



НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ / SCIENTIFIC- TECHNICAL JOURNAL

В НОМЕРЕ / IN THIS RELEASE:

- ОЦЕНКИ ХАРАКТЕРИСТИК НАДЕЖНОСТИ В ПРЕДПОЛОЖЕНИИ НЕПОЛНОГО ВОССТАНОВЛЕНИЯ
- *ASSESSMENT OF RELIABILITY PERFORMANCE UNDER THE ASSUMPTION OF INCOMPLETE RECOVERY*
- МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАДЕЖНОСТИ КОМПЛЕКСА «ОБЪЕКТ ЗАЩИТЫ – СИСТЕМА БЕЗОПАСНОСТИ» ПРИ НЕЧЕТКОЙ ИСХОДНОЙ ИНФОРМАЦИИ
- *MATHEMATICAL MODEL OF DEPENDABILITY FOR A COMPLEX "FACILITY OF PROTECTION – SAFETY SYSTEM" IN CASE OF FUZZY INITIAL INFORMATION*
- ОБЕСПЕЧЕНИЕ КАЧЕСТВА И АНАЛИЗ НАДЕЖНОСТИ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ НА ПРИМЕРЕ КОМПЛЕКСА АТЛАНТ
- *QUALITY ASSURANCE AND RELIABILITY ANALYSIS OF INFORMATION MEASURING SYSTEMS EXEMPLIFIED BY THE SYSTEM ATLANT*
- АНАЛИЗ НАДЕЖНОСТИ СЕТЕЙ, СОСТОЯЩИХ ИЗ ИДЕНТИЧНЫХ ЭЛЕМЕНТОВ
- *RELIABILITY ANALYSIS OF NETWORKS CONSISTING OF IDENTICAL ELEMENTS*
- РЕЗЕРВИРОВАНИЕ КАК СОСТАВНАЯ ЧАСТЬ ПРОБЛЕМЫ НАДЕЖНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ
- *REDUNDANCY AS PART OF THE RELIABILITY PROBLEM IN ELECTRIC-POWER INDUSTRY*
- ДОСТОВЕРНОСТЬ ПЕРЕДАЧИ ОТВЕТСТВЕННЫХ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ СХЕМ ПОРОГОВОЙ ФРАГМЕНТАЦИИ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ
- *ACCURACY OF VITAL MESSAGES TRANSMISSION USING THRESHOLD FRAGMENTATION METHODS AND ANTINOISE CODING*
- ОЦЕНКА РИСКОВ, СВЯЗАННЫХ С ИЗЛОМАМИ БОКОВЫХ РАМ ТЕЛЕЖЕК ГРУЗОВЫХ ВАГОНОВ
- *ASSESSMENT OF RISKS RELATED TO FRACTURES AND DEFECTS OF SIDE FRAMES OF FREIGHT CAR BOGIES*
- МОДЕЛЬ И МЕТОД ДЛЯ ОПРЕДЕЛЕНИЯ ПОДСИСТЕМ, НАИБОЛЕЕ ПОДВЕРЖЕННЫХ ДЕСТАБИЛИЗИРУЮЩИМ ВОЗДЕЙСТВИЯМ, В ИЕРАРХИИ СОСТАВНОГО ОБЪЕКТА ЗАЩИТЫ
- *MODEL AND METHOD FOR DEFINITION OF SUBSYSTEMS MOST EXPOSED TO DISTURBANCES AS PART OF A COMPLEX FACILITY OF PROTECTION*

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.

Главный редактор

Шубинский И.Б., д.т.н., проф.

Редколлегия

Бочков А.В., к.т.н.
Дзиркал Э.В., к.т.н.
Замышляев А.М., к.т.н.
Каштанов В.А., д.ф.-м.н., проф.
Кофанов Ю.Н., д.т.н., проф.
Лецкий Э.К., д.т.н., проф.
Нетес В.А., д.т.н., проф.
Розенберг И.Н., д.т.н.
Стась К.Н., к.т.н.
Тарасов А.А., д.т.н., проф.
Уткин Л.В., д.т.н., проф.
Ушаков И.А., д.т.н., проф.
Черкесов Г.Н., д.т.н., проф.
Шебе Х., д.ф.-м.н.
Щербаков О.В., д.т.н., проф.
Юркевич Е.В., д.т.н., проф.

Выпускающий редактор
Патрикеева Е.В.

Издатель журнала

ООО «Журнал «Надежность»

Директор
Калинина И.В.

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

Верстка
Куртиш Б.С.

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

Статьи рецензируются.

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

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

ISSN 1729-2646

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

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

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

THE JOURNAL PROMOTER:

“Journal “Reliability” Ltd

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

Official organ of the Russian Academy of Reliability

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

Editor-in-chief

I. Shubinsky, Dr. Sci., prof.

Editorial board

A. Bochkov, PhD.

E. Dzirkal, PhD.

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

J. Kofanov, Dr. Sci., prof.

E. Letsky, Dr. Sci., prof.

V. Netes, Dr. Sci., prof.

I. Rozenberg, Dr. Sci., prof.

K. Stas, Ph. D.

F. Tarasov, Dr. Sci., prof.

L. Utkin, Dr. Sci., prof.

I. Ushakov, Dr. Sci., prof.

G. Cherkesov, Dr. Sci., prof.

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

O. Shcherbakov, Dr. Sci., prof.

E. Jurkevich, Dr. Sci., prof.

A. Zamyshlaev, Ph. D.

Commissioning editor

E. Patrikeeva

Publisher of the journal

LLC Journal “Dependability”

Director

I. Kalinina

The address:

109029, Moscow,

Str. Nizhegorodskaya, 27,

Building 1, 1, office 209

Ltd Journal “Dependability”

www.dependability.pro

Make-up

B. Kurtish

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

Printing order

Papers are reviewed.

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

СОДЕРЖАНИЕ/CONTENTS

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

ОЦЕНКИ ХАРАКТЕРИСТИК НАДЕЖНОСТИ В ПРЕДПОЛОЖЕНИИ НЕПОЛНОГО ВОССТАНОВЛЕНИЯ Чумаков И.А., Антонов А.В.	3
ASSESSMENT OF RELIABILITY PERFORMANCE UNDER THE ASSUMPTION OF INCOMPLETE RECOVERY Chumakov I.A., Antonov A.V.	12
ОБЕСПЕЧЕНИЕ КАЧЕСТВА И АНАЛИЗ НАДЕЖНОСТИ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ НА ПРИМЕРЕ КОМПЛЕКСА АТЛАНТ Никитаев В.Г., Пронищев А.Н., Власов В.А., Власова С.В.	21
QUALITY ASSURANCE AND RELIABILITY ANALYSIS OF INFORMATION MEASURING SYSTEMS EXEMPLIFIED BY THE SYSTEM ATLANT Nikitayev V.G., Pronichev A.N., Vlasov V.A., Vlasova S.V.	26
АНАЛИЗ НАДЕЖНОСТИ СЕТЕЙ, СОСТОЯЩИХ ИЗ ИДЕНТИЧНЫХ ЭЛЕМЕНТОВ Ткачев О.А.	30
RELIABILITY ANALYSIS OF NETWORKS CONSISTING OF IDENTICAL ELEMENTS Tkachev O.A.	45
РЕЗЕРВИРОВАНИЕ КАК СОСТАВНАЯ ЧАСТЬ ПРОБЛЕМЫ НАДЕЖНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ Федотова Г.А.	60
REDUNDANCY AS PART OF THE RELIABILITY PROBLEM IN ELECTRIC-POWER INDUSTRY Fedotova G.A.	70

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

ДОСТОВЕРНОСТЬ ПЕРЕДАЧИ ОТВЕТСТВЕННЫХ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ СХЕМ ПОРОГОВОЙ ФРАГМЕНТАЦИИ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ Ададуров С.Е., Ададуров А.С., Мальцев Г.Н.	80
ACCURACY OF VITAL MESSAGES TRANSMISSION USING THRESHOLD FRAGMENTATION METHODS AND ANTINOISE CODING Adadurov S.E., Adadurov A.S., Maltsev G.N.	90

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

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАДЕЖНОСТИ КОМПЛЕКСА «ОБЪЕКТ ЗАЩИТЫ – СИСТЕМА БЕЗОПАСНОСТИ» ПРИ НЕЧЕТКОЙ ИСХОДНОЙ ИНФОРМАЦИИ Перегула А.И.	99
MATHEMATICAL MODEL OF DEPENDABILITY FOR A COMPLEX “FACILITY OF PROTECTION – SAFETY SYSTEM” IN CASE OF FUZZY INITIAL INFORMATION Pereguda A.I.	114
ОЦЕНКА РИСКОВ, СВЯЗАННЫХ С ИЗЛОМАМИ БОКОВЫХ РАМ ТЕЛЕЖЕК ГРУЗОВЫХ ВАГОНОВ Ермаков А.О., Новожилов Е.О.	129
ASSESSMENT OF RISKS RELATED TO FRACTURES AND DEFECTS OF SIDE FRAMES OF FREIGHT CAR BOGIES Ermaikov A.O., Novozhilov E.O.	138
МОДЕЛЬ И МЕТОД ДЛЯ ОПРЕДЕЛЕНИЯ ПОДСИСТЕМ, НАИБОЛЕЕ ПОДВЕРЖЕННЫХ ДЕСТАБИЛИЗИРУЮЩИМ ВОЗДЕЙСТВИЯМ, В ИЕРАРХИИ СОСТАВНОГО ОБЪЕКТА ЗАЩИТЫ Абрамова Н.А., Макаренко Д.И., Телицына Т.А.	146
MODEL AND METHOD FOR DEFINITION OF SUBSYSTEMS MOST EXPOSED TO DISTURBANCES AS PART OF A COMPLEX FACILITY OF PROTECTION Abramova N.A., Makarenko D.I., Telitsyna T.A.	159
КНИГА И.Б.ШУБИНСКОГО «СТРУКТУРНАЯ НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»	171
BOOK BY SHUBINSKY I.B. STRUCTURAL RELIABILITY OF INFORMATION SYSTEMS	171
КНИГА И.Б.ШУБИНСКОГО «ФУНКЦИОНАЛЬНАЯ НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»	172
BOOK BY SHUBINSKY I.B. FUNCTIONAL RELIABILITY OF INFORMATION SYSTEMS	172
ГНЕДЕНКО – ФОРУМ	173
GNEDENKO FORUM	174

Чумаков И.А., Антонов А.В.

ОЦЕНКИ ХАРАКТЕРИСТИК НАДЕЖНОСТИ В ПРЕДПОЛОЖЕНИИ НЕПОЛНОГО ВОССТАНОВЛЕНИЯ

Статья описывает современные способы параметрической оценки ведущей функции потока (ВФП) и параметра потока отказов в предположении неполного восстановления с использованием моделей Кижима. Проводится сравнение моделей между собой, а также с моделями, предполагающими полное или минимальное восстановление элемента (однородный и неоднородный пуассоновские процессы соответственно). Для оценки параметров модели используется метод максимизации функции правдоподобия. Для оценки ведущей функции потока, заданной в неявном виде, наиболее популярным методом является моделирование по методу Монте-Карло. В статье рассматривается пример применения разработанной методики для расчета характеристик надежности элементов, входящих в состав штатного оборудования энергоблоков АС.

Ключевые слова: неполное восстановление, модели Кижима, ведущая функция потока, параметр потока отказов.

Введение

Анализ надежности элементов и систем действующих АЭС является актуальной задачей современного этапа развития ядерной энергетики. Для проведения таких исследований применяются вероятностно-статистические методики оценки характеристик надежности. Наиболее употребительными для расчета надежности восстанавливаемых систем являются модели, предполагающие полное либо минимальное восстановление. Функционирование современных технических систем, как правило, представляет собой более сложный процесс, для которого характерно неполное или частичное восстановление. Различные типы восстановления могут быть классифицированы следующим образом:

- полное восстановление. Элемент восстанавливается до состояния, которое было у него на начальный момент времени («как новый», в зарубежной литературе используется термин «as good as new»). Данный тип восстановления можно трактовать как замену отказавшего элемента на новый.
- минимальное восстановление «как было перед отказом» («as bad as old»). Элемент восстанавливается до состояния, которое было у него на момент отказа.
- неполное восстановление «хуже чем новое, но лучше чем было перед отказом» («better than old but worse than new»). После восстановления элемент переходит в некоторое промежуточное состояние между двумя вышеописанными категориями.

- специфический случай «хуже, чем перед отказом» («worse than old»). После восстановления объект находится в состоянии худшем, чем до отказа.

Соответственно однородный процесс восстановления используется для моделирования полного восстановления, неоднородный пуассоновский процесс применяется для моделирования минимального восстановления. Такие процессы хорошо изучены и широко применяются на практике. Однако в наше время становятся все более востребованными модели, позволяющие учитывать неполное восстановление элемента, в том числе модель обобщенного процесса восстановления. Среди основополагающих работ на эту тему можно отметить [1]. Модели Кижима являются предметом исследования настоящей работы.

1. Обобщенный процесс восстановления, модели Кижима

Пусть v_{i-1} – виртуальный возраст элемента на момент $(i-1)$ -го восстановления. X_i – i -ая наработка на отказ. Тогда X_i имеет следующую функцию распределения [2-3]:

$$F_i(x) = \frac{F(x + v_{i-1}) - F(v_{i-1})}{1 - F(v_{i-1})}; \quad (1)$$

отсюда вероятность безотказной работы (ВБР) можно записать в виде:

$$P_i(x) = 1 - F_i(x) = \frac{P(x + v_{i-1})}{P(v_{i-1})}; \quad (2)$$

где $F(x)$ – функция распределения наработки до первого отказа для абсолютно нового элемента. Реальный возраст элемента можно записать в виде:

$$S_n = \sum_{i=1}^n x_i, S_0 = 0;$$

где X_i – i -тая наработка до отказа.

