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013.

5. **Rozenberg E.N., Shubinskiy I.B.** Functional Safety of RailwayAutomation Systems: Methods and Models. Moscow: VNIIAS MPS UIC, 2005.- 155 p.

Бочков К.А., Сивко Б.В.

ВЫБОР И ОПРЕДЕЛЕНИЕ ФУНКЦИИ БЕЗОПАСНОСТИ ПРИ ВЕРИФИКАЦИИ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Рассмотрены вопросы определения, формализации и выбора функции безопасности, применяемой при разработке и доказательстве корректности программного обеспечения микропроцессорных систем железнодорожной автоматики и телемеханики. Приведены способы выбора функции безопасности на основании технического задания, ограниченности ресурсов, используемой стратегии обеспечения безопасности и общих требований к характеристикам системы.

Ключевые слова: *верификация, валидация, функциональная безопасность, функция безопасности, доказательство корректности, критически важные объекты информатизации.*

В настоящее время в новых разработках широко используется микроэлектронная база в системах железнодорожной автоматики и телемеханики (СЖАТ), что расширяет её возможности и позволяет реализовывать и предоставлять более широкую функциональность для эксплуатируемых систем. Но в то же время разработка, верификация и последующая эксплуатация данных систем должны соответствовать и удовлетворять принятому на железнодорожном транспорте уровню безопасности. Традиционно в СЖАТ использовалась релейная база, когда построение происходило на принципе аппаратной реализации функций безопасности, а микропроцессорные системы представляют собой аппаратно-программные комплексы (АПК), большинство функций которых реализуется программно. В то же время при построении современных микропроцессорных СЖАТ преобладающим способом является использование COTS-технологий, но при этом разработка программного обеспечения (ПО) является наиболее сложным элементом этих систем. Кроме того, для микроэлектронных СЖАТ отсутствуют единые, универсальные и общепризнанные способы доказательства безопасности и в связи с этим необходимо применять комплекс методов и средств по повышению уровня безопасности на всех этапах жизненного цикла системы, а разработка новых способов доказательства безопасности является актуальной задачей.

Одним из возможных способов поиска ошибок и повышения качества ПО в рамках применяемого комплекса подходов является доказательство корректности, которое относится к формальным методам (*Formal Methods*) [1] и успешно используется для верификации микропроцессорных устройств на Белорусской железной дороге [2, 3, 4]. Для систем, связанных с безопасностью, стандарт IEC 61508 имеет градацию уровней полноты безопасности от SIL-1 до SIL-4, а железнодорожные систе-

мы должны соответствовать наиболее строгому уровню SIL-4, который настоятельно рекомендует применение формальных методов для критически важных систем информатизации [5].

Формальные методы в качестве доказательства корректности могут быть применены как для готового ПО, так и на ранних этапах разработки всего АПК, но в любом случае одним из первых шагов верификации является определение функции безопасности, подлежащей проверке на корректность [4, 6].

Функция безопасности представляет собой формализованное условие по отношению к верифицируемой системе, выполнение которого позволяет сделать заключение о безопасности функционирования СЖАТ. Для одного и того же АПК функция безопасности может быть определена по-разному, а выбор доказываемого условия может происходить на разных этапах жизненного цикла системы.

Разработка и эксплуатация ПО, а также ряд исследований говорят о том, что чем позже обнаруживается ошибка, тем сложнее как выявить её, так и исправить, и тем больше проблем она может принести [7, 8]. При этом исправление ошибок, допущенных при формулировании требований к системе, обходится в десятки раз дороже ошибок, допущенных во время реализации [9, 10]. Определение функции безопасности, которое относится к формализации решаемой задачи, является спецификацией по отношению к доказательству корректности и обладает теми же свойствами, что и постановка требований при разработке ПО. Потенциальные ошибки, допускаемые при определении данной функции, негативно влияют на качество верификации и могут приводить к искажению результатов доказательства корректности и, как следствие, его полному пересмотру.

На рис. 1 показана последовательность этапов анализа на безопасность с определением функции безопасности.

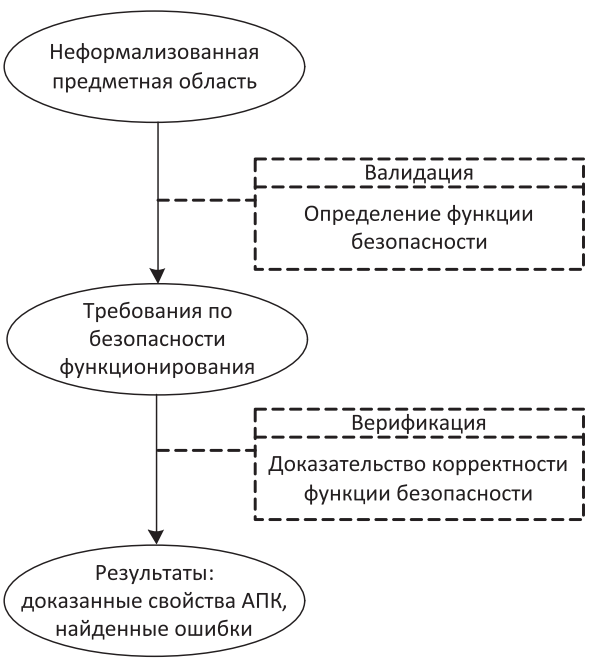


Рис. 1. Последовательность этапов анализа на безопасность

Условия для определения функции безопасности устанавливаются на этапе валидации на основании характеристик применяемых компонентов, множества используемых методов, стратегий обеспечения безопасности и практического опыта в рассматриваемой предметной области [11]. Данный процесс независим от последующей верификации – он определяет подлежащие проверке

свойства и формирует исходные данные, на основании которых задается функция безопасности, используемая в доказательстве корректности. Если допускаются ошибки на этапе валидации, либо не принимаются во внимание особенности поведения, влияющие на безопасность, то это непосредственным образом влияет на качество последующей верификации. Кроме того, какие бы эффективные и диверситетные методы и средства не использовались во время доказательства корректности, они не в состоянии выявить и решить проблемы, созданные во время проектирования, так как они работают с одинаковой спецификацией и только конечный пользователь может указать на ошибку, допущенную при составлении требований.

Мировой опыт эксплуатации критически важных систем информатизации говорит о том, что аварии и катастрофы происходят из-за множества факторов, при этом значительная часть происшествий происходит (в том числе) из-за ошибок, допущенных при формулировке требований к системе [11, 12, 13]. Например, имеется большое количество причин, из-за которых морской корабль может быть подвержен риску: столкновение с айсбергом, коррозия, взрыв груза и др. Инженерам не обязательно знать все источники рисков, но при этом во время проектирования могут быть приняты формализованные решения для минимизации опасности: корабль должен оставаться на плаву при заданном пределе количества пробоин, необходимо наличие спасательных средств и требуется проведение предварительных мероприятий. Пароход “Титаник” был спроектирован так, чтобы оставаться на плаву в случае затопления 4 или менее первых отсеков, что можно назвать функцией безопасности. К сожалению, столкновение с айсбергом привело к затоплению 5 первых отсеков [11]. Функция безопасности была задана исходя из практического опыта и знаний того времени, и после её определения проектирование системы проводилось уже на её основании. Но, как показывает история, такой подход не означает, что все возможные опасности устранены.

При проектировании систем могут приниматься неявные допущения, которые напрямую не связаны с безопасностью функционирования, но могут повлиять на работу всего АПК. Например, допущение того, что траектории самолётов всегда будут выше уровня моря, может привести к ошибкам ПО во время полета над территориями ниже уровня моря и отказу всей системы [14].

Условия безопасности работы системы могут отличаться при изменении окружения или условий функционирования, что актуально для СЖАТ, и в частности это в значительной степени проявляется при переходе с релейной базы на микроэлектронную. Например, при проведении испытаний на безопасность схем блочной маршрутно-релейной централизации проверка зависимостей по стрелочно-путевым секциям проводится один раз независимо от положения стрелок, входящих в секцию, а также независимо от рода и направления маршрута, задаваемого через секцию. Независимость от перечисленных факторов обуславливается свойствами реле первого класса надежности и схемными решениями по проверке взаимозависимостей. Однако в случае применения микропроцессорной базы с симметричными отказами АПК не обладает теми же свойствами, и верификация ПО должна проводиться с учётом всех возможных вариантов, которые могут быть в рассматриваемых условиях функционирования с рассмотрением всех возможных отказов микроэлектронной элементной базы в соответствии с ТНПА.

Таким образом, одной из проблем валидации является определение условий, подлежащих проверке, а особенности данного процесса таковы, что после формализации нет однозначного критерия и уверенности в том, что утвержденная доказываемая функция является необходимой и достаточной [15]. Во время последующей разработки или анализа на безопасность может быть выяснено, что заданные рамки слишком строги и доказательство корректности провести невозможно, или напротив, слишком слабы, из-за чего уменьшается вероятность нахождения ошибок в ПО.

Микроэлектронные СЖАТ обладают сложностью, которая затрудняет формализацию допускаемого и безопасного поведения. Из-за этого с большой вероятностью могут быть допущены ошибки. Для решения данной проблемы может быть определена такая функция безопасности, в которой данные недостатки отсутствуют. Кроме того, при разработке и при доказательстве корректности нет необходимости строгого выбора функции безопасности – это может быть любая функция, удовлетворяющая условиям на рис. 2.

Рис. 2. Выбор доказываемой функции безопасности

Описание для указанных областей:

А – по каким-либо причинам система не выполнила условие доказываемой функции безопасности, но это не привело к опасному отказу;

Б – поведение системы удовлетворяет условию функции безопасности;

Таким образом, доказываемая функция безопасности всегда должна быть такой же или более строгой, чем допускаемое безопасное поведение. Поведение разработанной системы должно удовлетворять условию доказываемой функции безопасности.