Модель «Kijima I» предполагает, что n -ное восстановление влияет только на повреждения, полученные элементом между $(n-1)$ -ым и n -ым отказом, уменьшив добавленный возраст элемента с X_i до qX_i . Виртуальный возраст элемента после n -ного восстановления можно записать в виде:

$$v_n = v_{n-1} + qX_n = q \sum_{i=1}^n X_i = qS_n; v_0 = 0; \quad (3)$$

где $q \geq 0$ – некоторый параметр модели, характеризующий степень n -ного восстановления. Здесь и на протяжении всей статьи предполагается $q = \text{const}$, хотя в общем случае значение q может различаться для каждого восстановления.

Модель «Kijima II» предполагает, что n -ное восстановление влияет на суммарные повреждения, полученные элементом на протяжении всего времени его функционирования:

$$v_n = q(v_{n-1} + X_n) = q(q^{n-1}X_1 + q^{n-2}X_2 + \dots + X_n). \quad (4)$$

Рассмотрим некоторые частные значения параметра q :

Случай $q=0$ описывает полное восстановление. Случайные процессы (3-4) вырождаются в однородные процессы восстановления.

Случай $q=1$ описывает минимальное восстановление. Случайные процессы (3-4) вырождаются в неоднородные пуассоновские процессы.

Случай $0 < q < 1$ описывает неполное восстановление «хуже чем новое, но лучше чем было перед отказом», являющееся предметом изучения данной статьи.

Наконец, специфический случай $q > 1$ – восстановление «хуже, чем перед отказом», в статье не рассматривается.

Математическое ожидание среднего числа отказов на интервале $(0; t]$ также известно как «функция восстановления», «ведущая функция потока» (в зарубежной литературе – «Cumulative Intensity Function», например [3]). В дальнейшем в тексте статьи используется термин «ведущая функция потока» (ВФП). Для случая неполного восстановления данная величина определяется уравнением [1, 3]:

$$H(t) = \int_0^t (g(\tau | 0) + \int_0^\tau h(x)g(\tau - x | x)dx)d\tau, \quad (5)$$

где:

$$g(t | x) = \frac{f(t + qx)}{1 - F(qx)}; h(t) = \frac{dH(t)}{dt}; f(t) = \frac{dF(t)}{dt}.$$

Решение (5) невозможно аналитическим путем и даже численное решение затруднительно [3]. В 1998 году Каминским и Кривцовым был предложен способ вычисления ведущей функции потока, использующий метод Монте-Карло. В настоящее время именно этот подход широко применяется для исследования обобщенных процессов восстановления. Для моделирования по методу Монте-Карло необходимо предполагать вид функции распределения наработки до первого отказа, параметры функции распределения, а также значения параметра q . Оценка параметров возможна различными способами.

2. Оценка параметров модели в предположении распределения Вейбулла

Каминский и Кривцов в своей работе [3] предлагают использовать метод наименьших квадратов:

$$\min_{\theta_1, \theta_2, \dots, \theta_p, q} \left(\sum_{i=1}^n (H_{эм}(t_i) - H_{МК}(t_i, \theta_1, \theta_2, \dots, \theta_p, q))^2 \right),$$

где $H_{эм}$ – эмпирическая ведущая функция потока; $H_{МК}$ – оценка функции по методу Монте-Карло; $(\theta_1, \theta_2, \dots, \theta_p)$ – вектор параметров распределения.

Оценка вектора $(\theta_1, \theta_2, \dots, \theta_p)$ и параметра модели q подобным образом влечет за собой большие вычислительные расходы.

Рассмотрим подробнее альтернативный подход, заключающийся в использовании метода максимального правдоподобия [2, 4, 5]. Предположим, что наработка до первого отказа имеет распределение Вейбулла. Необходимо заметить, что функция этого распределения имеет различные формы записи. В данной работе будем использовать следующий вид распределения, несколько упрощающий дальнейшие расчеты:

$$F(x) = 1 - \exp(-\lambda x^\beta). \quad (6)$$

Перепишем ВБР i -той наработки на отказ (2) с использованием (6):

$$P_i(x) = \frac{P(x + v_{i-1})}{P(v_{i-1})} = \frac{\exp(-\lambda(x + v_{i-1})^\beta)}{\exp(-\lambda v_{i-1}^\beta)} = \exp(\lambda(v_{i-1}^\beta - (x + v_{i-1})^\beta));$$

где $v_{i-1} = v_{i-1}(x_1, x_2, \dots, x_{i-1}, q)$ – виртуальный возраст элемента после $(i-1)$ -го отказа, равный (3) либо (4) в зависимости от используемой модели. Далее находим плотность распределения:

$$f_i(x) = -\frac{\partial P(x)}{\partial x} = \lambda \beta (x + v_{i-1})^{\beta-1} \exp(\lambda(v_{i-1}^\beta - (x + v_{i-1})^\beta)).$$

Функция правдоподобия

$$L(\lambda, \beta, q) = \prod_{i=1}^n f_i(x_i) = (\lambda \beta)^n \prod_{i=1}^n (x_i + v_{i-1})^{\beta-1} \exp(\lambda(v_{i-1}^\beta - (x_i + v_{i-1})^\beta)).$$

Возьмем натуральный логарифм от обеих частей

$$\ln L(\lambda, \beta, q) = n(\ln \lambda + \ln \beta) + \lambda \sum_{i=1}^n [v_{i-1}^\beta - (x_i + v_{i-1})^\beta] + (\beta - 1) \sum_{i=1}^n \ln(x_i + v_{i-1}). \quad (7)$$

Далее мы можем продифференцировать полученную логарифмическую функцию правдоподобия (7) по каждому из аргументов λ, β, q , приравнять производные к нулю и решить полученную систему относительно λ, β, q . К сожалению, аналитического решения для такой системы не было найдено, поэтому для решения применяются численные методы [2, 4, 5]. Стоит заметить, что современные программы математического моделирования (Matlab и т.п.) позволяют эффективно вычислять максимум заданной функции от многих переменных, избавляя от зачастую громоздких операций дифференцирования и явного указания системы уравнений.

3. Применение метода Монте-Карло для оценки характеристик процесса восстановления

3.1. Оценка ведущей функции потока

Считая известным вид функции распределения и имея оценки параметров, мы можем моделировать случайные процессы (3-4). Для оценки ВФП в точке T необходимо разыграть последовательность случайных величин – наработок до отказа. N_j – число отказов, произошедших до времени T , есть смоделированное значение функции восстановления, далее моделирование повторяется необходимое число раз S . Итоговая оценка функции $H_{MK}(T)$ вычисляется как среднее из смоделированных значений [5]:

$$H_{MK}(T) = \frac{1}{S} \sum_{i=1}^S N_i. \quad (8)$$

Воспользуемся методом обратных функций [6, стр. 371-373] для моделирования наработок на отказ. Функция распределения наработки определяется (1). Обозначим $F_i(x)=U$, запишем полученное выражение

$$U = \frac{F(x + v_{i-1}) - F(v_{i-1})}{1 - F(v_{i-1})}.$$

Откуда находим

$$x = F^{-1}((1 - F(v_{i-1}))U + F(v_{i-1})) - v_{i-1}. \quad (9)$$

Функция, обратная функции распределения Вейбулла в формуле (6), равна

$$F^{-1}(y) = \left[-\frac{\ln(1-y)}{\lambda} \right]^{\frac{1}{\beta}}. \quad (10)$$

Подставив (6) и (10) в (9), получим итоговую формулу для моделирования i -той наработки на отказ:

$$x_i = [(v_{i-1})^\beta - \frac{\ln U}{\lambda}]^{\frac{1}{\beta}} - v_{i-1}.$$

Для моделирования необходимо разыграть $U \sim U[0;1]$.

3.2. Оценка параметра потока отказов

ГОСТ [7] выделяет мгновенный параметр потока отказов (МППО), как предел отношения числа отказов на интервале, к длине интервала, стремящейся к нулю:

$$h(t) = \lim_{\Delta t \rightarrow 0} \frac{E(N(t + \Delta t) - N(t))}{\Delta t} = \frac{dH(t)}{dt};$$

а также средний параметр потока отказов (СППО) – среднее значение МППО на конечном интервале времени

$$\bar{h}(t_1; t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} h(t) dt.$$

В данной работе нас будет интересовать оценка СППО, которая может быть получена методом Монте-Карло аналогично ведущей функции потока (8):

$$h_{МК}(T) = \frac{1}{S} \sum_{i=1}^S \frac{n_i}{\Delta_i}; \quad (11)$$

где n_i – число отказов на интервале Δ_i , причем T – середина интервала Δ_i .

3.3. Оценка погрешности вычислений

Как известно, при использовании метода Монте-Карло можно получить оценку погрешности не гарантированно, а лишь с некоторой степенью достоверности. Согласно [8, стр.234] и центральной предельной теореме, получаем верхнюю границу ошибки вычислений интеграла по методу Монте-Карло (8) с коэффициентом доверия β :

$$\delta \leq t_\beta \sqrt{\frac{D(H_{МК})}{S}};$$

где: t_β – значение аргумента функции Лапласа $\Phi(t)$, при котором $\Phi(t) = \beta/2$ [6, стр. 365], $t_\beta = 3$ для $\beta = 0,997$ (правило трех сигм).

Неизвестную дисперсию $D(H_{МК})$ мы можем заменить ее несмещенной оценкой D :

$$D = H_{МК}^2 - (H_{МК})^2 = \frac{S}{S-1} \left(\sum_{i=1}^S N_i^2 - \left(\sum_{i=1}^S N_i \right)^2 \right).$$

Откуда искомая формула погрешности вычисления ВФП методом Монте-Карло в некоторой точке принимает вид:

$$\delta \leq t_{\beta} \sqrt{\frac{\sum_{i=1}^S N_i^2 - (\sum_{i=1}^S N_i)^2}{S-1}}; \quad (12)$$

Заметим, что $\delta \sim \sqrt{1/S}$, где S – количество итераций моделирования значения $H_{MK}(T)$ в точке T . Выбор в качестве S величины порядка 10^6 позволяет добиваться точности, приемлемой для большинства расчетов и не является проблемой при наличии современных вычислительных средств.

4. Пример расчета

Проведем расчет параметров представленной модели на реальных данных. Для этого воспользуемся информацией об отказах устройств накопления и обработки информации, работающих в составе штатного оборудования атомных станций. Для выбранного устройства за время эксплуатации $T \approx 4,5 \cdot 10^4$ ч. было зафиксировано 112 отказов. В качестве распределения наработки до первого отказа выбрано распределение Вейбулла. Используемые модели, соответствующие значения логарифмической функции правдоподобия (7) и оценки параметров приведены в таблице 1:

Таблица 1. Оценки параметров модели

Модель	$\ln L$	λ	β	q
Полное восстановление	-253.1316	0.3588	0.8563	-
Минимальное восстановление	-242.0335	0.0038	1.7130	-
Kijima I	-242.0336	0.0038	1.7131	0.9998
Kijima II	-241.8521	0.0017	1.8863	0.9930

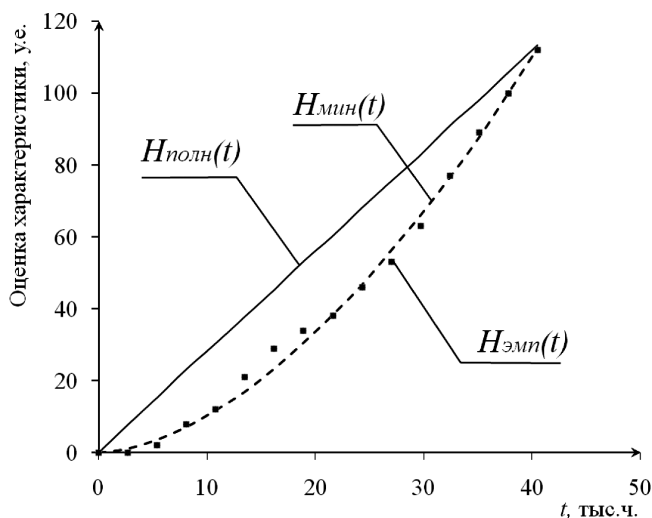


Рис. 1. Оценки ВФП для моделей полного и минимального восстановления

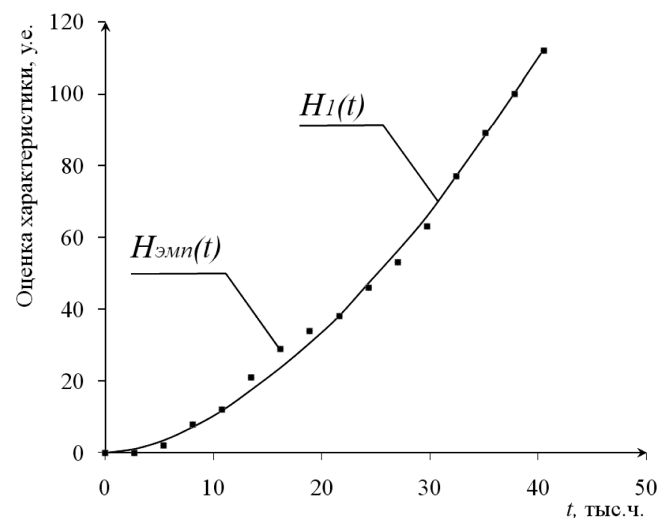


Рис. 2. Оценка ВФП для модели Kijima I

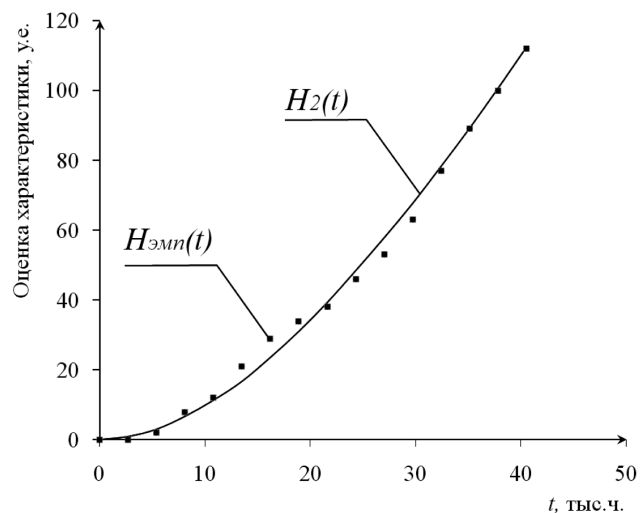


Рис. 3. Оценка ВФП для модели Kijima II

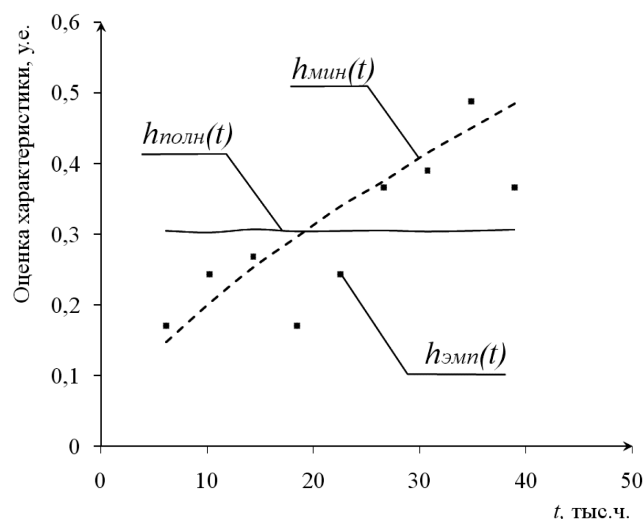


Рис. 4. Оценки СППО для моделей полного и минимального восстановления

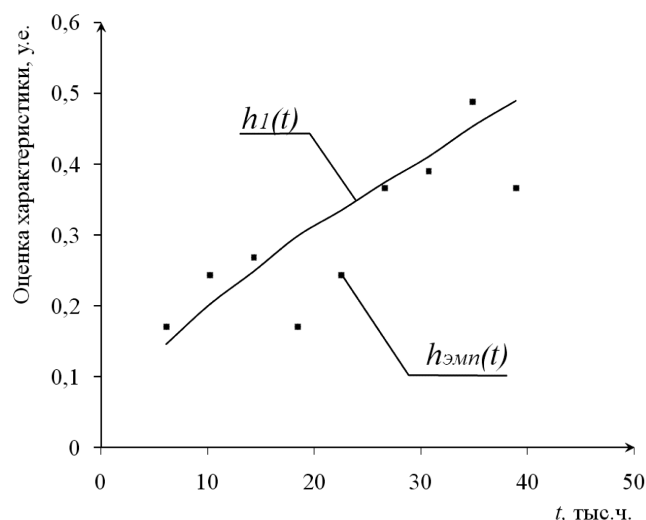


Рис. 5. Оценка СППО для модели Kijima I

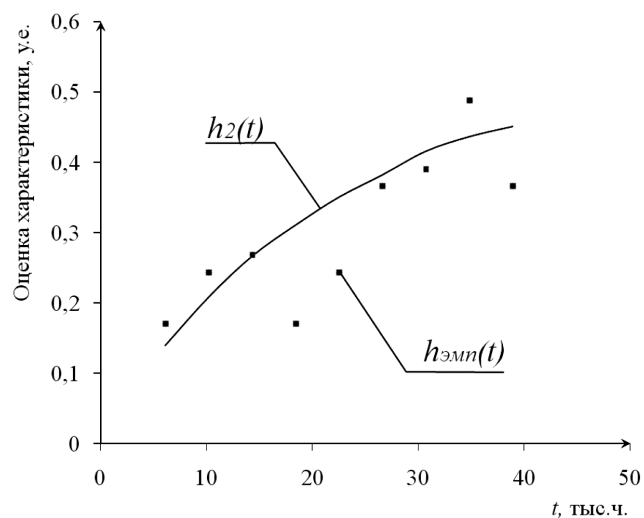


Рис. 6. Оценка СППО для модели Kijima II

Точечные оценки значений ВФП (8) и СППО (11) приведены на рисунках 1-6 соответственно. На данных рисунках приняты следующие обозначения:

$H_{\text{эмп}}(t)$ и $h_{\text{эмп}}(t)$ — эмпирические ВФП и СППО;

$H_{\text{полн}}(t)$ и $h_{\text{полн}}(t)$ — оценки ВФП и СППО в предположении полного восстановления;

$H_{\text{мин}}(t)$ и $h_{\text{мин}}(t)$ — оценки ВФП и СППО в предположении минимального восстановления;

$H_1(t)$ и $h_1(t)$ — оценки ВФП и СППО для модели Kijima I;

$H_2(t)$ и $h_2(t)$ — оценки ВФП и СППО для модели Kijima II.

Стоит заметить, что при выборе для S — количества итераций моделирования значения функции — величины порядка 10^6 , погрешность (12) вычисления функции по методу Монте-Карло составляет, как правило, не более 1% с уровнем доверительной вероятности 0,997.

Согласно приведенным в таблице 1 значениям функции правдоподобия, наилучшей моделью (минимум значения функции правдоподобия) для конкретного обработанного набора данных является модель «Kijima II». Основываясь на небольшой разнице в значениях функции правдоподобия (в пределах 0,5%), можно заключить, что для обработанных данных разница между моделями

Кижима и моделью неоднородного пуассоновского процесса в предположении минимального восстановления невелика и не позволяет с большой достоверностью указать наилучшую модель из исследуемых. Подобный вывод также подкрепляют представленные в таблице 1 схожие оценки параметров распределения Вейбулла и параметра q , характеризующего степень восстановления.

Заключение

В отличие от однородного и неоднородного процессов восстановления, модели обобщенного процесса восстановления, в т.ч. модели Кижима, позволяют учитывать случай неполного восстановления «хуже чем новое, но лучше чем было перед отказом». В статье описан метод оценки ведущей функции потока и среднего параметра потока отказов с использованием моделей «Kijima I» и «Kijima II», показывающий соответствие реальным данным. Проведены расчеты параметров модели по данным эксплуатации устройств накопления и обработки информации, работающих в составе штатного оборудования атомных станций.

Список литературы

1. Kijima M., Sumita N. A Useful Generalization of Renewal Theory: Counting Process Governed by Non-negative Markovian Increment. *Journal of Applied Probability* №23, 71-88, 1986.
2. Wibowo W. On approaches for repairable system analysis : Renewal Process, Nonhomogenous Poisson Process, General Renewal Process. Indonesia, *Jurnal Industri*, Volume IX, №1, 60-66, 2010.
3. Каминский М., Кривцов В. Применение метода Монте-Карло к оценке обобщенного процесса восстановления при анализе данных об отказах в период действия гарантийных обязательств. *Reliability: Theory & Applications* №1, January 2006 С. 32-34.
4. Kaminsky M. Krivtsov V. G1-Renewal Process as Repairable System Model, *Reliability and Risk Analysis: Theory & Applications*, #3, Vol.1, pp. 7-14, 2010.
5. Guo H., Liao H., Pulido J. Failure Process Modeling For Systems With General Repairs. MMR 2011. International Conference on Mathematical Methods in Reliability. "Methodology, Practice and Interference". Beijing, 2011
6. Гмурман В.Е. Теория вероятностей и математическая статистика. –М.: Высшая школа, 2000. – 480 с.
7. ГОСТ 53480-2009. Надежность в технике. Термины и определения.
8. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. –М.: Наука, 2003. – 635 с.

Chumakov I.A., Antonov A.V.

ASSESSMENT OF RELIABILITY PERFORMANCE UNDER THE ASSUMPTION OF INCOMPLETE RECOVERY

The paper describes modern techniques of parametrical estimation of the failure rate leading function and the assessed failure rate under the assumption of incomplete recovery using Kijima models. Models are compared among themselves and with the models assuming full or minimal recovery of a component (homogeneous and nonhomogeneous Poisson processes respectively). For estimating model parameters, the method of maximum likelihood function is used. For estimating the failure rate leading function given in implicit form, the most popular method of modeling is the Monte-Carlo method. The paper also offers an example of application of the developed technique for calculation of reliability characteristics of components, which are part of the regular equipment of NPP power units.

Keywords: incomplete recovery, Kijima models, rate leading function, assessed failure rate.

Introduction

The analysis of components reliability and systems of operating NPP is an urgent problem of the present stage in development of nuclear power. The probabilistic-statistical techniques for estimation of reliability characteristics are applied to carry out such researches. The most common for calculation of reliability of recovered systems are the models assuming full or minimal recovery. The functioning of modern technical systems, as a rule, is more complex process, for which incomplete or partial recovery is typical. Various types of recovery can be classified as follows:

1) full recovery; the component is restored up to the condition, which it had at the initial moment of time (“as new”, in foreign literature the term “as good as new” is used). The given type of recovery can be treated as replacement of the failed component with a new one.

2) minimal recovery of a component “as it was before failure” (“as bad as old”). The component is recovered up to the condition, which it had at the moment of failure.

3) incomplete recovery of a component “is worse than new but better than it was before failure” (“better than old but worse than new”). After recovery, the component passes in some intermediate condition between two above described categories.

4) specific case “is worse than before failure” (“worse than old”). After recovery, the object is in a worse condition than before failure.

Accordingly, homogeneous process of recovery is used for modeling of full recovery, nonhomogeneous Poisson process is applied to modeling of minimal recovery. Such processes are well studied and widely

used in practice. However, presently there are more demands for models, allowing us to consider incomplete recovery of a component, including a model of the generalized process of recovery. The study [1] is among the basic works on this subject. Kijima models are an object of the present research.

1. Generalized process of recovery, Kijima models

Let v_{i-1} is the virtual age of a component for the time of $(i-1)$ -th recovery. X_i is the i -th time between failures. Then X_i has following function of distribution [2-3]:

$$F_i(x) = \frac{F(x + v_{i-1}) - F(v_{i-1})}{1 - F(v_{i-1})}; \quad (1)$$

hence, the probability of non-failure operation can be written down in the following form:

$$P_i(x) = 1 - F_i(x) = \frac{P(x + v_{i-1})}{P(v_{i-1})}; \quad (2)$$

where $F(x)$ is the function of distribution of time to the first failure (for a new component). The real age of the component can be written down in the following form:

$$S_n = \sum_{i=1}^n x_i, S_0 = 0;$$

where X_i is the i -th time to failure.

The model “Kijima I” assumes that the n -th recovery influences only the damages suffered by a component between $(n-1)$ -th and n -th failures reducing the added age of the component from X_i up to qX_i . The virtual age of a component after the n -th recovery can be written down as follows:

$$v_n = v_{n-1} + qX_n = q \sum_{i=1}^n X_i = qS_n; v_0 = 0; \quad (3)$$

where $q \geq 0$ is some parameter of the model describing the degree of the n -th recovery. Here and in what follows, it is supposed that $q = \text{const}$, though, generally, the value of q can differ for each recovery.

The model “Kijima II” assumes that the n -th recovery influences the total damages suffered by a component during the whole time of its functioning:

$$v_n = q(v_{n-1} + X_n) = q(q^{n-1}X_1 + q^{n-2}X_2 + \dots + X_n). \quad (4)$$

Let us consider some particular values of parameter q :

The case $q=0$ describes full recovery. Random processes (3-4) degenerate into homogeneous processes of recovery.

The case $q=1$ describes the minimal recovery. Random processes (3-4) degenerate into heterogeneous Poisson processes.

The case $0 < q < 1$ describes incomplete recovery “worse than new but better than it was before failure” that is a subject of this paper study.

Finally, the specific case $q > 1$, i.e. the recovery “is worse than it was before failure”, is not considered in this study.

Expectation of the average number of failures on an interval $(0; t]$ is also known as “function of recovery”, “the failure rate leading function” (in foreign literature as “Cumulative Intensity Function”, for example, in [3]). In what follows, the term “the failure rate leading function” is used in the text of this paper. For a case of incomplete recovery, the given value determined by the equation [1, 3]:

$$H(t) = \int_0^t (g(\tau | 0) + \int_0^\tau h(x)g(\tau - x | x)dx)d\tau, \quad (5)$$

where:

$$g(t | x) = \frac{f(t + qx)}{1 - F(qx)}; h(t) = \frac{dH(t)}{dt}; f(t) = \frac{dF(t)}{dt}.$$

The solution of (5) is impossible analytically, and even the numerical solution is difficult [3]. In 1998 Kaminsky and Krivtsov offered the method for calculation of the failure rate leading function using a Monte-Carlo approach. Now this approach is widely applied to research of the generalized processes of recovery. For modeling based on the Monte-Carlo method, it is necessary to assume the form of distribution function of operating time to the first failure, parameters of distribution function, and the value of the parameter q . The estimation of parameters is possible in various ways.

2. Estimation of model parameters under the assumption of Weibull distribution

Kaminsky and Krivtsov in the work [3] suggest using the least square method:

$$\min_{\theta_1, \theta_2, \dots, \theta_p, q} \left(\sum_{i=1}^n (H_{\text{emn}}(t_i) - H_{MK}(t_i, \theta_1, \theta_2, \dots, \theta_p, q))^2 \right),$$

where H_{emn} is an empirical failure rate leading function,

H_{MK} is estimation of the function using the Monte-Carlo method,

$(\theta_1, \theta_2, \dots, \theta_p)$ is a vector of distribution parameters.

The estimation of the vector $(\theta_1, \theta_2, \dots, \theta_p)$ and the model parameter q in a similar way entails heavy great computing expenses.