Накопленный авторами опыт верификации критически важных объектов информатизации микропроцессорных СЖАТ говорит о том, что определение доказываемой функции безопасности разрабатываемых и существующих АПК необходимо проводить на основании:

– используемой стратегии обеспечения безопасности – например, во время проектирования может быть использована стратегия применения логических элементов с несимметричными отказами (h_1-надежные элементы) и система должна придерживаться её во время всего жизненного цикла [16];

– требований безопасности ко всей системе – например, верифицируемый компонент должен выдерживать заданные временные диапазоны сигналов взаимодействия с другими компонентами системы;

– требований безопасности к рассматриваемому АПК – например, система обязана сохранять инвариант и переходить в безопасное состояние в случае внутренних сбоев.

Таким образом, результатом верификации является доказательство того, что свойства рассматриваемого ПО выполняют требования безопасности к нему и к его окружению, а также согласованы с используемой стратегией обеспечения безопасности.

Определение доказываемой функции безопасности может проводиться на основании только технического задания (ТЗ) разрабатываемого АПК, но в этом случае формализация функции безопасности может оказаться сложным и трудоемким процессом. В связи с этим возможен переход к доказательству более строгой функции безопасности, нежели той, которая определена исходя из в требований безопасности ТЗ и учёта полноты критериев опасного отказа.

Рассмотрение требований к системе в отношении стратегии обеспечения безопасности, безопасного внутреннего поведения и согласования взаимодействия с внешними компонентами позволяет быстрее и эффективнее разбивать доказываемую цельную функцию на эквивалентные, но более простые функции, что уменьшает сложность верификации и улучшает её качество.

Формулировка функции безопасности не является конечным решением и при необходимости функция безопасности может быть изменена на любую другую, удовлетворяющую условиям, показанным на рис. 2. Опыт верификации говорит о том, что переход к другой функции безопасности следует проводить тогда, когда в новом рассматриваемом ракурсе поведение системы становится:

– более детерминированным – можно более точно сказать, как ведет себя система в тех или иных ситуациях;

– менее сложным – снижаются затраты анализа на безопасность и время, требуемое на понимание процессов, имеющих место в системе.

Основными применяемыми авторами способами изменения функции безопасности является её расширение (ослабление, более слабое определение) и сужение (усиление, более строгое определение). Кроме этого, функция безопасности может быть изменена не как строгое ослабление или усиление, но в любом случае, она должна находиться в рамках допускаемого безопасного поведения (см. рис. 2).

Рассмотрим три функции безопасности f_1, f_2 и f_3, каждая из которых зависит от вектора аргументов $\bar{\alpha}$ и имеет область значений истина/ложь (*true/false*). Тогда усилением функции f_2 является переход к такой функции f_3, при котором выполняются условия (1) и (2):

$$\forall\ (f_3(\alpha) = true\ )\quad f_2(\alpha) = true \tag{1}$$

$$\exists\ (f_2(\alpha) = true\ )\quad f_3(\alpha) = false. \tag{2}$$

Ослаблением функции f_2 является переход к такой функции f_1, при котором выполняются условия:

$$\forall\ (f_2(\alpha) = true)\quad f_1(\alpha) = true \tag{3}$$

$$\exists\ (f_1(\alpha) = true)\quad f_2(\alpha) = false. \tag{4}$$

Таким образом, ослаблением функции является переход от одной функции f_2 к другой функции f_1 таким образом, что всегда, когда истинна f_2, то истинна и f_1, но при этом существуют такие истинные значения f_1, при которых f_2 ложна. Усилением является аналогичный обратный переход. Графически отношения между функциями показаны на рис. 3.

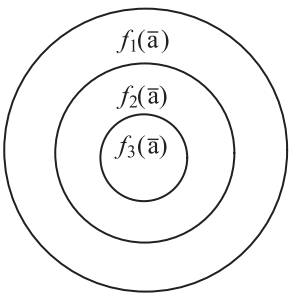


Рис. 3. Усиление и ослабление функций безопасности

Рассмотрим пример функций безопасности, выбор которых может повлиять на доказательство корректности. Предположим, что имеется ПО АПК, вся функциональность которого выполняется в замкнутом цикле, у которого каждое последующее выполнение должно быть отличимым от предыдущего и для этого в памяти хранится идентификатор *id*. Будем считать, что число циклов конечно и каждый из них пронумерован последовательно во времени от *1* до *n*, и, соответственно, существует множество идентификаторов $\alpha = \{id_1, id_2, \ldots, id_n\}$.

Для рассматриваемого случая приведем несколько вариантов функции безопасности. Первый пример:

$$f_1(\alpha) = true, \forall\ (i \in N, i < n)\quad id_i \neq id_{i+1}.$$

Данная функция гарантирует отличие идентификатора от предыдущего и может быть использована для безопасного обновления входящей информации.

Вторая функция безопасности гарантирует уникальность идентификатора за все время работы АПК с момента его запуска и может быть использована для обновления информации, которое происходит не на каждом витке полного цикла:

$$f_2(\alpha) = true, \forall\ (i \neq j \in N;\ i, j \leq n)\quad id_i \neq id_j.$$

Следующая функция безопасности гарантирует, что каждый последующий идентификатор ровно на 1 больше предыдущего и может быть использована для расчёта количества полных циклов между событиями:

$$f_3(\alpha) = true, \forall\ (i \in N, i < n)\quad id_{i+1} = 1 + id_i.$$

Функция f_3 более строгая, чем функция f_2, которая в свою очередь, более строгая, чем f_1.

Верифицировать более строгую функцию сложнее, чем более слабую – на это тратится большее количество ресурсов и не всегда это удается. Но, если есть возможность, то рекомендуется доказывать корректность более строгой функции, так как это имеет следующие положительные эффекты:

– получаем более точное представление о том, как работает система – свойства и поведение определяются более строго;

– снижается анализируемая сложность функционирования и тем самым повышается вероятность нахождения ошибок;

– доказанные функции могут быть использованы в дальнейшем для более эффективного проведения других доказательств корректности рассматриваемого АПК.

Однако в случае анализа на безопасность, когда невозможно доказать корректность в предложенном виде или отсутствуют ресурсы для проведения такого объема работ, возможно ослабление проверяемой функции при условии, что это позволит сделать заключение о безопасности ПО.

Определение функции безопасности для проведения верификации является важным этапом анализа на безопасность и её выбор представляет собой компромисс между имеющимися ресурсами и доказываемыми свойствами. Практика показывает, что избежать компромисса удается только в случае, если система подготовлена к тому, чтобы быть верифицируемой, когда задачи определения функции безопасности решаются до этапов разработки и проектирования, что возможно только для разрабатываемых и проектируемых АПК [4, 6].

Описываемое определение выбора функции безопасности было опробовано на верификации ПО устройств связи с напольными объектами СЖАТ, такими как блоки телеуправления 16-1 [2], светооптические светодиодные системы [3] и многопроцессорные блоки ТУ-8Б и ТС-16Б микропроцессорной централизации «Ипуть» [6].

Таким образом, разработанные общие принципы построения функций безопасности позволяют улучшить формализацию спецификаций доказательства безопасности ПО сложных АПК критически важных систем информатизации, а задача доказательства безопасности упрощается, если в процессе разработки используются методы построения контролепригодного ПО.

Литература

1. **Butler R.W.** «What is Formal Methods?» NASA LaRC Formal Methods Program, 2001.

2. **Сивко Б.В.** Доказательство корректности блока телеуправления 16-1 диспетчерской централизации «Нёман» // Вестник БелГУТа: Наука и Транспорт. – 2012. – №1(24). – С.18–21.

3. **Харлап С.Н., Сивко Б.В.** Верификация программного обеспечения микропроцессорной светооптической светодиодной системы // Вестник БелГУТа: Наука и Транспорт. – 2012. – №1 (24). – С.22–25.

4. **Сивко Б.В.** Проектирование безопасного программного обеспечения микропроцессорных устройств автоматики и телемеханики // Проблемы безопасности на трансп.: тезисы докл. VI Междунар. науч. – практ. конф., Гомель, 29–30 ноября 2012 г. / М-во образования Респ. Беларусь, М-во трансп. и коммуникаций Респ. Беларусь, Бел. ж. д., Белорус. гос. ун-т трансп.: редкол.: В.И.Сенько (отв. ред.) [и др.]. – Гомель, 2012. – С.205.

5. **David Smith J.** «Safety Critical Systems Handbook. A Straightforward Guide to Functional Safety, IEC 61508 and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849» / David J. Smith and Kenneth G. L. Simpson // Elsevier Ltd., 2010.

6. **Сивко Б.В.** Доказательство корректности программного обеспечения многопроцессорных устройств связи с объектами железнодорожной автоматики и телемеханики // Вестник БелГУТа: Наука и Транспорт. – 2012. – №2(25). – С.27-30.

7. **Fagan M.E.** Design and code inspections to reduce errors in program development, IBM Systems Journal, Volume 15 Issue 3, September 1976, p. 182–211.

8. **Boehm B.W.** Software engineering. IEEE Transactions on Computers 25:1226–1241, 1976.

9. **Telles M., Hsieh Y., Telles M.A.** The Science of Debugging // The Coriolis Group, 2001.

10. **Boehm B.W., Papaccio P.N.** Understanding and controlling software costs // IEEE Trans Softw Eng 14(10):1462–1477, October 1988.