Let us consider in more detail the alternative approach consisting in use of a method of maximal likelihood [2, 4, 5]. We shall assume that the mean time to the first failure has a Weibull distribution. It is necessary to notice that the function of this distribution has various forms of writing. In this paper, we shall use the following kind of distribution simplifying a little bit the further calculations:

$$F(x) = 1 - \exp(-\lambda x^\beta). \quad (6)$$

Let us rewrite the probability of non-failure operation for the i -th time to failure (2) using (6):

$$P_i(x) = \frac{P(x + v_{i-1})}{P(v_{i-1})} = \frac{\exp(-\lambda(x + v_{i-1})^\beta)}{\exp(-\lambda v_{i-1}^\beta)} = \exp(\lambda(v_{i-1}^\beta - (x + v_{i-1})^\beta));$$

where $v_{i-1} = v_{i-1}(x_1, x_2, \dots, x_{i-1}, q)$ is the virtual age of a component after the $(i-1)$ -th failure is equal to (3) or to (4) depending on a model used. Further, we shall find the density of distribution:

$$f_i(x) = -\frac{\partial P(x)}{\partial x} = \lambda \beta (x + v_{i-1})^{\beta-1} \exp(\lambda(v_{i-1}^\beta - (x + v_{i-1})^\beta)).$$

The function of likelihood:

$$L(\lambda, \beta, q) = \prod_{i=1}^n f_i(x_i) = (\lambda \beta)^n \prod_{i=1}^n (x_i + v_{i-1})^{\beta-1} \exp(\lambda(v_{i-1}^\beta - (x_i + v_{i-1})^\beta)).$$

Let us take the natural logarithm from both parts:

$$\ln L(\lambda, \beta, q) = n(\ln \lambda + \ln \beta) + \lambda \sum_{i=1}^n [v_{i-1}^\beta - (x_i + v_{i-1})^\beta] + (\beta - 1) \sum_{i=1}^n \ln(x_i + v_{i-1}). \quad (7)$$

Then, we can derive the received logarithmic function of likelihood (7) on each of arguments λ, β, q , to equate derivatives to zero and to solve the received system in relation to λ, β, q . Unfortunately, the analytical solution for such a system has not been found, therefore numerical methods are applied to the solution [2, 4, 5]. It is necessary to notice that modern software for mathematical modeling (Matlab, etc.) allow calculating effectively the maximum of the given function from many variables saving us from often bulky operations of deriving and explicit reference to a system of equations.

3. Application of Monte-Carlo method for estimation of characteristics of recovery process

3.1. Estimation of failure rate leading function

Assuming that the form of a distribution function is known and having estimations of parameters, we can model random processes (3-4). For estimation of the failure rate leading function at point T , it is necessary to use a sequence of random variables – mean times to failure. N_j , i.e. the number of failures which have occurred till time T , is the simulated value of recovery function, and further, simulation is repeated a necessary number of times S . The final estimation of function $H_{MK}(T)$ is calculated as an average from the simulated values [5]:

$$H_{i\hat{E}}(T) = \frac{1}{S} \sum_{i=1}^S N_i. \quad (8)$$

Let us apply the method of inverse functions [6, p. 371-373] for modeling a mean time between failures. The distribution function of mean time between failures is determined as (1). We shall designate $F_i(x)=U$ and write down the obtained expression:

$$U = \frac{F(x + v_{i-1}) - F(v_{i-1})}{1 - F(v_{i-1})};$$

from which we shall find:

$$x = F^{-1}((1 - F(v_{i-1}))U + F(v_{i-1})) - v_{i-1}. \quad (9)$$

An inverse Weibull distribution function in the form of (6) is equal to the following:

$$F^{-1}(y) = \left[-\frac{\ln(1-y)}{\lambda} \right]^{\frac{1}{\beta}}. \quad (10)$$

Having substituted (6) and (10) in (9), we shall obtain the final formula for modeling the i -th mean time between failures:

$$x_i = \left[(v_{i-1})^\beta - \frac{\ln U}{\lambda} \right]^{\frac{1}{\beta}} - v_{i-1}.$$

To carry out simulation, it is necessary to use $U \sim U[0; 1]$.

3.2. Estimation of failure rate

GOST [7] distinguishes an instantaneous parameter of failure rate (IPFR), as a limit ratio of the number of failures on an interval to the length of that interval tending to zero:

$$h(t) = \lim_{\Delta t \rightarrow 0} \frac{E(N(t + \Delta t) - N(t))}{\Delta t} = \frac{dH(t)}{dt};$$

and also the average parameter of failure rate (APFR) is the average value of IPFR on a finite interval of time:

$$\bar{h}(t_1; t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} h(t) dt;$$

In this study, we are interested in estimation of APFR, which can be obtained by a Monte-Carlo method similarly to the failure rate leading function (8):

$$h_{MK}(T) = \frac{1}{S} \sum_{i=1}^S \frac{n_i}{\Delta_i}; \quad (11)$$

where n_i is the number of failures on an interval Δ_i , and T is the middle of an interval Δ_i .

3.3. Estimation of an error of calculations

As is known, when using a Monte-Carlo method, it is possible to obtain an error estimation, which is not guaranteed, but only insured with some degree of confidence. According to [8, p.234] and the central limit theorem, we obtain the upper boundary of an error of integral calculations using a Monte-Carlo method (8) with confidence factor β :

$$\delta \leq t_\beta \sqrt{\frac{D(H_{MK})}{S}};$$

where t_β is the value of the argument of Laplace function $\Phi(t)$, for which $\Phi(t) = \beta/2$ [6, p. 365]. $t_\beta = 3$ for $\beta = 0,997$ (three sigma rule).

The unknown dispersion $D(H_{MK})$ can be replaced by its unbiased estimate D :

$$D = H_{MK}^2 - (H_{MK})^2 = \frac{S}{S-1} \left(\sum_{i=1}^S N_i^2 - \left(\sum_{i=1}^S N_i \right)^2 \right).$$

From which the required formula for an error of calculation the failure rate leading function by using a Monte-Carlo method takes the following form at some point:

$$\delta \leq t_\beta \sqrt{\frac{\sum_{i=1}^S N_i^2 - \left(\sum_{i=1}^S N_i \right)^2}{S-1}}; \quad (12)$$

It should be noted that $\delta \sim \sqrt{1/S}$, where S is the number of iterations of modeling the value $H_{MK}(T)$ at point T . The choice of the value of order 10^6 as S allows us to achieve the accuracy acceptable for the majority of calculations and is not a problem for modern computing means.

4. An example of calculation

Let us calculate parameters of the presented model using real data. For this purpose, we shall take advantage of the information on failures of accumulation and processing data devices, operating in the structure of the NPP regular equipment. For the chosen device during operation $T \approx 4,5 \cdot 10^4$ h, 112 failures have been registered. A Weibull distribution has been selected as distribution of mean time to

the first failure. The used models, the corresponding values of logarithmic function of likelihood (7) and estimations of parameters are presented in Table 1:

Table 1. Estimations of model parameters

Model	lnL	λ	β	q
Full recovery	-253.1316	0.3588	0.8563	-
Minimal recovery	-242.0335	0.0038	1.7130	-
Kijima I	-242.0336	0.0038	1.7131	0.9998
Kijima II	-241.8521	0.0017	1.8863	0.9930

Point estimations of values of the failure rate leading function FRLF (8) and APFR (11) are presented in Figures 1-6 respectively. In the given figures, the following designations are accepted:

$H_{\text{эмн}}(t)$ and $h_{\text{эмн}}(t)$ are empirical FRLF and APFR;
 $H_{\text{полн}}(t)$ and $h_{\text{полн}}(t)$ are estimations of FRLF and APFR under the assumption of full recovery.;
 $H_{\text{мин}}(t)$ and $h_{\text{мин}}(t)$ are estimations of FRLF and APFR under the assumption of minimal recovery;
 $H_1(t)$ and $h_1(t)$ are estimations of FRLF and APFR for Kijima I model;
 $H_2(t)$ and $h_2(t)$ are estimations FRLF and APFR for Kijima II model.

It should be noted that if the choice of S (the number of iterations for modeling of function value) is equal to the size of order 10^6 , the error (12) of function estimation using a Monte-Carlo method makes up, as a rule, no more than 1% with the level of confidence probability 0,997.

According to the values of the function of likelihood presented in Table 1, the best model (a minimal value of function of likelihood) for the specific processed data set is the Kijima II model. Based on a small difference in values of function of likelihood (within the limits of 0,5 %), it is possible to conclude that, for the processed data, the difference between Kijima models and the model of heterogeneous Poisson process under the assumption of the minimal recovery is insignificant and does not allow us to specify

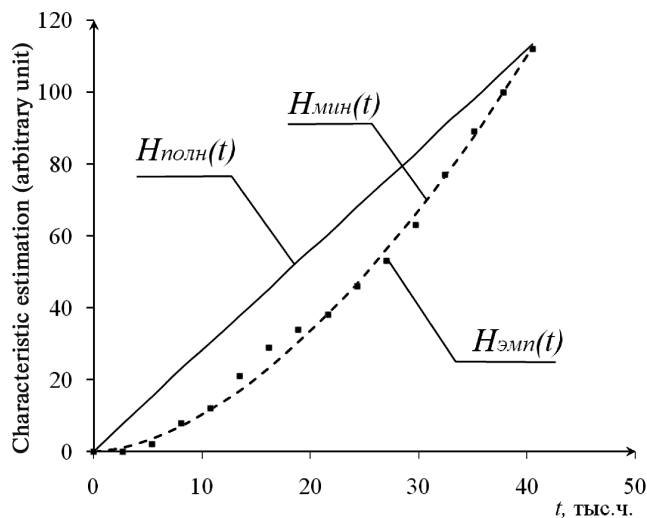


Fig. 1. Estimations of the failure rate leading function for models of full and minimal recovery

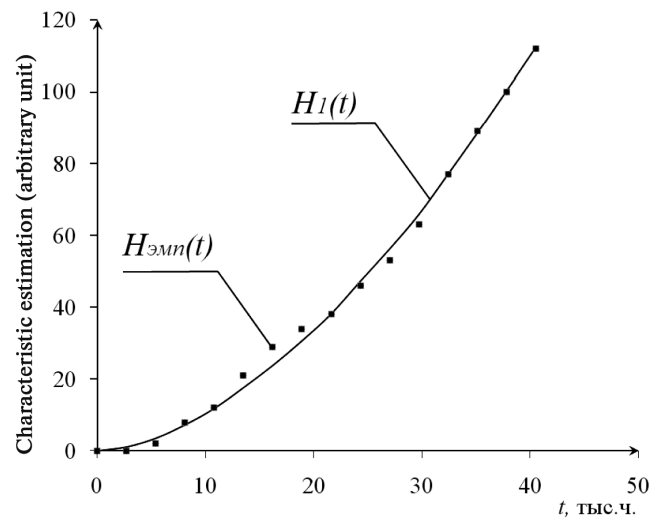


Fig. 2. Estimation of the failure rate leading function for Kijima I model

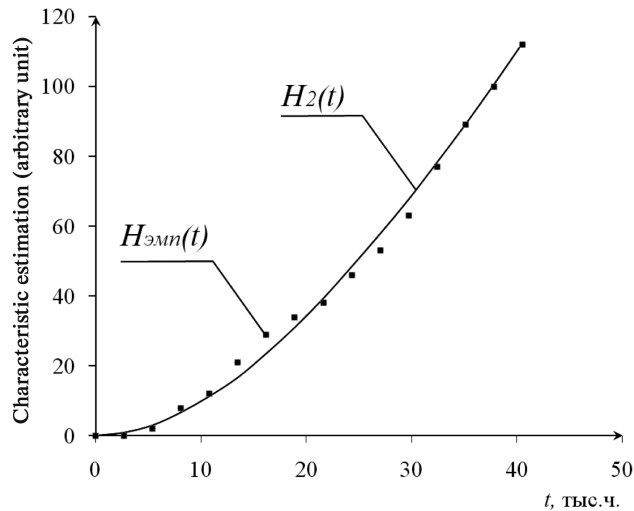


Fig. 3. Estimation of the failure rate leading function for Kijima II model

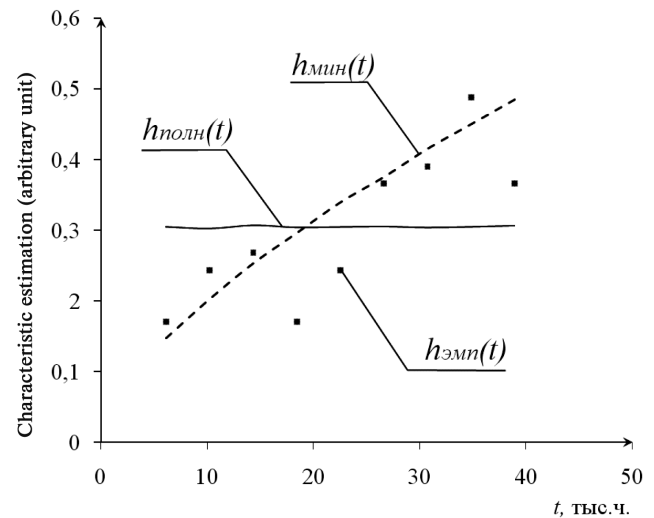


Fig. 4. Estimations of APFR for models of full and minimal recovery

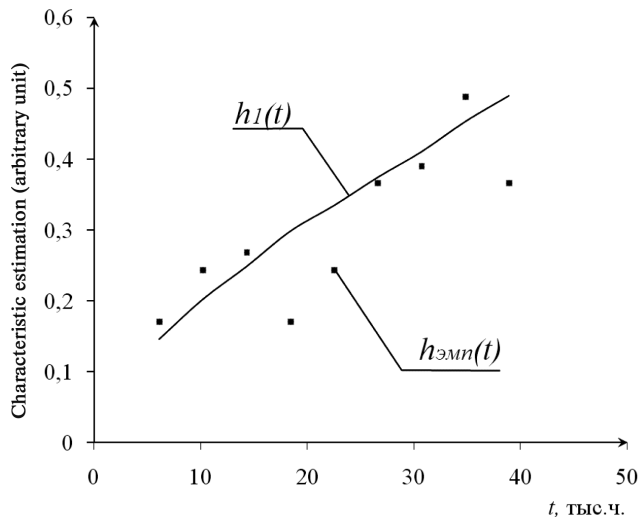


Fig. 5. Estimation of APFR for Kijima I model

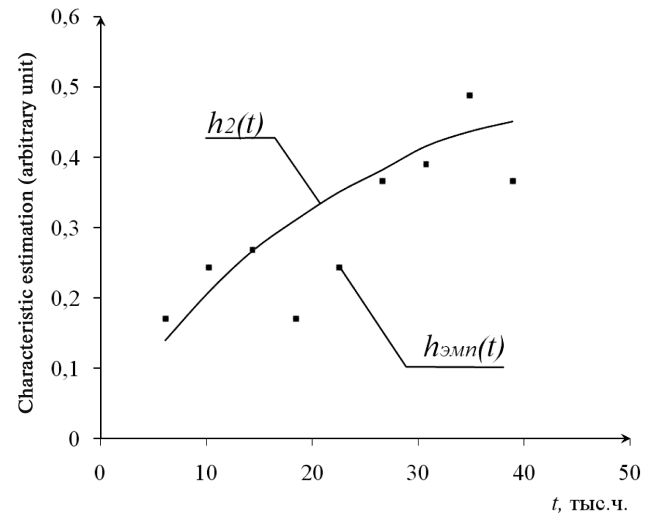


Fig. 6. Estimation of APFR for Kijima II model

with the high confidence the best model from investigated ones. The similar conclusion is also supported by the similar estimations of parameters of Weibull distribution presented in Table 1 and the parameter q describing a recovery degree.

Conclusion

Unlike homogeneous and nonhomogenous processes of recovery, a model of the generalized process of recovery, including Kijima models, allow us to take into account a case of incomplete recovery “worse than new but better than it was before failure”. This paper describes the method of estimation of the failure rate leading function and the mean assessed failure rate with use of models “Kijima I” and “Kijima II” showing conformity to real data. Calculations of model parameters according to accumulation and processing operation data of devices functioning within the regular equipment of NPP power units have been presented.

References

1. **Kijima M., Sumita N.** A Useful Generalization of Renewal Theory: Counting Process Governed by Non-negative Markovian Increment. *Journal of Applied Probability* №23, 71-88, 1986.
2. **Wibowo W.** On approaches for repairable system analysis: Renewal Process, Nonhomogenous Poisson Process, General Renewal Process. Indonesia, *Jurnal Industri*, Volume IX, №1, 60-66, 2010.
3. **Kaminsky M., Krivtsov V.** Application of Monte-Carlo approach to estimation of the generalized process of recovery at the analysis of data about failures during validity of guarantee certificates. *Reliability: Theory and Applications* №1, January 2006 pp.32-34.
4. **Kaminsky M., Krivtsov V.** G1-Renewal Process as Repairable System Model, *Reliability and Risk Analysis: Theory and Applications*, #3, Vol.1, pp. 7-14, 2010.
5. **Guo H., Liao H., Pulido J.** Failure Process Modeling For Systems With General Repairs. *MMR* 2011. International Conference on Mathematical Methods in Reliability. “ Methodology, Practice and Interference “. Beijing, 2011
6. **Gmurman V.E.** Probability theory and mathematical statistics.-M.: Higher school, 2000. – 480 p.
7. GOST 53480-2009. Reliability in technical equipment. Terms and definitions.
8. **Bahvalov H.C., Zhidkov N.P., Kobelykov G.M.** Numerical methods.-M.: Nauka, 2003. – 635 p.

Никитаев В. Г., Проничев А. Н., Власов В. А., Власова С. В.

ОБЕСПЕЧЕНИЕ КАЧЕСТВА И АНАЛИЗ НАДЕЖНОСТИ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ НА ПРИМЕРЕ КОМПЛЕКСА АТЛАНТ

Приводится описание разработанных мер повышения качества комплекса Атлант и надежности его работы.

Ключевые слова: надежность, интенсивность отказов, поддержка принятия решений, качество онкологической диагностики.

Для решения задач повышения качества диагностики онкологических заболеваний создана телемедицинская сеть «РОСАТОМ-ФМБА-МИФИ» с центром управления на кафедре «Компьютерные медицинские системы» Национального исследовательского ядерного университета «МИФИ» (НИЯУ МИФИ). Телемедицинская сеть построена на базе высокотехнологичных комплексов онкологической диагностики Атлант и объединяет многочисленных абонентов на территории России, таких как медсанчасти (МСЧ), научные центры, клинические больницы [1]. В диагностическую сеть включены: НИЯУ МИФИ, Российский онкологический научный центр им. Н.Н.Блохина РАМН, ЦМСЧ №141 (г.Удомля, Калининская АЭС), МСЧ №135 (г. Десногорск, Смоленская АЭС), МСЧ №125 (г. Курчатова, Курская АЭС), МСЧ №118 (г. Полярные Зори, Кольская АЭС), МСЧ №33 (г. Нововоронеж, Нововоронежская АЭС), ЦМСЧ №38 (г. Сосновый Бор, Ленинградская АЭС), Саратовский медицинский центр ФМБА (г. Балаково, Балаковская АЭС). Планируется дальнейшее расширение телемедицинской сети по всей территории РФ путем введения новых серверных мощностей и подключения дополнительных абонентов к сети.

Комплекс Атлант является важнейшим инструментом для реализации технологии поддержки принятия врачебных решений на базе экспертных систем и дистанционного консультирования, а также своевременной и оперативной поддержки медицинского персонала необходимыми данными, которые могут быть затребованы, например, в процессе проведения хирургической операции. При участии специалистов Российского онкологического центра им. Н.Н. Блохина РАМН, Клинических больниц № 83 и № 85 и др. в рамках комплекса сформирована уникальная эталонная база знаний, содержащая цветные изображения препаратов опухолей различных органов и соответствующие им стандартизованные описания.

Экспертные системы основаны на базе данных, которая хранится на серверах в центре управления телемедицинской сетью. При этом каждое медицинское учреждение имеет свою копию базы. Это связано с тем, что прямое обращение к базе значительно повышает нагрузку на сеть и, следовательно, снижает скорость работы. Обращение потребителей к архиву консультаций должно происходить с минимальными временными затратами и минимальной нагрузкой на сеть. Поэтому формат оцифрованных изображений (разрядность, разрешение, сжатие и т.д.) определяется требуемым качеством изображения, достаточным для достоверной диагностики. Избыточность передаваемых данных отрицательно сказывается на скорости передачи и времени, которое затрачивается на консультацию. Особо остро эта проблема стоит во время экспресс-диагностики при операциях, когда хирург ждет ответа врача-диагноста для определения объема и тактики хирургического вмешательства.

Материалом для создания базы знаний послужили многочисленные клинические случаи, подробно описанные высококвалифицированными врачами (экспертами), что позволяет рядовым врачам при работе с комплексом Атлант опираться на опыт ведущих специалистов страны при принятии ответственных диагностических решений.

В рамках системы реализована поддержка принятия врачебных решений при гистологической диагностике, построенной на базе автоматизированных систем обработки изображений, которая оказывает незаменимую помощь при постановке диагноза. Диагностический комплекс Атлант, в котором реализованы модели компьютерного макро- и микроанализа, технологии оперативной передачи запрашиваемых данных и дистанционного консультирования, успешно эксплуатируется более 10 лет в клинической практике.

К системам ответственного назначения, к классу которых относится Атлант, предъявляются высокие требования к качеству и надежности функционирования. Выполнение данных требований обеспечивается подбором соответствующих программно-аппаратных средств и архитектуры системы, применяемыми протоколами передачи данных. Среди опасных факторов, негативно влияющих на работоспособность системы, особо следует выделить угрозы, связанные с потерей или искажением передаваемых данных, что требует проведения ряда дополнительных мероприятий по повышению надежности.

В качестве среды передачи данных в комплексе Атлант используется широко применяемая глобальная сеть Интернет. Данное средство имеет ряд недостатков, таких, как зависимость от провайдеров, возможное падение скорости передачи данных при перегрузках сети, подверженность несанкционированному доступу и др. Последний вопрос крайне актуален в настоящее время. При полностью открытом обмене возникает проблема достоверности получаемой информации. Оперативная медицинская информация должна быть защищена. По этой причине возникла необходимость применения специальных методов защиты медицинских данных. Разработанный программный продукт позволяет решать следующие задачи:

- проверка и подтверждение подлинности источника сообщения;
- конфиденциальность и целостность данных (т.е. гарантия невозможности несанкционированного изменения информации);
- аутентификация (подтверждение подлинности сторон).

Комплекс Атлант обеспечивает проведение оперативных дистанционных медицинских консультаций в реальном времени и с должным качеством связи, поэтому должен обладать высокой отказоустойчивостью и способностью быстро восстанавливаться после сбоев. За отказы системы будем принимать любые события, приводящие к невозможности передачи изображения, а также

частичной или полной потери связи. Это могут быть отказы аппаратуры, обеспечивающей регистрацию оптического изображения, формирование цифровых данных и их обработку, сбои в каналах передачи данных и др. Подобные отказы в медицинской оперативной практике являются недопустимыми.

В связи с этим для повышения надежности разработчиками рассматриваемой системы была применена специальная программа мониторинга сети, которая предоставляет возможность дистанционного анализа неполадок и быстрого реагирования на них. Как показала практика эксплуатации телемедицинской сети «Росатом-ФМБА-МИФИ», удаленные от центра управления узлы сети зачастую имеют ограниченную пропускную способность интернет-каналов. В некоторых случаях скорость передачи каналов не превышает 256 Кб/с и может опускаться даже ниже. Задача программы мониторинга состоит в оперативном отслеживании состояния сети и нахождении неисправностей (например, проблем, вызванных перегруженными и/или отказавшими серверами, другими устройствами или сетевыми соединениями, периодической потери соединения, снижении производительности сети, длительной загрузки серверов и др.). Программа мониторинга является эффективным инструментом для управления компьютерной сетью и выполняет ряд важных функций, в их числе:

- контроль и мониторинг ресурсов компьютерной сети;
- выделение необходимой памяти для выполнения вычислительных задач;
- управление конфигурацией сети;
- диагностика неисправностей.

Внедрение компьютерного комплекса поддержки принятия решений при проведении анализа и постановке диагноза неизбежно поднимает вопрос точности рекомендуемых решений автоматизированных систем диагностики. Поскольку правильное описание микроскопического препарата в сильной мере зависит от качества цифрового изображения, особое внимание было уделено разработке цветовой калибровки комплекса, позволяющей минимизировать погрешности при автоматизированной выдаче экспертной информации. Для этой цели медицинским персоналом совместно с техническими специалистами осуществлен выбор специального оборудования, которое включает микроскопы, блоки управления микроскопами, фотоаппараты, платы захвата, видеокарты, устройства сопряжения. Написаны специальные программы управления камерами и блоками управления микроскопами, библиотеки программ для анализа изображений. Для автоматизированной диагностики разработаны алгоритмы принятия решений и создано специальное программное обеспечение, позволяющее представить изображения в нужном формате и качестве. Адекватность работы автоматизированной системы диагностики была подтверждена экспертами на практике, а также аналитически [2]. Проведенный эксперимент по оценке ошибок в диагностике с применением комплекса Атлант показал, что с применением комплекса молодые врачи допускали ошибку в сложных случаях диагностики лишь в 5% случаев, в то время как при самостоятельно проводимой диагностике (без применения комплекса) ошибки в сложных случаях составили 25%.

Анализ многолетней эксплуатации телемедицинской сети «Росатом-ФМБА-МИФИ», базирующейся на комплексах Атлант и функционирующей с 2000г. позволил выявить имеющиеся недостатки системы и принять меры по недопущению в будущем возникавших в ходе работы сбоев.

Важной характеристикой системы является вероятность отказа проведения сеанса для конкретного пользователя. Для оценки этой вероятности будем использовать широко применяемый экспоненциальный закон распределения времени безотказной работы. Поэтому для начала оценим интенсивность отказа для комплекса Атлант.

В качестве исходных данных для расчетов примем следующие: за весь период работы было проведено 2760 сеансов связи с пользователями, при этом три сеанса оказались несостоявшимися по следующим причинам:

- один из узлов сети пострадал от вирусной атаки (в настоящее время установлена соответствующая защита и подобные отказы отсутствуют);
- другой отказ был вызван механическими повреждениями кабельного разъема из-за неаккуратного обращения с оборудованием (вина пользователя);
- третий отказ произошел по причине нарушения контакта в плате управления.

Так как в результате проведенных усовершенствований в сети причина первого вида сбоя устранена, будем считать, что для сети, соответствующей современному состоянию, за время эксплуатации произошло два фактически значимых сбоя. Ввиду независимости работоспособности отдельных узлов в сети по имеющимся данным (результатам эксплуатации) можно дать оценку интенсивности отказов комплекса Атлант для отдельного пользователя:

- проводилось $N=2760$ испытаний сеансов связи (время одного испытания $T = 1$ час);
- два сеанса ($n=2$) оказались неудачными.

В условиях экспоненциального закона распределения времени отказов оценка $\hat{\lambda}$ параметра λ получается методом максимального правдоподобия [3]:

$$\hat{\lambda} = \frac{n}{\sum_{i=1}^n t_i + (N - n)T},$$

где t_i – наблюдаемые в эксперименте времена отказов, $i = 1, 2, \dots, n$,

N – объем выборки,

T – продолжительность испытаний.

В нашем случае численное значение интенсивности отказов λ_0 , полученное по опытным данным, равно $\lambda_0 = 0,0007$ (1/час).

Вероятность отказа P системы при данном значении λ за 1 час будет равна:

$$P_T = 1 - \exp[-\lambda T] < 1 - \exp[-0,7 * 10^{-3}] \approx 0,0007.$$

Для построения верхней доверительной границы параметра λ учтем, что число n появляющихся отказов в работе системы распределено согласно биномиальному закону, который хорошо аппроксимируется законом Пуассона с параметром $\mu = NP$. Для величины μ верхняя доверительная граница μ_B определяется из уравнения [4]:

$$\sum_{k=1}^n \frac{\mu_B^k}{k!} \exp\{-\mu_B\} = \alpha,$$

где α – уровень значимости.

Данная граница вычислена и равна $\mu_B = 5,3$ при уровне значимости $\alpha = 0,1$ и числе отказов $n = 2$. Это значение μ_B соответствует случайному событию, которое заключается в том, что это событие происходит при большом числе испытаний $N = 2760$ и его можно рассматривать как сумму мало-

вероятных независимых событий, закон распределения числа появления каждого из них также является законом Пуассона с параметром $\mu_1 = \lambda T$. Закон Пуассона является воспроизводящим [5] по параметру μ , поэтому $\mu = N\mu_1$. Поскольку между величинами μ_1 и μ имеется взаимно однозначное соответствие $\mu_1 = f(\mu) = \frac{\mu}{N}$, то верхняя доверительная граница μ_{1B} для параметра μ_1 равна

$$\mu_{1B} = f(\mu_B) = \frac{\mu_B}{N} \approx 2 \cdot 10^{-3} \text{ и } \lambda_{1B} = 2 \cdot 10^{-3} \text{ (1/час.)}$$

Важно отметить, что сбои со стороны центра управления телемедицинской сетью «Росатом-ФМБА-МИФИ», находящегося на кафедре «Компьютерные медицинские системы» НИЯУ МИФИ за весь период десятилетней эксплуатации не наблюдались. Поэтому повышение надежности работы комплексов Атлант возможно за счет предупреждения отказов оборудования пользователей.