11. **Nancy G. Leveson,** Software safety in embedded computer systems. Communications of the ACM, 34(2):34–46, February 1991.

12. **Charles Perrow.** Normal Accidents: Living with High Risk Technologies. Basic Books, New York, NY, 1984.

13. **Ivars Peterson**, Fatal Defect: Chasing Killer Computer Bugs, Times Books, New York, 1995.

14. **Nancy G. Leveson.** Safeware: System Safety and Computers. Addison-Wesley, 1995.

15. **Gerhart S.L., Yelowitz L.,** Observations of Fallibility in Applications of Modern Programming Methodologies // IEEE Trans. Software Eng., vol. 2, no. 3, 1976, pp. 195–207.

16. **Сапожников В.В., Кравцов Ю.А., Сапожников Вл.В.** Дискретные устройства железнодорожной автоматики и телемеханики // М. Транспорт, 1988.

Bochkov K.A., Sivko B.V.

SELECTION AND DEFINITION OF SAFETY FUNCTION WHEN VERIFYING RAILWAY SIGNALLING AND REMOTE CONTROL COMPUTER-BASED SYSTEMS

The paper considers the issues of definition, formalization and selection of safety function used for the development and correctness demonstration of software of railway signalling and remote control systems. It also provides ways of searching for and changing of safety function based on a specification, limitation of resources, an applied safety strategy and general requirements for system performance.

Keywords: *verification, validation, functional safety, safety function, correctness demonstration, critical computer-based objects.*

Nowadays, new developments widely use computer base in railway signalling and remote control systems, which extends their performance features and makes it possible to implement and provide wider functionality for operating systems. At the same time, however, development, verification and subsequent operation of these systems should correspond and satisfy to the safety level adopted in railway industry. Traditionally, railway signalling and remote control systems used relays, when the construction was based on the principle of hardware implementation of safety functions, while computer-based systems are hardware-software complexes (HSC) in which the majority of functions are implemented in software. At the same time the use of COTS technologies prevails in constructing modern computer-based railway signalling and remote control systems, whereas the development of software (SW) is the most complicated element of these systems. Besides, for computer-based railway signalling and remote control systems there are no uniform, universal and generally accepted methods of safety proof, and in this reference one should apply a complex of methods and means to increase a safety level at all stages of a system life cycle, and an urgent task is the development of new safety case techniques.

One of the possible ways of search for errors and improvement of SW quality within the framework of a used complex of approaches is the demonstration of correctness, which belongs to formal methods [1] and is successfully used for verification of microprocessor devices on the Belarus railway [2, 3, 4]. For the systems associated with safety, standard IEC 61508 has a range of safety integrity levels from SIL 1 up to SIL 4, and railway systems should correspond to the most rigorous level SIL 4, which urgently recommends application of formal methods for critical control systems [5].

As the demonstration of correctness, formal methods can be applied for ready-made SW as well as at early stages of development of the entire HSC, but in any case, one of the first steps of verification is the definition of a safety function subject to the demonstration of correctness [4, 6].

A safety function represents a formalized condition in relation to verified system, whose satisfaction allows us to make the conclusion about a function safety of railway signalling and remote control systems. For the same HSC, a safety function can be defined differently, and a condition to be satisfied can be chosen at different stages of a system life cycle.

The development and application of SW as well as a number of studies show that the later the error is detected, the more difficult is to reveal and correct it, and more problems can be caused by such error [7, 8]. It should be noted that the correction of errors made at the stage of preparing system requirements is ten times more expensive than that of errors made during system implementation [9, 10]. The definition of a safety function, which belongs to formalization of a problem to be solved, is a specification in relation to the demonstration of correctness and possesses the same properties, as the statement of requirements for SW development. The potential errors made at the stage of defining a safety function, negatively influence the quality of verification and can lead to distortion of results of correctness demonstration and, as a consequence, to its full revision.

Fig. 1 shows the sequence of safety analysis stages with defining a safety function.

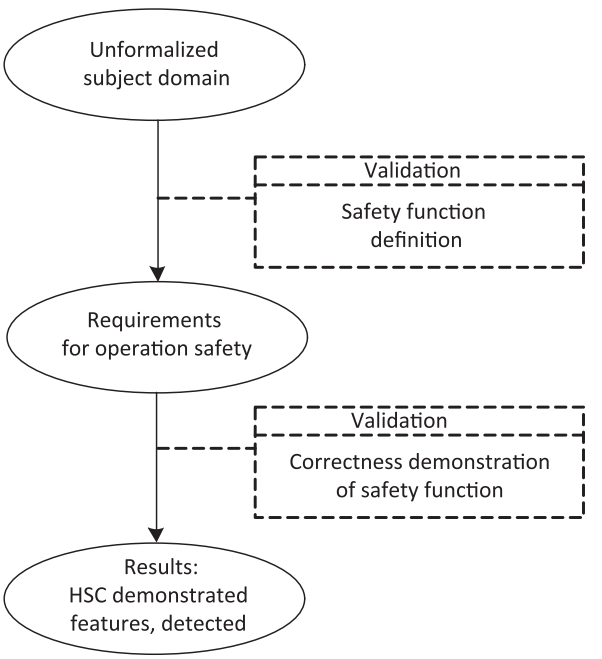


Fig. 1. Sequence of safety analysis stages

Conditions for defining a safety function are defined at the stage of validation based on the characteristics of components used, a variety of methods used, safety strategy and practical experience in the subject domain under consideration [11]. The given process is independent of the subsequent verification: it defines test parameters and forms the initial data, based on which a safety function used in the demonstration of correctness is specified. If errors are made at the validation stage, or behavior features influencing safety are not considered, then it directly influences the quality of a subsequent verification. Also, however effective and diverse methods and means were used during correctness demonstration, they are not capable to reveal and correct problems made during designing as they work according to the same specification, and the end user only can identify an error made at the stage of preparing requirements.

The global experience of application of safety critical systems shows that accidents and disasters occur because of a set of factors, and the significant part of incidents take place due to mistakes made at the stage of preparing system requirements [11, 12, 13]. For example, there are a lot of reasons why a sea ship can be subject to risks: collision with an iceberg, corrosion, explosion of cargo, etc. It is not necessary for engineers to know all sources of risks, but at the same time the formalized decisions for minimization of hazards can be taken during designing: a ship should stay afloat at the specified limit quantity of leaks, saving means should be available, and preliminary actions should be carried out. The steamship Titanic was designed to stay afloat in case of flooding 4 or less first compartments, and this can be named as a safety function. Unfortunately, collision with an iceberg led to flooding of the five first compartments [11]. A safety function was set based on practical experience and knowledge of that time and upon its definition the system was designed on its basis. But, as the history shows, such approach does not mean that all possible hazards are eliminated.

When designing systems, one can accept implicit assumptions, which directly are not related to functional safety but can affect the operation of the whole HSC. For example, an assumption that trajectories of aircrafts will always be above a sea level can lead to SW errors during flights above territories that are below a sea level and to failure of the whole system [14].

Safety conditions of system operation can differ in case of changes of environment or operating conditions that are urgent for railway signalling and remote control systems, and in particular it substantially show itself in case of transition from relays into computer base. For example, when carrying out safety tests of circuits of a route-block relay interlocking, checkout of dependences on point-track sections is carried out once, irrespective of the position of points which are included in the section, and also irrespective of the type and direction of a route set through a section. Independence from the listed factors is conditioned by properties of the first class reliability relay and circuitry for interdependence checkout. However, in case of application of computer base with symmetric failures, HSC does not possess the same properties, and SW verification should be carried out in view of all possible alternatives, which can exist in considered conditions of functioning, with all possible failures of microelectronic elements, according to respective standards, taken into account.

Thus, one of the validation problems is the definition of conditions subject to checkout, and features of the given process are such that after formalization there is no unambiguous criterion and confidence that the adopted function to be proved and demonstrated is necessary and sufficient [15]. During subsequent development or safety analysis it can be found out that the framework set is too strict and it is impossible to carry out correctness demonstration, or on the contrary, the framework is too weak, and thus the probability of detection of SW errors decreases.

Railway signalling and remote control systems possess complexity, due to which strict conditions of accepted safe behavior are complex in formalization, and thus their definition can demand a lot of resources and there is a greater probability to make errors. In order to solve the given problem, one can define such safety function where the given disadvantages are absent. Besides, when developing and demonstrating the correctness, there is no necessity in rigorous selection of a safety function – it can be any function satisfying to the conditions presented in Fig. 2.

The description for the specified areas is:

A – For some reason, the system has not met the condition of a demonstrated safety function, but it has not led to a hazardous failure;

B – The system behavior satisfies to the safety function condition.

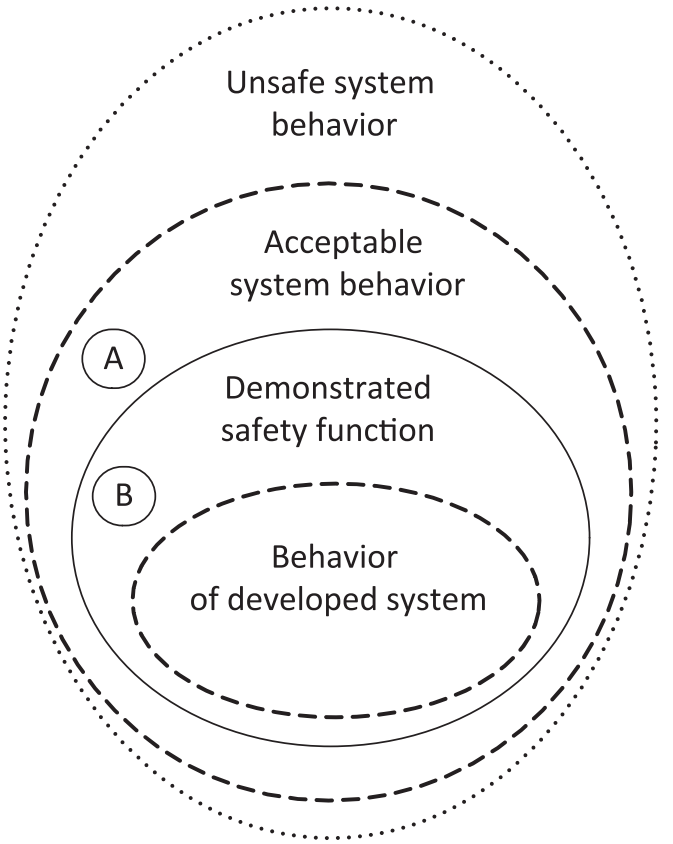


Fig. 2. Selection of safety function for demonstration

Thus, the demonstrated safety function should always be the same or more rigorous than acceptable safe behavior. The behavior of a system under development should satisfy to the condition of a demonstrated safety function.

The experience accumulated by the authors as regards verification of safety critical objects of railway signalling and remote control systems shows that the definition of a demonstrated safety function for developed and existing HSCs should be carried out on the basis of:

– applied safety strategy – for example, during the design stage the strategy of application of logical elements with asymmetrical failures (h_1-reliable elements) can be used and the system should follow it during the whole life cycle [16];

– safety requirements for the whole system – for example, the verified component should stand up to the specified time ranges of signals of interaction with other system components;

– safety requirements for HSC under consideration – for example, the system shall keep invariant and pass into a safe state in case of internal failures.

Thus, the result of verification is the proof that the properties of SW under consideration meet safety requirements for it and for its environment, and also are coordinated with the used safety strategy.

The definition of a demonstrated safety function can be made only on the basis of requirements specification (RS) of a developed HSC, but in this case, safety function formalization may turn out to be difficult and labor-intensive process. In this connection the transition to the demonstration of a more rigorous safety function rather than that was defined based on safety requirements specified in RS and considering the completeness of hazardous failure criteria.

The consideration of requirements for a system as regards a safety strategy, safe internal behavior and coordination of interaction with external components allows us to break down a demonstrated integral

function faster and more effectively into equivalent but simpler functions that reduces the complexity of verification and improves its quality.

The statement of a safety function is not a final decision, and if necessary a safety function can be changed to any other one satisfying to the conditions shown in Fig. 2. The experience of verification shows that transition to other safety function should be carried out when in terms of new consideration the system behavior becomes:

– more determined – It is possible to tell more accurately how the system behaves in those or other situations;

– less complex – there is reduction of costs of safety analysis and time required to understand processes taking place in the system.

The basic methods used by the authors to change a safety function are its extension (easing, weaker definition) and narrowing (strengthening, more rigorous definition). Also, a safety function can be changed not as rigorous easing or strengthening, but in any case it should keep within the framework of acceptable safe behavior (see Fig. 2).

Let us consider three functions of safety f_1, f_2 and f_3, each depending on a vector of arguments $\bar{\alpha}$ and having a range of true/false values. Then strengthening of function f_2 is the transition to such function f_3 when conditions (1) and (2) are met:

$$\forall\ (f_3(\alpha) = true)\quad f_2(\alpha) = true \tag{1}$$

$$\exists\ (f_2(\alpha) = true)\quad f_3(\alpha) = false. \tag{2}$$

The easing of function f_2 is the transition to such function f_1 when the following conditions are met:

$$\forall\ (f_3(\alpha) = true)\quad f_2(\alpha) = true \tag{3}$$

$$\exists\ (f_2(\alpha) = true)\quad f_3(\alpha) = false. \tag{4}$$

Thus, the easing of a function consists in the transition from one function f_2 to another function f_1 in such a manner that always when f_2 is true, then f_1 is also true, but at the same time there are such true values f_1 when f_2 is false. Strengthening is similar to return transition. Graphically relations between functions are shown in Fig. 3.

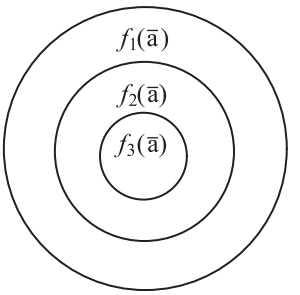


Fig. 3. Strengthening and easing of safety functions

Let us consider an example of safety functions whose choice can affect the demonstration of correctness. We shall assume that there is HSC SW whose whole functionality is carried out in a closed cycle where each subsequent execution should be distinguishable from the previous one and for this

purpose the identifier *id* is stored in the memory. We shall believe that the number of cycles is finite and each of them is numbered sequentially in time from *1* up to *n*, and, accordingly, there is a set of identifiers $\alpha = \{id_1, id_2, ..., id_n\}$.

For the case under consideration we shall introduce several alternatives of a safety function. The first example:

$$f_1(\alpha) = true, \forall\ (i \in N, i < n) \quad id_i \neq id_{i+1}$$

The given function guarantees the difference of the identifier from the previous one and can be used for safe updating of the input information.

The second safety function ensures uniqueness of the identifier for all operating time of HSC from the moment of its operation start and can be used for updating of the information, which takes place not on each turn of a full cycle:

$$f_2(\alpha) = true, \forall\ (i \neq j \in N; i, j \leq n) \quad id_i \neq id_j$$

The following safety function ensures that each subsequent identifier is exactly by 1 more than the previous one and this function can be used for quantity calculation of full cycles between events:

$$f_3(\alpha) = true, \forall\ (i \in N, i < n) \quad id_{i+1} = 1 + id_i$$

Function f_3 is more rigorous than function f_2, which in turn, is more rigorous than function f_1.

To verify a more rigorous function is more complicated than to verify a weaker function as a lot of resources is spent for it and it is not always possible. But, if there is an opportunity, then it is recommended to demonstrate correctness of a more rigorous function as it has the following positive effects:

– obtaining more exact representation of how the system operates – its properties and behavior are defined more strictly;

– reducing complexity of analyzed operation and by that increasing the probability of detection of errors;

– proved or demonstrated functions can be further used for more effective implementation of other correctness demonstrations for HSC under consideration.

However, in case of safety analysis when it is impossible to demonstrate correctness in the offered form or there are no resources for carrying out such amount of works, the easing of a verified function is possible provided that it will allow us to making a conclusion about SW safety.

The definition of a safety function for verification purposes is an important stage of safety analysis and its choice represents a trade-off between available resources and properties to be demonstrated. Practice shows that we can avoid a trade-off only in case when a system is prepared to be verified, when problems of safety function definition are solved before stages of development and designing, which is only possible for HSC to be designed and developed [4, 6].

The described definition of safety function choice has been tested on verification of SW for communication devices with outdoor devices of railway signalling and remote control systems, such as remote control units 16-1 [2], optical LED systems [3] and TU-8B and TC-16B multiprocessing units of “Iputj” computer-based interlocking [6].

Thus, the developed general principles of safety function construction allow us to improve the formalization of specifications of safety cases for HSC SW as part safety critical systems, and the problem of a safety case is simplified if during designing the methods of development of testable SW are used.

References

1. **Butler R.W.** "What is Formal Methods?" NASA LaRC Formal Methods Program, 2001.

2. **Sivko B.V.** Correctness demonstration of the 16-1 remote control unit for "Niemen" centralized traffic control // BelGUT Bulletin: Science and Transport. - 2012. #1 (24). – pp. 18-21.

3. **Harlap S.N., Sivko B.V. S**oftware verification for microprocessor based optical LED systems // BelGUT Bulletin: Science and Transport. - 2012. - #1 (24). – pp. 22-25.

4. **Sivko B.V.** Safe software designing of microprocessor based devices of railway signalling and remote control systems // Problems of safety on transport: Report synopsis, VI International Scientific and practical Symposium, Gomel, November, 29-30, 2012 / Ministry of Education - Belarus, Ministry of transport and communications, Belarus State University of Transport, - Gomel, 2012. – p. 205.

5. **David Smith J.** "Safety Critical Systems Handbook. A Straightforward Guide to Functional Safety, IEC 61508 and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849" / David J. Smith and Kenneth G. L. Simpson // Elsevier Ltd., 2010.

6. **Sivko B.V**. SW correctness demonstration for multiprocessing devices of communication with facilities of railway signalling and remote control systems // BelGUT Bulletin: Science and Transport. - 2012. - #2 (25). – pp. 27-30.

7. **Fagan M.E.** Design and code inspections to reduce errors in program development, IBM Systems Journal, Volume 15 Issue 3, September 1976, p. 182-211.

8. **Boehm B. W.** Software engineering. IEEE Transactions on Computers 25:1226-1241, 1976.

9. **Telles M., Hsieh Y., Telles M.A.** The Science of Debugging // The Coriolis Group, 2001.

10. **Boehm B.W., Papaccio P.N.** Understanding and controlling software costs // IEEE Trans Softw Eng 14:1462-1477, October 1988.

11. **Nancy G. Leveson,** Software safety in embedded computer systems. Communications of the ACM, 34:34-46, February 1991.

12. **Charles Perrow.** Normal Accidents: Living with High Risk Technologies. Basic Books, New York, NY, 1984.

13. **Ivars Peterson**, Fatal Defect: Chasing Killer Computer Bugs, Times Books, New York, 1995.

14. **Nancy G. Leveson.** Safeware: System Safety and Computers. Addison-Wesley, 1995.

15. **Gerhart S.L., Yelowitz L.** Observations of Fallibility in Applications of Modern Programming Methodologies // IEEE Trans. Software Eng., vol. 2, no. 3, 1976, pp. 195-207.