Литература

1. **Никитаев В.Г., Проничев А.Н., Бердникович Е.Ю., Чистов К.С.** Стратегия построения высокотехнологичных комплексов компьютерной микроскопии: опыт разработки и внедрения в атомную промышленность и медицину. Приборы и системы. Управление, контроль, диагностика. № 10, 2011, с. 1-4.
2. **Власов В.А., Никитаев В.Г., Проничев А.Н., Чистов К.С.** Построение статистических тестов для испытания автоматизированных медицинских систем анализа микроскопических изображений. Приборы и системы управления, контроль, диагностика. – № 4. – 2008.
3. **Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д.** Математические методы в теории надежности. М.: Наука, 1964.
4. **Власов В.А.** Оценки и доверительные интервалы. М.: МИФИ, 2006.
5. **Рао С.** Линейные статистические методы и их применение. «НАУКА». Главная редакция физико-математической литературы. Москва 1968.

Nikitaev V.G., Pronichev A.N., Vlasov V.A., Vlasova S.V.

QUALITY ASSURANCE AND RELIABILITY ANALYSIS OF INFORMATION MEASURING SYSTEMS EXEMPLIFIED BY THE SYSTEM ATLANT

The paper presents description of the developed measures for improving the quality of the system Atlant and reliability of its operation.

Keywords: *reliability, failure rate, decision support, quality of cancer diagnosis.*

Telemedicine network “Rosatom-FMBA-MIFI” with the control center at the department of Computer Medical Systems of the National Research Nuclear University at Moscow Engineering and Physical Institute (NRNU MIFI) has been created to solve the problems of improving the quality of cancer diagnostics. The telemedicine network is based on high-technology systems of the cancer diagnostics Atlant, and it integrates multiple consumers in Russia, such as medical care units (MCU), academic centers and clinical hospitals [1]. The diagnostic network includes: NRNU MIFI, Blokhin Cancer Research Center of RAMN, CMSU # 141 (Udomlya, Kalinin NPP), MCU # 135 (Desnogorsk, Smolensk NPP), MCU # 125 (Kurchatov, Kursk NPP), MCU # 118 (Poliarny zory, Kolskaya NPP), MCU # 33 (Novovoronezh, Novovoronezh NPP) CMSU # 38 (Sosnovy Bor, Leningrad NPP), Saratov Medical Center FMBA (Balakovo, Balakovo NPP). Further expansion of the telemedicine network throughout Russia by introduction of new server capacities and porting additional users to the network is scheduled.

The system Atlant is an important tool for the implementation of technology to support medical decision-making based on expert systems and remote consulting, as well as on timely and operational support of medical staff by necessary data, which may be requested, for example, during surgical operation. Unique reference knowledge base containing color images of tumor samples in various organs and the corresponding standardized descriptions has been formed within the system frame with the participation of specialists of Blokhin Russian Cancer Center of RAMN, Clinical Hospitals # 83 and # 85, and others.

Expert systems are based on a database, which is stored on servers in the control center of telemedicine network. In addition, each medical institution has its own copy of the database. This is because a direct access to the base greatly increases the load on the network and, therefore, reduces data communication equipment speed. Addressing of customers to consultation archive should be carried out with minimum time and minimal load on the network. Therefore, the format of digitized images (number of digits, resolution, compression, etc.) is defined by a required picture quality, sufficient for reliable diagnostics. Redundancy of transmitted data affects the transmission rate and the time spent on consultation. Particularly acute this

problem is in rapid diagnostics during operations when the surgeon is waiting for a medical diagnostician answer to determine the volume and approach of surgical intervention.

The initial source for building the knowledge base was the numerous clinical cases described in detail by highly qualified doctors (experts), and that allows ordinary doctors working with the system Atlant to rely on the country's leading experts in making important diagnostic decisions.

The system includes support for making medical decisions during histological diagnostics, built on the basis of automated image processing systems, which provides invaluable help in the diagnosis formulation. The diagnostic system Atlant, which implemented a computer model of the macro and microanalysis, the technology of rapid transmission of requested data and remote consulting, has been successfully used for more than 10 years in clinical practice.

The strict requirements of quality and reliability are made for vital systems, where the system Atlant belongs to. Implementation of these requirements is insured by selection of suitable hardware-software tools and system architecture, applied communication protocols. Among hazardous factors unfavorably affecting the efficiency of the system are notably the threats associated with the loss or corruption of transmitted data, which requires a number of additional measures to improve data reliability.

The World Wide Web is used as the data transmission medium in the system Atlant. The medium has a number of drawbacks, such as dependence on the provider, a possible decrease in the rate of data transmission during network congestion, illegal access, etc. The latter issue is extremely relevant now. The problem of reliability of received information arises in case of fully open data exchange. Online medical information must be protected. For this reason, it became necessary to use special methods for the protection of medical data. The developed software product allows solving the following tasks:

- verification and authentication of the source of messages;
- confidentiality and integrity of data (i.e. assurance against unauthorized change of information);
- authentication (notarization of the parties).

The system Atlant provides online remote medical consultations in real time and with proper quality of communication; therefore, it must have a high level of fault tolerance and the ability to quickly recover after failures. We shall consider any events leading to the impossibility of image transmission, and partial or total loss of communication as a system failure. It can be failures of hardware that ensures the registration of optical images, generation of digital data and its processing, failures in data transmission channels, etc. These failures in medical operational practices are unacceptable.

Therefore, to improve the reliability, the developers of the system under consideration have used special software for monitoring the network, which affords an opportunity of remote analysis of faults and rapid response. The practice of telemedicine network operation "Rosatom-FMBA-MIFI" has shown that the network nodes that are remote from the control centre often have limited capacity of Internet-channels. In some cases, the transmission rate of channels does not exceed 256 Kb/s and can drop even lower. The objective of software for monitoring is the online tracing of the network state and fault detection (for example, problems caused by overloaded and/or failed servers, other devices or network connections, occasional connection loss, reduced network performance, long boot of servers, etc.). The monitoring software is an effective tool for managing a computer network, and it performs a number of important functions, including:

- control and monitoring of network resources;
- allocation of memory required to execute computing tasks;
- network configuration management;
- fault diagnostics.

The introduction of the computer system for decision support in the analysis and formulation diagnosis inevitably raises the accuracy issue of decisions recommended by automated diagnostic systems. Since the correct description of a microscopic sample largely depends on the quality of a digital image, special attention has been paid to the development of color calibration in the system to minimize errors in the automated issuance of expert information. For this purpose, medical staff together with technicians have selected special equipment, which includes microscopes, microscope control units, cameras, capture cards, video cards, interface devices. Software libraries for image analysis and special programs have been developed to control cameras and control units of microscopes. Algorithms of decision-making for automated diagnostics have been developed and special software created to provide images in the correct format and quality. Experts in practice as well as analytically [2] have confirmed the adequacy of the automated diagnostics system. They experiment carried out to assess errors in diagnostics using the system Atlant showed that by applying the system young doctors erred in only 5% of difficult diagnostic cases, while in self-reliant diagnostics (without using the system) errors in complex cases made up 25 %.

The analysis of long-term operation of telemedicine network “Rosatom-FMBA-MIFI”, which is based on Atlant systems and has been functioning since 2000, has allowed to reveal the shortcomings of the system and to take action to prevent failures in the future, which have occurred during the system operation.

An important feature of the system is the probability of failure during specific user session. To estimate this probability, we will use the widely applied exponential law of distribution of uptime. Therefore, first, we shall estimate the failure rate of the system Atlant.

We shall take the following as initial data for the calculations: 2760 communication sessions with users were conducted for the whole period of the system operation, with three sessions not held for the following reasons:

- one of the nodes of the network suffered from a virus attack (at present the appropriate securities have been installed and there is no of such failures);
- another failure was caused by mechanical damage of the cable connector due to the careless handling of equipment (user fault);
- the third failure occurred due to poor connection at the system controlling card.

Since, as a result of conducted improvements in the network, the cause of the first mode failure has been eliminated, we shall believe that in the network corresponding to the up-to-date state, there were two actually significant failures during the operation time. In view of operability independence of individual nodes in the network, the failure rate of the system Atlant for a single user can be estimated from the available data (results of operation):

- $N = 2760$ tests of communication sessions were conducted (one test time $T = 1$ hour);
- two sessions ($n = 2$) turned out to be failure.

Under conditions of an exponential law of distribution of failure time, the estimate $\hat{\lambda}$ of the parameter λ is obtained by the method of maximum likelihood [3]:

$$\hat{\lambda} = \frac{n}{\sum_{i=1}^n t_i + (N - n)T},$$

where t_i is failure times observed in the experiment, N is the sample size, T is the duration of tests.

In our case, the numerical value of failure rate λ_0 obtained from the experimental data is equal to $\lambda_0 = 0,0007$ (1/hr).

The probability of failure P of the system for a given value λ per one hour will be:

$$P_T = 1 - \exp[-\lambda T] < 1 - \exp[-0,7 * 10^{-3}] \approx 0,0007.$$

For the construction of the upper confidence limit on the parameter λ , we shall take into account that the number of failures n occurring in the system is distributed according to the binomial law, which is well approximated by the Poisson distribution with parameter $\mu = NP$. The upper confidence limit for the value μ is determined from the equation given in [4]:

$$\sum_{k=1}^n \frac{\mu_B^k}{k!} \exp\{-\mu_B\} = \alpha,$$

where α is the level of significance.

This limit has been calculated and it is equal $\mu_B = 5.3$ with the level of significance $\alpha = 0.1$ and the number of failures $n = 2$. This value μ_B corresponds to a random event, which consists in the fact that this event occurs during a large number of tests $N=2760$, and it can be considered as the sum of independent low-probability events, the distribution law of each event quantity occurrence is also a Poisson distribution with parameter $\mu_1 = \lambda T$. Poisson law is a reproducing law [5] by the parameter μ , therefore $\mu = N\mu_1$. As between the quantities μ_1 and μ there is unambiguous correspondence, the upper confidence limit μ_{1B} for the parameter μ_1 is the following

$$\mu_{1B} = f(\mu_B) = \frac{\mu_B}{N} \approx 2 * 10^{-3} \text{ and } \lambda_{1B} = 2 * 10^{-3} \text{ (1/h)}.$$

It should be noted that failures of the telemedicine network control center “Rosatom-FMBA-MIFI” located at the Department of Computer Medical Systems NRNU MIFI were observed over the entire ten-year period of the system operation. Therefore, the reliability improvement of the system Atlant is possible through preventing failures of user equipment.

References

1. **Nikitayev V.G., Pronichev A.N., Berdnikovich E.U., Chistov K.S.** Strategy of constructing high-tech systems for computer microscopy: experience of development and implementation of such systems in the nuclear industry and medicine. Devices and systems. Management, monitoring and diagnostics. # 10, 2011, p. 1-4.
2. **Vlasov V.A., Nikitayev V.G., Pronichev A.N., Chistov K.S.** Statistical trials construction for testing automated medical systems of microscopic images analysis. Devices and systems of control, monitoring and diagnostics, # 4, 2008.
3. **Gnedenko B.V., Belyaev U.K., Solovyev A.D.** Mathematical methods and theory of reliability. Moscow: Nauka, 1964.
4. **Vlasov V.A.** Estimates and confidence intervals. Moscow Engineering and Physical Institute, 2006.
5. **Rao S.** Linear statistical methods and their application. “Science.” Chief editorial board of physical and mathematical literature. Moscow, 1968.

Ткачев О.А.

АНАЛИЗ НАДЕЖНОСТИ СЕТЕЙ, СОСТОЯЩИХ ИЗ ИДЕНТИЧНЫХ ЭЛЕМЕНТОВ

Предлагаются аналитические модели, которые позволяют получить выражения для определения показателей надежности сетей, состоящих из идентичных элементов. Для сетей, состоящих из восстанавливаемых элементов, в качестве показателей надежности рассматриваются: среднее время работы до отказа и среднее время восстановления в стационарном режиме работы. При оценке надежности сетей, состоящих из невосстанавливаемых элементов, таким показателем является среднее времени работы до отказа.

Ключевые слова: Показатели надежности сети, марковские процессы, среднее время работы до отказа, среднее время восстановления.

Введение

Многие современные технические системы имеют сетевую структуру. В качестве примера можно привести телекоммуникационные, энергетические и транспортные системы. При проектировании подобных систем большое внимание уделяют обеспечению высокого уровня надежности.

Надежность сети зависит от целого ряда факторов: надежности элементов, топологии, используемых алгоритмов управления. В данной работе предлагается методика оценки показателей надежности сети по ее топологии.

При анализе надежности сетей представляет значительный интерес определение значений показателей, характеризующих динамику изменения состояний сети. Для сетей, состоящих из восстанавливаемых элементов, такими показателями являются среднее время работы до отказа и среднее время восстановления в стационарном режиме работы. При оценке надежности сетей, состоящих из невосстанавливаемых элементов, таким показателем является среднее время работы до отказа.

Эти показатели надежности сети могут быть определены, если процесс изменения состояний сети представить в виде марковского процесса, состояния которого характеризуются числом отказавших элементов и состоянием сети.

Простейшим критерием работоспособности сети является связность. Сеть является связной, если между любой парой узлов имеется хотя бы один путь.

В рассматриваемых примерах в качестве критерия работоспособности будет использована связность сети, однако полученные выражения справедливы и при использовании других критериев работоспособности сети.

Модель надежности сети, состоящей из идентичных восстанавливаемых элементов

Сети относятся к классу систем со сложной структурой. Характерным свойством таких систем является то, что при определенном числе отказавших элементов система может находиться как в работоспособном состоянии, так и в состоянии отказа. Например, о сети, представленной на рис.1, нельзя точно сказать, будет ли она связной, если удалить два или три ребра.