16. **Sapozhnikov V.V., Century B., Kravtsov Ju.A., Sapozhnikov Vl.V.** Discrete devices of railway signalling and remote control systems // M. Transport, 1988.

Нетес В.А., Тарасьев Ю.И., Шпер В.Л.

АКТУАЛЬНЫЕ ВОПРОСЫ СТАНДАРТИЗАЦИИ ТЕРМИНОЛОГИИ В ОБЛАСТИ НАДЁЖНОСТИ

Почти четыре века назад английский философ Фрэнсис Бэкон в своем трактате «Новый органон» писал: «Громкие и торжественные диспуты ученых часто превращаются в споры относительно слов и имен, а благоразумнее было бы (согласно обычаю и мудрости математиков) с них и начать для того, чтобы посредством определений привести их в порядок». Публикации по надёжности на русском языке стали появляться с середины 1950-х годов, поэтому в начале 1960-х годов для основных понятий в этой области появилась потребность «посредством определений привести их в порядок».

Первый документ такого рода был разработан АН СССР в течение 1960–1961 годов и опубликован в 1962 году [1]. В его создании принимали участие такие крупные ученые и специалисты, как А.И. Берг, Н.Г. Бруевич, Б.В. Гнеденко, В.И. Сифоров, Я.М. Сорин, И.А. Ушаков, Я.Б. Шор и др. Термины были просмотрены с точки зрения соответствия языковым нормам в Институте русского языка АН СССР. Проект был выпущен тиражом 600 экземпляров и разослан для обсуждения, было получено 110 отзывов с замечаниями и предложениями. Сейчас можно только мечтать о таком уровне и масштабе разработки!

Надёжность в [1] определялась как «свойство системы (элемента системы), обусловленное главным образом её безотказностью и ремонтопригодностью и обеспечивающее выполнение задания в установленном для системы (элемента) объёме». Отсюда видно, что уже тогда надёжность считалась сложным свойством, включающим свойства безотказности и ремонтопригодности. Помимо них определялись также такие свойства, как сохранность (впоследствии трансформировавшаяся в сохраняемость), восстанавливаемость, включающая как частный случай самовосстанавливаемость, и др. А вот долговечность, считающаяся в настоящее время одним из основных свойств, составляющих надёжность, тогда была определена как суммарная наработка невосстанавливаемого элемента от начала эксплуатации (использования) до момента возникновения отказа. Таким образом, за прошедшее время наша интерпретация некоторых терминов претерпела значительные изменения.

Несколько лет спустя был принят первый государственный стандарт на термины и определения в области надёжности ГОСТ 13377–67, пересмотренный и обновленный в 1975 году (ГОСТ 13377–75). В 1980-е годы появилась уже группа стандартов «Надёжность в технике», получившая номер 27, в рамках которой создавались и новые терминологические стандарты ГОСТ 27.002–83 и ГОСТ 27.002–89. Наконец в 2009 году был принят российский стандарт ГОСТ Р 27.002–2009 (вначале получивший обозначение ГОСТ Р 53480–2009). Век этого документа оказался недолог, и на его судьбе стоит остановиться подробнее.

ГОСТ Р 27.002–2009 был разработан с учетом основных нормативных положений международного терминологического стандарта по надежности МЭК 60050 (191):1990. Таким образом был реализован один из основных принципов стандартизации, установленный в статье 12 Федерального закона РФ «О техническом регулировании», – применение международного стандарта как основы разработки национального стандарта. При этом стоит уточнить, что ГОСТ Р 27.002–2009 является неэквивалентным стандартом по отношению к МЭК 60050 (191):1990 и поэтому не может считаться гармонизированным. Таким образом, заглавие статьи [2], посвященной принятию ГОСТ Р 27.002–2009 – «Терминология в области надёжности гармонизирована!» – строго говоря, не соответствует действительности.

Почему за основу был взят именно стандарт МЭК? Основными глобальными международными организациями по стандартизации являются: МЭК (Международная электротехническая комиссия – International Electrotechnical Commission, IEC), ИСО (Международная организация по стандартизации – International Organization for Standardization, ISO) и МСЭ (Международный союз электросвязи – International Telecommunication Union, ITU). Между ними осуществляется тесное взаимодействие и координация работы в рамках альянса WSC (World Standard Cooperation – Всемирное сотрудничество по стандартам).

В соответствии с соглашением между этими организациями ведущую роль в области стандартизации надёжности играет именно МЭК, а ИСО и МСЭ при разработке своих документов опираются на её стандарты. Например, определение понятия «надёжность», приведенное в стандарте ИСО 9000 (имеется идентичный российский ГОСТ Р ИСО 9000), взято именно из МЭК 60050 (191):1990. Этот стандарт представляет собой главу 191 Международного электротехнического словаря (International Electrotechnical Vocabulary, IEV), обозначаемую также IEV-191. Вообще, всю терминологическую работу в МЭК координирует Технический комитет (ТК) 1. В частности, им организован специальный интернет-портал, называемый «Электропедия» (http://www.electropedia.org/), предоставляющий онлайновый доступ к IEV.

Стандартизацией в области надежности в МЭК занимается ТК 56, который так и называется «Надёжность» (Dependability). Он имеет статус «горизонтального» (межотраслевого, общетехнического) комитета, обслуживающего все «вертикальные» отраслевые технические комитеты МЭК и ИСО. Более подробно с деятельностью МЭК/ТК 56 можно ознакомиться в [3]. К сожалению, в последние годы из-за отсутствия соответствующего финансирования наши эксперты не могут принимать активное участие в работе ТК 56. Впрочем, другие государства бывшего СССР в нём вообще никак не представлены.

Для стандарта МЭК 60050 (191):1990 существует официальный перевод на русский язык, который создавался вскоре после принятия ГОСТ 27.002–89 и был с ним в какой-то степени согласован. Однако на момент начала работы над ГОСТ Р 27.002–2009 в МЭК/ТК 56 активно шла разработка новой редакции терминологического стандарта (IEV-191, Ed. 2), поскольку всем было ясно, что его 1-я редакция (IEV-191, Ed. 1), т.е. действующий стандарт МЭК 60050 (191):1990, уже устарел. Поэтому разработчики ГОСТ Р 27.002–2009 надеялись, что смогут взять за основу новый стандарт МЭК (IEV-191, Ed. 2). Однако работа в ТК 56 затянулась, принятие нового стандарта МЭК было отложено, а вот у нас на соответствующую корректировку плана стандартизации Росстандарт не пошел, в результате чего пришлось ориентироваться на стандарт почти 20-летней давности. К сожалению, при этом не был в должной мере учтён существующий русский перевод этого стандарта.

Кроме того, у нас изменились процедуры разработки и принятия стандартов. В отличие от того, как это делалось раньше, проект не рассылался всем заинтересованным организациям и специалистам, не обсуждался на научно-технических семинарах. Конечно, формально все действующие процедуры были соблюдены, проект выставлялся для ознакомления в Интернете, на него можно было давать отзывы, однако многие специалисты об этом даже не знали. В результате,

с одной стороны, многие организации не были заранее ознакомлены с основными принципами нового стандарта и доводами, обосновывающими необходимость изменений. С другой стороны, разработчики стандарта не получили обратной связи относительно имеющихся в новом стандарте ошибок и неточностей.

В результате ГОСТ Р 27.002–2009 вызвал неприятие и резкую критику многих специалистов [4–6]. Основные предъявляемые к нему претензии можно разделить на две группы: 1) отход от некоторых положений предшествующих отечественных стандартов; 2) ошибки, неточности, отсутствие системности при переводе терминов и определений, взятых из стандарта МЭК. Разработчики отвечали на критику в адрес своего детища [7], но итог оказался не в его пользу. Приказом Росстандарта № 1843-ст от 29.11.2012 было приостановлено применение ГОСТ Р 27.002–2009 и восстановлено применение ГОСТ 27.002–89.

Конечно, возврат к стандарту 25-летней давности – это вынужденная временная мера. Поэтому одновременно с решением о возврате к стандарту 1989 года, было принято решение о разработке нового терминологического стандарта по надежности. Это должен быть уже не только российский, а межгосударственный стандарт СНГ. Учитывая международный (хотя и региональный) характер создаваемого стандарта, еще большую важность приобретает опора на официальный международный стандарт.

Данный аспект приобрел особое значение в связи с вступлением России в ВТО. Присоединение нашей страны к этой организации делает весьма актуальным вопрос о гармонизации национальных стандартов с их международными аналогами. Сегодня уровень гармонизации – это один из показателей, о котором постоянно говорят руководители национального органа по стандартизации, и который они призывают увеличивать. Поэтому новый ГОСТ должен быть, по возможности, максимально согласован с международным стандартом (МС) МЭК 60050-191 (IEV-191, Ed. 2), который будет принят в ближайшее время.

С другой стороны, во всех странах СНГ когда-то использовались стандарты СССР, с которыми желательно сохранить преемственность. Уже сейчас понятно, что разрабатываемый новый ГОСТ вряд ли удастся сделать эквивалентным по отношению к МС МЭК (это ясно из обстоятельств, отмеченных ниже).