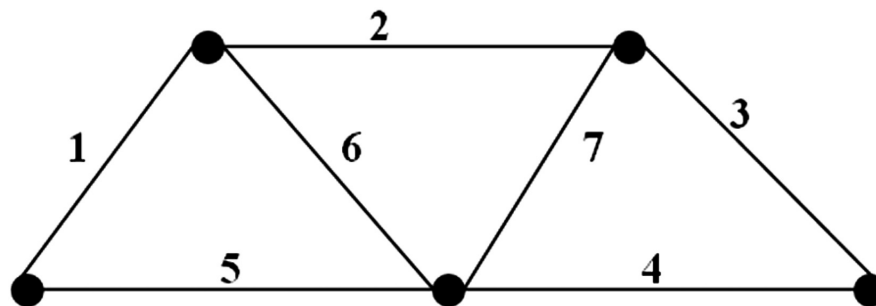


Рис.1. Пример сети

В качестве основного параметра, который позволит нам определить рассматриваемые показатели надежности сети, будем использовать число сечений мощности i . Обозначим этот параметр Y_i .

Определим значения Y_i для сети, представленной на рис. 1. Так как рассматриваемая сеть двух-связная, то удаление одного ребра не может нарушить ее связность, следовательно, $Y_1 = 0$. Для определения значений Y_2 и Y_3 рассмотрим все возможные состояния сети при удалении 2 и 3 ребер соответственно.

В результате анализа сети представленной на рис. 1 можно определить, что в рассматриваемой сети имеется 2 сечения мощности 2 и 14 сечений мощности 3, следовательно, $Y_2 = 2$, $Y_3 = 14$. Любая комбинация из i ребер при $i > 3$ будет являться сечением.

Зная значения Y_i можно определить значения вероятности того, что при отказе i ребер окажется несвязной. Обозначим этот показатель Z_i .

Значение Z_i равно отношению Y_i к общему числу возможных комбинаций i элементов из n , где n — число ребер в сети

$$Z_i = \frac{Y_i}{\binom{n}{i}}. \quad (1)$$

Рассмотрим марковский процесс, описывающий изменение состояний сети при отказе и восстановлении ее ребер. Каждое состояние процесса характеризуется определенной комбинацией отказавших ребер и состоянием сети (связна, несвязна).

Обозначим (i') связные состояния, и (i'') несвязные состояния сети при i отказавших ребрах.

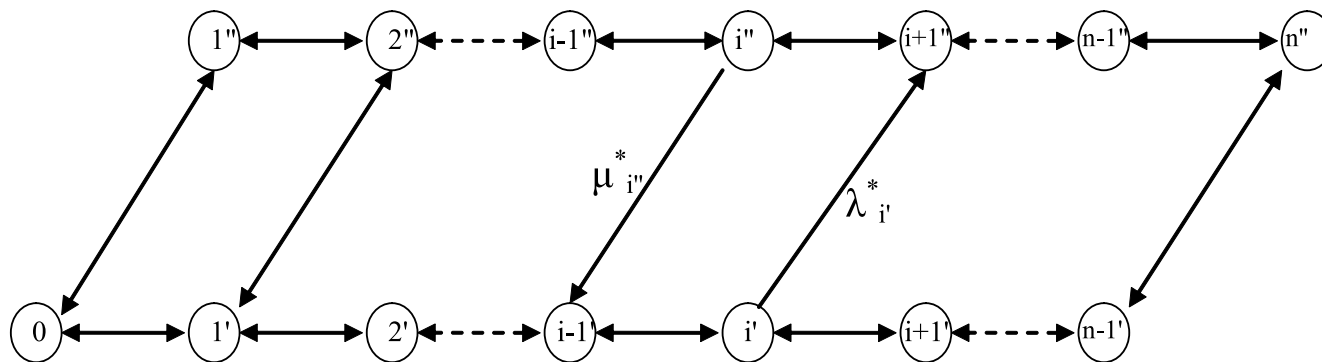


Рис. 2. Марковский процесс изменения состояний сети

Обозначим E_+ множество связанных состояний сети, E_- множество несвязных состояний сети.

В [1] показано, что среднее время пребывания марковского процесса на множестве состояний E_+ до первого перехода в одно из состояний множества E_- может быть определено из выражения (2).

$$T_{E_+} = \frac{\sum_{i=0}^n P_{i'}}{\sum_{i=0}^n P_{i'} \lambda_{i'}^*}. \quad (2)$$

Среднее время пребывания процесса на множестве несвязных состояний E_- до первого перехода в одно из состояний множества E_+ может быть определено из выражения (3).

$$T_{E_-} = \frac{\sum_{i=0}^n P_{i''}}{\sum_{i=0}^n P_{i''} \mu_{i''}^*}, \quad (3)$$

где $P_{i'}$, $P_{i''}$ — вероятности состояний;

$\lambda_{i'}^*$ — интенсивность перехода из состояния (i') в состояние $(i+1)''$;

$\mu_{i''}^*$ — интенсивность перехода из состояния (i'') в состояние $(i-1)'$.

Суммарная интенсивность отказов ребер в состоянии i равна $(n-i)\lambda$, суммарная интенсивность восстановлений — $i\mu$; следовательно

$$\lambda_{i'}^* = (n-i)\lambda Z_i^* \quad (4)$$

$$\mu_{i''}^* = i\mu Z_{i''}^{**}, \quad (5)$$

где Z_i^* — вероятность того, что при отказе одного ребра сеть из связанного состояния (i') перейдет в несвязное состояние $(i+1)''$;

$Z_{i''}^{**}$ — вероятность того, что при восстановлении одного ребра сеть из несвязного состояния (i'') перейдет в связанное состояние $(i-1)'$.

Взаимосвязь значений Z_i^* , Z_i^{**} и Z_i была установлена в работе [2].

Значения Z_i^* и Z_i^{**} могут быть определены из выражений (6) и (7) соответственно

$$Z_i^* = \frac{Z_{i+1} - Z_i}{1 - Z_i} \quad (6)$$

$$Z_i^{**} = \frac{Z_{i-1}}{Z_i}. \quad (7)$$

Подставив значения λ_i^* и μ_i^* из выражений (4) и (5) в выражения (2) и (3) соответственно, получим:

$$T_{E_+} = \frac{\sum_{i=0}^n P_i}{\lambda \sum_{i=0}^n P_i (n-i) Z_i^*} \quad (8)$$

$$T_{E_-} = \frac{\sum_{i=0}^n P_i}{\mu \sum_{i=0}^n i P_i (1 - Z_i^{**})}. \quad (9)$$

Значения P_i , P_i^* могут быть определены следующим образом.

Так как все ребра идентичны по надежности, то все состояния с i отказавшими ребрами равновероятны. Вероятность того, что в сети в состоянии отказа будет находиться i ребер, равна

$$P_i = \frac{(\lambda / \mu)^i \binom{n}{i}}{(1 + \lambda / \mu)^n} \quad (10)$$

из определения Z_i следует:

$$P_i = (1 - Z_i) P_i \quad (11)$$

$$P_i^* = Z_i P_i. \quad (12)$$

Вероятность пребывания сети в связном состоянии в произвольный момент времени:

$$R = \sum_{i=0}^n P_i. \quad (13)$$

Значение R может быть так же определено из выражения:

$$R = \frac{T_{E_+}}{T_{E_+} + T_{E_-}} \quad (14)$$

Таблица 1. Значения $Y_i, Z_i, Z_i^*, Z_i^{}$ для сети на рис. 1**

i		Y_i	Z_i	Z_i^*	Z_i^{**}
0	1	0	0	0	0
1	7	0	0	0,095238	0
2	1	2	0,095238	0,336842	0
3	5	4	0,4	1	0,238095
4	5	5	1	0	0,4
5	1	1	1	0	1
6	7	7	1	0	1
7	1	1	1	0	1

Подставляя значения $Y_i, Z_i, Z_i^*, Z_i^{**}$ из табл.1 в выражения (8), (9), (14) при $\lambda=0,1$ (1/час) и $\mu=1$ (1/час) получим следующие значения рассматриваемых показателей надежности.

$$T_{E_+} = 23,769 \text{ час.}$$

$$T_{E_-} = 0,469 \text{ час.}$$

$$R = 0,980645$$

Приближенные оценки показателей надежности

Исследуя пределы полученных выражений при $\lambda/\mu \rightarrow 0$, [3], можно получить приближенные оценки рассматриваемых показателей надежности

$$T_{E_+} = \frac{1}{\lambda(\lambda/\mu)^{s-1} * S * Y_s} \quad (15)$$

$$T_{E_-} = \frac{1}{s * \mu}. \quad (16)$$

Для сети на рис. 1 $s=2, Y_s=2$

Подставляя эти значения в выражения 14,15,16 при $\lambda=0,1$ (1/час) и $\mu=1$ (1/час) получим

$$T_{E_+} = 25 \text{ час.}$$

$$T_{E_-} = 0,5 \text{ час.}$$

$$R = 0,980392$$

Сравнение с известными результатами

В целях проверки полученных выражений определим значения рассматриваемых показателей надежности системы на рис. 3, для которой известны аналитические оценки.

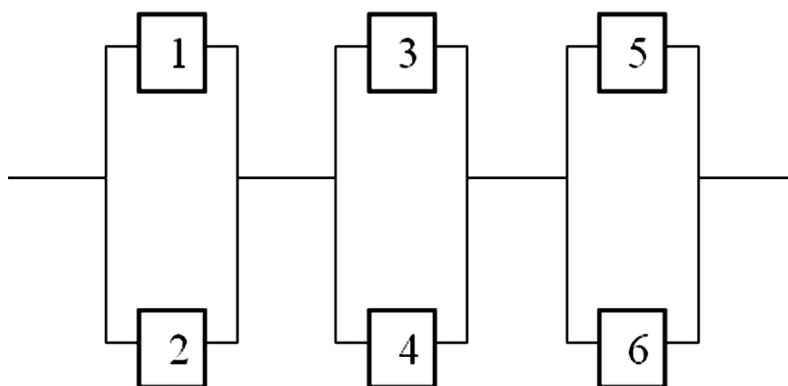


Рис. 3. Последовательно–параллельная система

В [4] можно найти следующие выражения.

Для s параллельно соединенных идентичных элементов с параметрами λ, μ

$$t_{E_+} = \frac{1}{s * \mu} \left[\left(1 + \frac{\mu}{\lambda} \right)^s - 1 \right]$$

$$t_{E_-} = \frac{1}{s * \mu}$$

$$r = \frac{t_{E_+}}{t_{E_+} + t_{E_-}}.$$

Для k одинаковых, последовательно соединенных восстанавливаемых подсистем

$$T_{E_+} = \frac{1}{k * (1/t_{E_+})}$$

$$R = r^k$$

$$T_{E_-} = T_{E_+} \frac{1-R}{R}.$$

Подставляя в эти выражения $s=2, k=3, \lambda=0,1(1/\text{час.}), \mu=1(1/\text{час.})$, получим

$$T_{E_+} = 20,000 \text{ час.}$$

$$R = 0,975411$$

$$T_{E_-} = 0,504 \text{ час.}$$

Для определения этих показателей надежности с использованием выражений (8), (9), (14), необходимо определить значения Y_i и Z_i .

Очевидно, что $Y_1=0$ и $Z_1=0,0$. При отказе 2 элементов существуют три комбинации, приводящие к несвязности (неработоспособности) системы (1,2), (3,4), (5,6). Всего возможных комбинаций 15, следовательно, $Y_2=3$ и $Z_2=3/15$. Для определения Y_3 и Z_3 , рассмотрим все возможные комбинации из 3 элементов, табл. 2. Из результатов, приведенных в табл.1 следует, что $Y_3=12$ и $Z_3=12/20$. При отказе 4 и более элементов система будет несвязна, следовательно, $Z_4 = Z_5 = Z_6=1$

Таблица 2. Состояния системы на рис. 3 при отказе 3 элементов

1	23	-	1	34	-
2	24	-	2	35	+
3	25	-	3	36	+
4	26	-	4	45	+
5	34	-	5	46	+
6	35	+	6	56	-
7	36	+	7	45	-
8	45	+	8	46	-
9	46	+	9	56	-
0	56	-	0	56	-

Таблица 3. Результаты расчета характеристик системы на рис. 3

i		P_i	Y_i	Z_i	$*_i$	Z^{**}_i	Q_i	R_i
0	1	0,5644739301	0	0	0	0	0,0000000000	0,5644739301
1	6	0,3386843580	0	0	0,2	0	0,0000000000	0,3386843580
2	15	0,0846710895	3	0,2	0,5	0	0,0169342179	0,0677368716
3	20	0,0112894786	12	0,6	1	0,33333	0,0067736872	0,0045157914
4	15	0,0008467109	15	1	0	0,6	0,0008467109	0,0000000000
5	6	0,0000338684	6	1	0	1	0,0000338684	0,0000000000
6	1	0,0000005645	1	1	0	1	0,0000005645	0,0000000000

Результаты остальных расчетов приведены в табл. 3. Подставляя данные из табл. 3 в выражения (26), (27), (37), получим:

$$T_{E_+} = 20,000 \text{ час.}$$

$$R = 0,975411$$

$$T_{E_-} = 0,504 \text{ час.}$$

Пример анализа надежности сети состоящей из идентичных восстанавливаемых элементов.

Обозначим m число узлов, n – число ребер. Следует обратить внимание на то, что для каждой пары значений n, m существует топология, обеспечивающая максимальный уровень надежности.

Для определения таких топологий были использованы алгоритмы, предложенные Г.Т. Артамоновым в работе [5].

Сеть с параметрами $m=20$, $n=24$.

Для достижения максимальной надежности нужно найти сеть минимального диаметра с количеством узлов $2*(n-m)$ имеющих степень 3, и равномерно распределить узлы степени 2 по ребрам этой сети. В результате будет получена сеть, представленная на рис. 4. Значения Y_i этой сети могут быть определены путем полного перебора всех возможных состояний. Результаты расчетов представлены в табл. 4а и табл. 4б.