Поэтому разработка нового стандарта представляет собой нелёгкую задачу. За нее согласилась взяться та группа специалистов, которая наиболее активно протестовала против ГОСТ Р 27.002–2009. В ходе нескольких обсуждений в рамках ТК 119 в июне 2013 года было принято решение о формировании рабочей группы (РГ), которой будет поручена разработка первой редакции нового стандарта. В неё вошли девять специалистов, представлявших различные отрасли промышленности: авиастроение, оборонную, связь, энергетику, в том числе, атомную, железнодорожный транспорт; НИИ и вузы: МИСИС, МТУСИ, РНИИ «Электростандарт», ВНИИНМаш, ИСЭМ СО РАН, Институт надежности машин и технологий СПбГПУ. Возглавил РГ председатель ТК 119 д.т.н. проф. Г.Н. Черкесов. В ноябре 2013 года на заседании ТК 119 было принято решение о согласовании общей структуры будущего стандарта, а также о наименовании его основных разделов: (1) Основные понятия; (2) Состояния; (3) Времена; (4) Отказы, дефекты, повреждения; (5) ТО, восстановление, ремонт; (6) Показатели надежности; (7) Нормирование и контроль надежности; (8) Резервирование; (9) Испытания на надежность.

По ряду вопросов мнения членов РГ разошлись. Один из важных вопросов, вызвавших разногласия – что брать за основу при разработке нового стандарта – ГОСТ 27.002–89 или МС МЭК.

От его решения зависит, в частности, определение основного термина «надежность». Согласно одной точке зрения, следует оставить то определение, которое было в ГОСТ 27.002–89: «Надежность – 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».

Согласно другой – желательно уйти от параметрического описания, ограниченность которого была признана уже в самом ГОСТ 27.002–89 (Приложение, пояснение к термину «надежность») и использовать формулировку МС МЭК (IEV-191, Ed. 2), которая на данный момент (в переводе одного из авторов) выглядит так: «Способность функционировать как и когда требуется» (Ability to perform as and when required).

Далее, в ГОСТ 27.002–89 надежность является комплексным свойством, которое в зависимости от назначения объекта и условий его применения может включать безотказность, долговечность, ремонтопригодность и сохраняемость или определенные сочетания этих свойств. В МС МЭК свойство сохраняемости отсутствует, но присутствуют другие свойства, например, готовность, которой нет в ГОСТ 27.002–89 (хотя там есть показатели, характеризующие это свойство, в частности, коэффициент готовности).

Кроме указанных выше двух важных отличий, МС отличается от ГОСТ присутствием нескольких десятков новых терминов и отсутствием ряда терминов, имевшихся в отечественном стандарте.

Члены РГ считают, что разрабатываемый стандарт должен взять все самое полезное из обоих стандартов (IEV-191, Ed. 2 и ГОСТ 27.002–89). Не вдаваясь пока что в дискуссию по нерешенным вопросам, мы хотели бы предоставить читателям возможность подумать над ними без какого-либо влияния с нашей стороны.

Отметим, что 30 января 2014 года в МИИТе прошел семинар по надежности под руководством д.т.н. проф. И.Б. Шубинского. Это единственный постоянно действующий семинар по надежности, реально работающий в Москве. На нем были представлены два доклада членов РГ, представлявших два различных подхода к разработке нового стандарта: «Актуальные вопросы стандартизации терминологии в области надёжности» В.Н. Нетеса и «Сравнительный анализ определений основных терминов (надежность, отказ, готовность) по ГОСТ 27.002–89 и стандарту МЭК» Ю.И. Тарасьева. По нашему общему мнению, это обсуждение не привело к появлению какого-то общего решения, т.е. разногласия между членами РГ пока что сохраняются.

Учитывая принципиальную важность создания нового терминологического стандарта, авторам хотелось бы, чтобы все заинтересованные в развитии работ в области надежности в РФ, откликнулись на данную публикацию, и высказали своё мнение по существу. Мы, со своей стороны, планируем в ближайшее время опубликовать вторую статью на эту тему, где будут подробно изложены аргументы обеих сторон по проблеме общего определения надежности и того, какой документ положить в основу нового ГОСТ.

Литература

1. Теория надёжности в области радиоэлектроники. Терминология: Сб. рекомендуемых терминов. Вып. 60 / АН СССР. Комитет техн. терминологии. Ин-т радиотехники и электроники. – М., 1962.

2. **Демидович Н.О.** Терминология в области надёжности гармонизирована! // Стандарты и качество. 2011. № 2.

3. **Богданова Г.А., Нетес В.А.** МЭК/ТК 56: стандартизация для надёжности // Методы менеджмента качества. 2009. № 5.

4. **Нетес В.А., Резиновский А.Я., Тарасьев Ю.И., Ушаков И.А., Фишбейн Ф.И., Шпер В.Л.** Деградация вместо гармонизации // Стандарты и качество. 2011. № 5.

5. **Ушаков И.А.** Незваный ГОСТ // Методы менеджмента качества. 2011. № 5.

6. **Григорьев А.** Новый ГОСТ – «мозги наизнанку»? // Стандарты и качество. 2011. № 9.

7. **Демидович Н.О.** В проблеме терминологии надёжности пора ставить точку // Стандарты и качество. 2011. № 10.

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

CURRENT ISSUES OF TERMINOLOGY STANDARDIZATION IN DEPENDABILITY

Nearly four centuries ago the English philosopher Francis Bacon, in his treatise "Novum Organum" wrote: "Loud and solemn debates of scientists often turn into disputes about words and names, and it would be prudent (according to custom and wisdom of mathematicians) to start with them and through the definitions put them in order". Publications on dependability in Russian began to appear in the mid of the1950s, therefore in the early of the 1960s the necessity appeared for the basic concepts in this area "through the definitions to put them in order".

The first document of this kind was developed by the USSR Academy of Sciences during 1960 – 1961 and published in 1962 [1]. Such eminent scientists and experts as A.I. Berg, N.G. Bruyevich, B.V. Gnedenko, V.I. Siforov, Y.M. Sorin, I.A. Ushakov, Y.B. Shore and other took part in development of the document. Terms were viewed from the perspective of linguistic standards compliance at the Institute of the Russian Language of the USSR Academy of Sciences. The project was released as 600 copies and distributed for discussion. Later on, 110 reviews with comments and suggestions were received. We can only dream of such a level and scale of development!

Dependability in [1] was defined as "a system or a system component property, mainly conditioned by its reliability and maintainability and providing implementation of tasks in the amount established for the system (component)". This shows that even at that time dependability was considered as a complex property, including properties of reliability and maintainability. Besides them, properties such as retention (later transformed into storageability), recoverability including, as a special case, self-restorability etc. were determined. But durability, which is currently considered as one of the basic properties, constituent part of dependability, at that time was defined as the cumulative time to failure of a non-recoverable element from the beginning of operation (use) until a failure occurs. Thus, over time, our interpretation of some terms has undergone significant changes.

A few years later the first national standard for terms and definitions in the field of dependability GOST 13377-67 was adopted, revised and updated in 1975 (GOST 13377-75). In the 1980s there was already a group of standards "Dependability in Engineering", which received number 27, within which new terminology standards GOST 27.002-83 and GOST 27.002-89 were developed. Finally in 2009, the Russian standard GOST R 27.002-2009 (at first called GOST R 53480-2009) was adopted. The age of this document proved to be short-lived, and it is necessary to dwell on the issue in more detail.

GOST R 27.002-2009 was developed in view of the basic regulations of international terminology standard for dependability IEC 60050 (191): 1990. Thus, one of the basic principles of standardization, established in clause 12 of the Federal Law "On technical regulation," i.e. application of an interna-

tional standard as the basis for developing a national standard, was implemented. At the same time it is necessary to clarify that GOST R 27.002-2009 is a nonequivalent standard in relation to IEC 60050 (191): 1990, and therefore, it cannot be regarded as harmonized. Thus, the title of article [2] devoted to the adoption of GOST R 27.002-2009 "Terminology in dependability has been harmonized" is, strictly speaking, untrue.

Why exactly was IEC taken as a basis? The main global International standardization organizations are: IEC (International Electrotechnical Commission), ISO (International Organization for Standardization) and ITU (International Telecommunication Union). Between them there is close cooperation and coordination within the alliance of WSC (World Standard Cooperation).

In accordance with the agreement between these organizations, it is IEC that plays the leading role in the standardization of dependability, and ISO and ITU are based on IEC standards in developing their documents. For example, the definition of the notion "dependability" that is introduced in ISO 9000 (there is an identical Russian standard GOST R ISO 9000), is taken from IEC 60050 (191): 1990. This standard represents Chapter 191 of the International Electrotechnical Vocabulary (IEV) and often is denoted as IEV-191. Generally, all the terminological work in IEC is coordinated by Technical Committee (TC) 1. Particularly, this Committee has organized a special online portal called "Electropedia" (http://www.electropedia.org/), which provides online access to IEV.

Standardization of dependability in IEC is dealt with by TC 56, which is called "Dependability". It has the status of a "horizontal" (inter-branch, general technical) committee, serving all "vertical" industrial technical committees of IEC and ISO. More detailed information on the activities of IEC/TC56 can be found in [3]. Unfortunately, in recent years due to lack of funding, our experts cannot participate actively in the work of TC 56. However, other former Soviet states are not represented in TC 56 at all.

IEC 60050 (191):1990 has the official translation into the Russian language, which was done shortly after the adoption of GOST R 27.002-89, and it was harmonized with IEC 60050 (191):1990 to some extent. However, at the start of working on GOST R27.002-2009, the new third edition of the standard terminology (IEV-191, Ed.2) was actively developed in IEC/TC56 as it was clear that the 1-st edition (IEV-191, Ed. 1), i.e. the current IEC standard 60050 (191): 1990 has been already outdated. Therefore, developers of GOST R 27.002-2009 hoped that they could take as a basis the new standard IEC (IEV -191, Ed.2). However, the work in TC56 has been delayed and adoption of the new IEC standard was postponed, but our Rosstandard did not take appropriate correction of standardization plan, as a result of what we have had to be guided by the standard developed almost 20 years ago. Unfortunately, the existing Russian translation of this standard has not been duly taken into account.

In addition, we have changed the procedures for developing and adopting standards. Unlike how it was done before, the project is not circulated to all interested organizations and experts, not discussed at scientific and technical seminars. Of course, all existing formal procedures were followed, the project was exhibited for information on the Internet, making it possible to provide feedbacks, but many experts did not even know about the project. As a result, on the one hand, many organizations were not previously acquainted with the basic principles of the new standard and the arguments justifying the changes. On the other hand, the developers of the standard did not receive any feedback on errors and inaccuracies in the new standard.

As a result, GOST R 27.002-2009 caused disapproval and sharp criticism of many specialists [4-6]. Basic claims can be divided into two groups: 1) deviation from some of the regulations of the preceding national standards; 2) errors, mistakes, lack of consistency in translation of terms and definitions taken from IEC. The developers responded to criticism of their offspring [7], but the result was not in its favor. By Rosstandard Order No.1843 dated 29.11.2012, the application of GOST R R27.002-2009 was suspended and the application of GOST 27.002-89 was restored.

Of course, the return to the standard of 25 years old is a necessary temporary measure. For this reason simultaneously with the decision to return to the standard of 1989, it was decided to develop a new terminology standard for dependability. It should be not only a Russian standard but also a CIS interstate standard. Given the international (albeit regional) nature of the developed standard, even a greater importance consists in the reliance on an official international standard.

This aspect has acquired special importance in connection with Russia joining WTO. Joining the organization brings weight to a topical issue of harmonization of national standards with their international counterparts. Today, the level of harmonization is one of the indicators, which is constantly being talked over by the heads of our national standardization body, and which they call to increase. Therefore, the new GOST must be as closely as possible harmonized with international standard (IS) IEC 60050 -191 (IEV -191, Ed. 2), which will be adopted in the near future.

On the other hand, all CIS countries once used the USSR's standards, and it is desirable to keep legacy. Now it is also clear that a new standard is unlikely to be made equivalent to IEC IS (this is clear from the circumstances mentioned below).

Therefore, it is not an easy task. The group of experts, which most actively protested against GOST R 27.002-2009, agreed to take the development of the new standard in their hands. During several discussions within TC 119 in June 2013, it was decided to form a working group (WG), which is tasked with developing the first version of the new standard. It includes nine experts representing various industries: aircraft building, defense, communications, energy, including atomic power engineering, railway transport; Research institutes and universities: MISA, MTUCI, RNII "Electrostandard" VNIINMASH, ESI SB RAS, Institute of Machine Dependability and Technology of Saint-Petersburg Technical University. Professor G.N. Cherkesov became the head of TC 119 WG. In November 2013 at the meeting of TC 119 the decision was taken on agreement of the overall structure of the future standard, as well as the name of its main sections: (1) Basic concepts; (2) States; (3) Times; (4) Failures, defects, damages; (5) Maintenance, recovery, repair; (6) Dependability indices; (7) Dependability rate setting (normalization) and control; (8) Redundancy; (9) Dependability test.

Opinions of WG members on several issues discarded. One of the main issues that caused disagreements is what to take as a basis for developing the new standard – GOST 27.002-89 or IEC MS.

In particular, the definition of the basic term "dependability" depends on a decision to be taken on that issue. According to one view, it is necessary to take the definition that was in GOST 27.002-89: "Dependability is an object property to keep in time, within the established limits, the values of all parameters characterizing the ability to perform the required functions in specified modes of operation and conditions of use, maintenance, storage and transportation".

According to another view, it is desirable to get away from the parametric descriptions, limitations, which were recognized in GOST 27.002-89 (Appendix, an explanation of the term "dependability"), and to use the definition of IEC IS (IEV-191, Ed. 2), which at the moment sounds as follows: "Ability to perform as and when required".

Next, in GOST 27.002-89 dependability is a complex property, which, depending on the purpose of the object and the conditions of its application may include reliability, durability, maintainability, and storageability or some combination of these properties. In IEC IS the property of storageability is absent, but there are other properties, such as availability, which is not present in GOST 27.002-89 (although there are indicators that characterize this property, in particular, the availability factor).

Besides the above two important differences, IS differs from GOST by the presence of several dozens of new terms and the lack of a number of terms that existed in the national standard.

WG members believe that the standard under development should include all the most useful concepts of the two standards (IEV-191, Ed. 2 and GOST 27.002-89). Without going so far in the discussion on the undecided issues, we would like to give readers a chance to think about them without any influence from our side.

It should be noted that the 30-th of January, 2014 in MIIT a seminar on dependability was conducted under the guidance of Professor I.B. Shubinsky. This is the only ongoing seminar on dependability, actually working in Moscow. Two reports of WG members, representing two different approaches to the development of the new standard were presented in the seminar: "Topical issues of terminology standardization in dependability" by V.N. Netes and "Comparative analysis of key terms' definitions (dependability, failure, availability) according to GOST 27.002-89 and IEC" by Y.I. Tarasyev. We agreed that this discussion did not lead to the emergence of some common decision, i.e. differences between the members of the WG still remain.

Given the crucial importance of creating the new terminology standard, the authors would like all persons involved in the development works in the area of dependability in the Russian Federation to respond to this publication, and express their views in essence. We, on the other hand, plan to soon publish a second article on this topic, which will detail the arguments on both sides on the issue of a general definition of dependability, and which document should be taken as a basis for the new GOST.

References

1. Dependability theory in the field of radio electronics. Terminology: Collection of recommended terms. Issue 60 / Academy of Sciences of the USSR. Committee of tech. terminology, Institute of Radio Engineering and Electronics. – M., 1962.

2. **Demidovich N.O.** Terminology in dependability is harmonized! // Standards and Quality. 2011. # 2.

3. **Bogdanova G.A., Netes V.A.** IEC/TC 56: standardization in dependability // Methods of Quality Management. 2009. #5.

4. **Netes V.A., Rezinovsky A. Ya., Tarasyev Y.I., Ushakov I.A., Fishbein F.I., Shper V.L.** Degradation instead of harmonization // Standards and Quality. 2011. # 5.

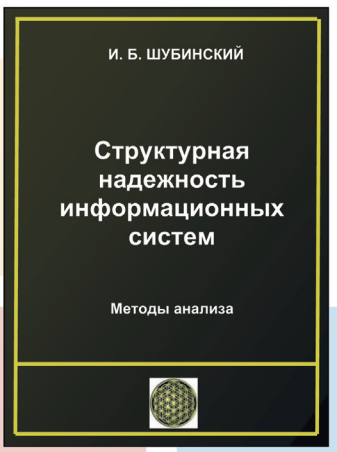
5. **Ushakov I.A.** Uninvited GOST // Methods of Quality Management. 2011# 5.

6. **Grigoriev A.** New GOST – "brains inside out"? // Standards and Quality. 2011. # 9.

7. **Demidovich N.O.** It is time to end the problem terminology of dependability // Standards and Quality. 2011. № #10.

НАДЁЖНОСТЬ
ISSN 1729-2646
НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

ПРЕДСТАВЛЯЕТ



Приобрести издание можно через редакцию ООО «Журнал «Надежность»

8 (495) 967-77-05, доб.186
8-916-105-81-31
(Патрикеева Евгения)

E.Patrikeeva@gismps.ru,
www.dependability.pro

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 70x100/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 17,55.
Тираж 700 экз. Заказ № 1452.

ООО «Журнал «Надежность»,
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 «Надежность»
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

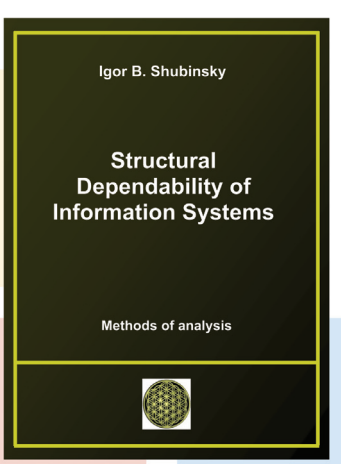
The book presents the basic concepts and parameters of the structural dependability of information systems. It discusses general and specific differences in dependability indices used in domestic and international standards, along with recent developments in approaches to dependability modeling. Markov 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
ISSN 1729-2646
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

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 70x100/16.
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
ISSN 1729-2646
НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

ПРЕДСТАВЛЯЕТ

Приобрести издание можно через редакцию ООО «Журнал «Надежность»

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 надежность информационных систем»
2012г.

В книге впервые представлена теория функциональной надежности информационных систем как составная часть общей теории надежности. Она включает понятия и определения; основные угрозы нарушения функциональной надежности информационных систем; систему показателей; методы оценки функциональной надежности цифровых устройств; методы и модели оценки функциональной надежности программного обеспечения. В отдельной главе рассмотрена функциональная надежность критически важных информационных систем, в том числе понятие критически важной системы, особенности оценки сбойных ошибок, оценки функциональной надежности операторов, оценки опасных отказов и рисков, требования к функциональной надежности 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 надежности 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 «Надежность»
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**

ООО «Журнал «Надежность»,
109029, г. Москва,
ул.Нижегородская, д.27, стр.1, офис 209
Тел./факс: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

Шубинский Игорь Борисович

ФУНКЦИОНАЛЬНАЯ 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 70x100/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 24,05.
Тираж 700 экз. Заказ № 1453.

Igor B. Shubinsky
FUNCTIONAL DEPENDABILITY OF INFORMATION SYSTEMS
2012

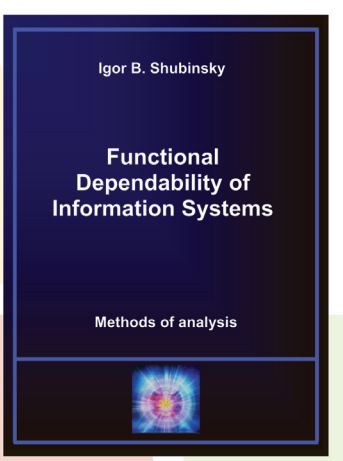
For the first time, this book presents the theory of functional dependability of information systems as a component of the general dependability theory. The book comprises basic concepts and definitions, major threats for the functional dependability of information systems, system parameters, methods 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
ISSN 1729-2646
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

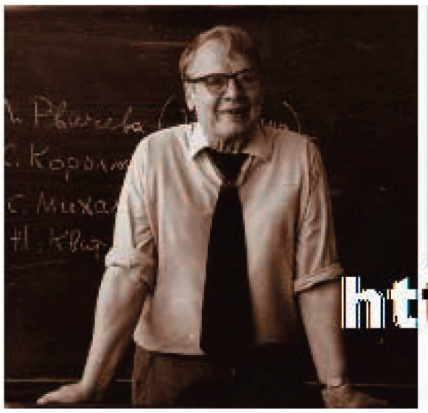
Journal Dependability Ltd.
109029, Moscow,
Nizhegorodskaya str., 27, bldg. 1, office 209
Tel. / Fax: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

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 70x100/16.
Offset printing. Offset paper. Conv. Sheet l. 24,05.
Circulation of 700 copies. Order number 1452.



Gnedenko e-Forum

International Group on Reliability

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!

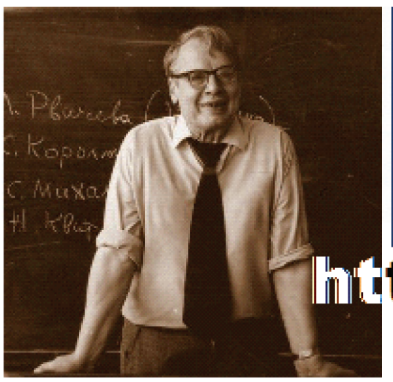
Добро пожаловать!

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.



Gnedenko e-Forum

International Group on Reliability

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

Абрамова Нина Александровна
доктор технических наук, заведующий лабораторией №51, Институт проблем управления им. В.А.Трапезникова РАН (ИПУ РАН)
тел.: +7 (495) 334-78-00
e-mail: kovriga@ipu.ru

Бочков Константин Афанасьевич
доктор технических наук, профессор, проректор по научной работе, научный руководитель НИЛ «Безопасность и ЭМС технических средств, «Белорусский государственный университет транспорта»
e-mail: bochkov1999@mail.ru

Володарский Владислав Афанасьевич
кандидат технических наук, старший научный сотрудник, профессор кафедры транспортных систем Красноярского института железнодорожного транспорта
тел. (8391) 221-60-72
e-mail: volodarsky.vladislav@yandex.ru

Гапанович Валентин Александрович
кандидат технических наук, главный инженер, старший вице-президент ОАО «РЖД»
тел.: +7 (495) 262-28-11

Дамзен Виктор Александрович
кандидат технических наук, доцент кафедры «Автомобили и автомобильное хозяйство», СГТУ им. Гагарина Ю.А.
тел.: +7 (906) 316-51-24
e-mail: damzen@yandex.ru

Елистратов Сергей Валерьевич
аспирант кафедры «Автомобили и автомобильное хозяйство», СГТУ им. Гагарина Ю.А.
тел.: +7 (927) 133-09-81
e-mail: elistratow.serg@yandex.ru

Коврига Светлана Вадимовна
научный сотрудник лаборатории №51, Институт проблем управления им. В.А.Трапезникова РАН (ИПУ РАН)
тел.: +7 (495) 334-78-00
e-mail: kovriga@ipu.ru

Макаренко Дмитрий Игоревич
старший научный сотрудник лаборатории №51, Институт проблем управления им. В.А.Трапезникова РАН (ИПУ РАН)
тел.: +7 (495) 334-78-00
e-mail: kovriga@ipu.ru

Медведев Аркадий Максимович
доктор технических наук, профессор, профессор кафедры 307, Московский авиационный институт
тел.: +7 (495) 158-46-48
e-mail: medvedevam@bk.ru

Нётес Виктор Александрович
доктор технических наук, профессор, начальник отдела прикладных задач развития телекоммуникаций, НТЦ «Комсет»
тел.: + 7 (495) 921-34-12

Пегушин Станислав Леонидович
аспирант, Пермский Национальный Исследовательский Политехнический Университет
тел.: +7 (951) 928-27-20
e-mail: staslp@mail.ru

Перегуда Аркадий Иванович
доктор технических наук, профессор, Обнинский институт атомной энергетики – филиал федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский ядерный университет «МИФИ»
тел.: +7 (962) 174-40-59
e-mail: Pereguda@iate.Obninck.ru

Розенберг Ефим Наумович
доктор технических наук, профессор, первый заместитель генерального директора ОАО «НИИАС»
тел.: +7 (499) 262-88-83, доб. 12222

Сивко Борис Витальевич
магистр технических наук, ассистент, лектор, «Белорусский государственный университет транспорта»
e-mail: bsivko@gmail.com

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

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»
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, Перм-

АВТОРЫ НОМЕРА / AUTHORS OF THIS ISSUE

ский Национальный Исследовательский Политехнический Университет
тел.: +7 (342) 2–391–506
e-mail: atp@pstu.ru

Abramova Nina Alexandrovna
Doctor of Technical Sciences, Head of Laboratory #51, V.A. Trapeznikov Institute of Control Sciences, Russian Academy of Sciences
Tel.: +7 (495) 334-78-00
E-mail: Lab51.ipu@gmail.com

Bochkov Konstantin Afanasievich
Doctor of Engineering, Professor, Pro-rector for scientific activities, Scientific Head of Equipment Safety and EMC Laboratory,
Byelorussian State University of Transport
E-mail: bochkov1999@mail.ru

Volodarsky Vladislav Afanasievich
PhD in engineering, senior researcher, associate professor of chair of transport systems,
Krasnoyarsk Institute of Railway Transport
Tel. (8391) 221-60-72
E-mail: volodarsky.vladislav@yandex.ru

Damzen Victor Alexandrovich
PhD Engineering, Assistant professor of Automobiles and Fleet Chair
Y.A. Gagarin SGTU
Tel.: +7 (906) 316-51-24
E-mail: damzen@yandex.ru

Gapanovich Valentin Alexandrovich
PhD Engineering, Chief Engineer, Senior Vice President of JSC RZD
Tel.: +7 (495) 262-28-11

Kovriga Svetlana Vadimovna
Researcher of Laboratory #51, V.A. Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences
тел.: +7 (495) 334-78-00
E-mail: kovriga@ipu.ru

Makarenko Dmitry Igorevich
Senior researcher of Laboratory #51, V.A. Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences
Tel.: +7 (495) 334-78-00
E-mail: Lab51.ipu@gmail.com

Medvedev Arkady Maksimovich
Doctor of technical Sciences, professor of Chair # 307, Moscow Aviation Institute
Tel.: +7 (495) 158-46-48
E-mail: medvedevam@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

Pegushin Stanislav Leonidovich
Post graduate student, Perm National Polytechnic Institute
Tel.: +7 (951) 928-27-20
E-mail: staslp@mail.ru

Pereguda Arkady Ivanovich
Professor, Doctor of Technical Sciences,
Obninsk Institute of Atomic Energy,
National Research Nuclear University MIFI
Tel.: +7 (962) 174-40-59
E-mail: Pereguda@iate.Obninck.ru

Rozenberg Efim Naumovich
Doctor of Technical Science, professor, First Deputy Director of JSC NIIAS
Tel.: +7 (499) 262-88-83, ext. 12222

Sivko Boris Vitalievich
Magister of Technical Sciences, assistant, lecturer
Byelorussian State University of Transport
E-mail: bsivko@gmail.com

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

Tarasyev Yuri Ivanovich Тарасьев
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

Yelistratov Sergey Valerievich
Post graduate student of Automobiles and Fleet Chair,
Y.A. Gagarin SGTU
Tel.: +7 (927) 133-09-81
E-mail: elistratow.serg@yandex.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@gismps.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 4 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, © 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 «RELIABILITY»

It is possible to subscribe to the journal for 2014:

- 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@gismps.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.

Текст необходимо набирать в редакторе Word 97-2003 шрифтом № 12; текст не форматируется. Абзацы организуются путем нажатия клавиши Enter. Текст статьи набирается через два интервала на странице формата А4; слева должно быть поле 4 см; страницы нумеруются, «красная строка» обязательна.

Все буквенные обозначения, приведенные на рисунках, необходимо пояснять в основном или подрисуночном 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, © — 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»

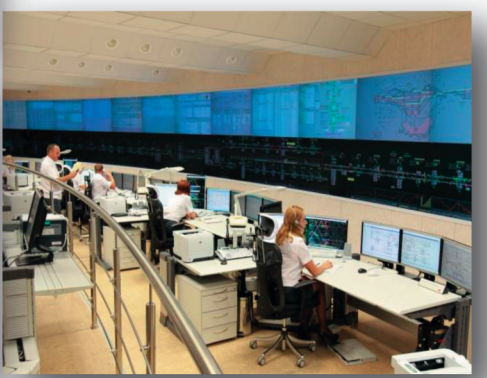
Подписаться на журнал на 2014 год можно:

- 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

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

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.

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.