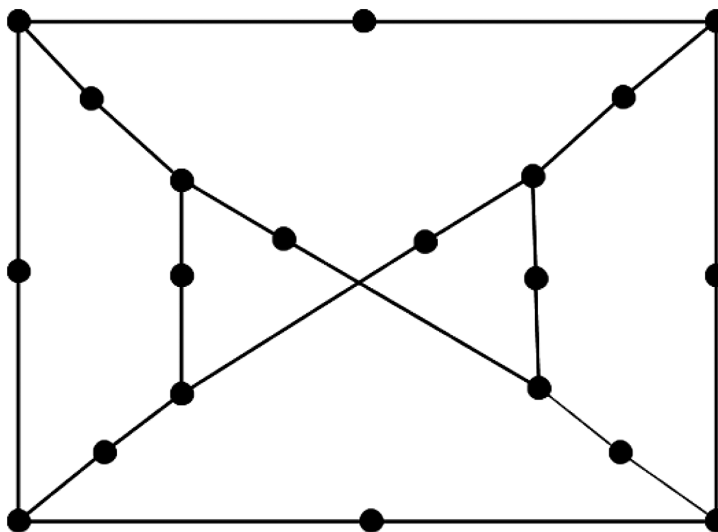


Рис. 4. Сеть с параметрами $m=20$, $n=24$

Таблица 4а. Значения Y_i и Z_i для сети на рис. 4

i	1	2	3	4	5	$i \geq 6$
Y_i	0	12	328	4082	29960	
Z_i	0	0,043478	0,162055	0,384252	0,704875	1

Таблица 4б. Значения T_{E+} , T_{E-} , R сети на рис. 4

λ	T_{E+}	T_{E-}	R
0,1	2,13	0,3334	0,864576
0,01	390,86	0,4845	0,998762
0,001	41415,64	0,4986	0,999988

Использование других критериев работоспособности и моделей надежности сети

До данного момента мы использовали в качестве критерия работоспособности связность всех узлов сети. Однако уместно задать вопрос: является ли отказом потеря связи с одним из узлов? Если мы считаем допустимой потерю связности с h -узлами, то можно использовать следующий

критерий работоспособности сети: сеть считается работоспособной, если число связных узлов $\geq m-h$. Данный критерий работоспособности сети рассматривался в работе [6].

Полученные результаты можно использовать и в этом случае, только необходимо внести соответствующие изменения в алгоритм определения значений Y_i . В табл. 5 приведены значения T_{E+} и R , при различных значениях h , для сети представленной на рис. 4.

Таблица 5. Значения T_{E+} , R при различных значениях h для сети на рис.4 ($\lambda=0,01$; $\mu=1$)

h	T_{E+}	R
1	5780,49	0,999943591
2	9843,50	0,999967012
3	31455,53	0,999990157

Можно ослабить ограничение на равнонадежность ребер. Каждое ребро можно представить в виде последовательного соединения определенного количества равнонадежных элементов. При этом в структуру сети вводятся фиктивные узлы. После таких преобразований определяются значения Z_i . Если отказал один из элементов, составляющих ребро, то это ребро удаляется из сети. Связность сети проверяется без учета фиктивных узлов.

Следует обратить внимание на то, что полученные результаты можно использовать в том случае, когда отказывают узлы, а ребра абсолютно надежны. Отказ узла можно промоделировать удалением всех ребер, исходящих из этого узла.

Данный метод анализа надежности сетей можно использовать и в тех случаях, когда работоспособными считаются только те состояния, при которых величина определенных параметров сети, например, время передачи или пропускная способность, будут удовлетворять заданным значениям.

Для сетей большой размерности статистическую оценку значений Z_i можно определить, используя метод Монте-Карло. Генерируется случайная комбинация из i отказавших элементов, после этого проверяется работоспособность сети. Отношение количества испытаний, при которых сеть окажется неработоспособной, к общему числу испытаний будет являться статистической оценкой Z_i .

Однако следует учитывать то, что для достижения высокой точности статистической оценки Z_i , количество испытаний должно быть достаточно велико (10^5 - 10^6).

Модель надежности сети состоящей из идентичных невосстанавливаемых элементов

Будем предполагать, что узлы сети абсолютно надежны, а ребра идентичны по надежности, отказывают независимо друг от друга и имеют экспоненциальное распределение времени работы до отказа.

Рассмотрим цепь Маркова, описывающую изменение состояний сети в моменты отказа ее элементов.

Если при наличии $i-1$ отказавших элементов сеть была работоспособна, то при отказе i -го элемента она с вероятностью Z_i^* переходит в неработоспособное состояние, или с вероятностью $1-Z_i^*$ останется в работоспособном состоянии.

Если при наличии $i-1$ отказавших элементов сеть была неработоспособна, то при отказе i -го элемента она с вероятностью 1 останется в неработоспособном состоянии.

Диаграмма переходов рассматриваемого процесса показана на рис. 5. Состояния i' соответствуют работоспособным состояниям сети, а состояния i'' соответствуют неработоспособным состояниям сети при отказе i элементов.

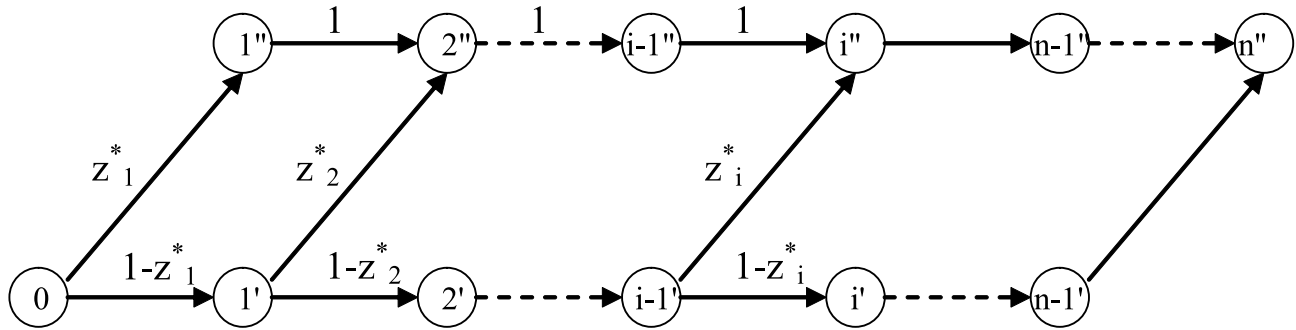


Рис. 5. Диаграмма изменения состояний сети

Введем обозначения $Q_{i'}$ – вероятность работоспособного состояния, а $Q_{i''}$ – вероятность неработоспособного состояния сети при отказе i элементов. Из определения Z_i следует

$$Q_{i'} = 1 - Z_i \quad (17)$$

$$Q_{i''} = Z_i. \quad (18)$$

В соответствии с диаграммой изменения состояний сети на рис. 5 можно записать

$$Q_{i'} = Q_{(i-1)'} (1 - Z_i^*) \quad (19)$$

откуда

$$Z_i^* = \frac{Q_{(i-1)'} - Q_{i'}}{Q_{(i-1)'}}. \quad (20)$$

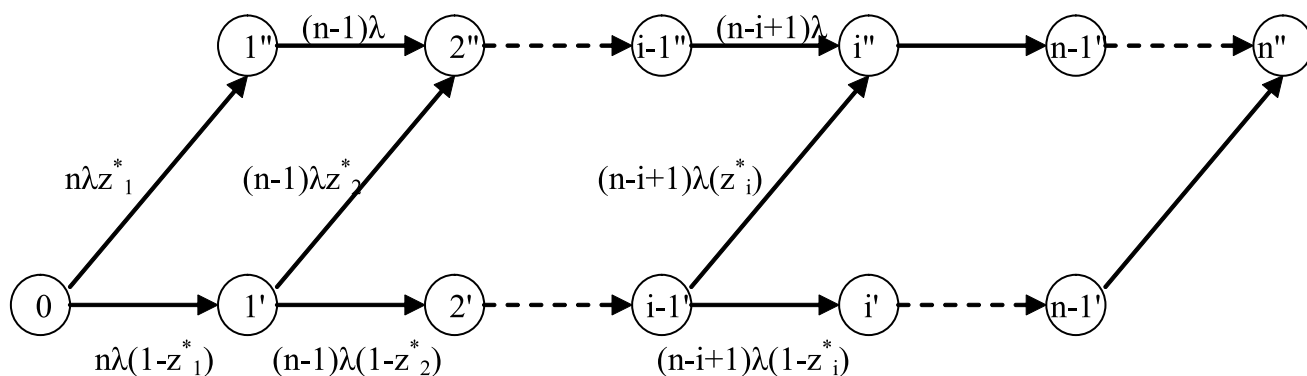
Подставляя в (20) значения $Q_{i'}$ и $Q_{i''}$ из (17) и (18), получим

$$Z_i^* = \frac{Z_i - Z_{i-1}}{1 - Z_{i-1}}. \quad (21)$$

Кроме того, из выражения (19) следует

$$Q_{i'} = \prod_{j=1}^i (1 - Z_j^*) = 1 - Z_i. \quad (22)$$

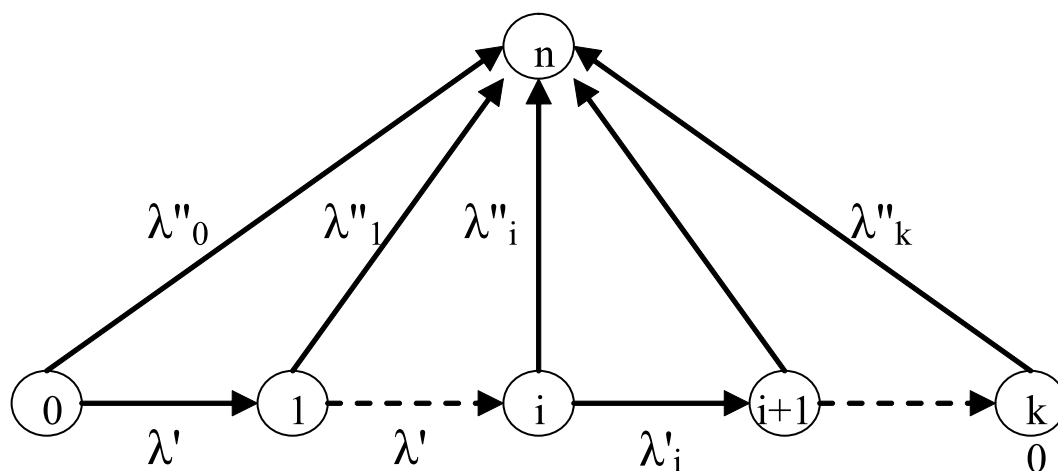
Для определения среднего времени работы до отказа рассмотрим непрерывный марковский процесс, описывающий поведение системы во времени. Состояния процесса задаются числом отказавших элементов и состоянием сети [7]. Диаграмма изменений состояний этого процесса показана на рис. 6.



Обозначим интенсивность отказов элементов λ . Пусть в некоторый момент времени имеется i отказавших элементов и сеть при этом работоспособна. За бесконечно малый промежуток времени Δt может произойти одно из следующих событий:

- Сеть останется в работоспособном состоянии. Вероятность этого события $(1-(n-i)\lambda \Delta t)$;
- Откажет еще один элемент и сеть перейдет в неработоспособное состояние. Вероятность этого события $(1-(n-i)\lambda Z_{i+1}^* \Delta t)$;
- Откажет еще один элемент, но сеть останется в работоспособном состоянии. Вероятность этого события $(1-(n-i)\lambda (1-Z_{i+1}^*) \Delta t)$.

В целях упрощения аналитических выкладок множество неработоспособных состояний заменим одним поглощающим состоянием (рис. 7).



Вероятности пребывания процесса в различных состояниях в произвольный момент времени $P_i(t)$ могут быть найдены путем решения следующей системы дифференциальных уравнений:

$$\frac{\partial P_0(t)}{\partial t} = -\lambda_0' P_0(t) - \lambda_0'' P_0(t) = -\lambda_0 P_0(t)$$

$$\frac{\partial P_i(t)}{\partial t} = \lambda'_{i-1} P_{i-1}(t) - \lambda'_i P_i(t) - \lambda''_i P_i(t) = \lambda'_{i-1} P_{i-1}(t) - \lambda_i P_i(t) \quad (23)$$

$$\frac{\partial P_n(t)}{\partial t} = \sum_{i=0}^k \lambda_i'' P_i(t)$$

Здесь

$$\lambda_i = (n-i)\lambda$$

$$\lambda_i' = (1 - Z_{i+1}^*) \lambda_i$$

$$\lambda_i'' = Z_{i+1}^* \lambda_i$$

k – максимальное число элементов, после отказа которых сеть может быть работоспособна.

Решим систему дифференциальных уравнений (23), используя преобразование Лапласа, при начальных условиях $P_0(0)=1$, $P_i(0)=0 \quad \forall i \neq 0$.

Введем обозначение

$$F(s) = \int_0^{\infty} P(t) e^{-st} dt$$

Тогда система дифференциальных уравнений (23) приводится к системе алгебраических уравнений относительно $F(s)$.

$$sF_0(s) = 1 - \lambda_0 F_0(s)$$

$$sF_i(s) = \lambda_{i-1}' F_{i-1}(s) - \lambda_i F_i(s) \quad (24)$$

$$sF_n(s) = \sum_{i=0}^k \lambda_i'' F_i(s)$$

Откуда имеем

$$F_0(s) = \frac{1}{s + \lambda_0}$$

$$F_i(s) = \frac{\lambda_{i-1}'}{s + \lambda_i} F_{i-1}(s) \quad (25)$$

$$F_n(s) = \frac{1}{s} \sum_{i=0}^k \lambda_i'' F_i(s).$$

Это решение позволяет получить выражение для среднего времени работы до отказа

$$T = \sum_{i=0}^k F_i(s) \Big|_{s=0}. \quad (26)$$

Раскрывая (25), получим

$$F_0(0) = \frac{1}{\lambda_0} = \frac{1}{n\lambda} \quad (27)$$

$$F_i(0) = \frac{\lambda'_{i-1}}{\lambda_i} F_{i-1}(0) = \frac{\prod_{j=1}^i (1 - Z_j^*)}{(n-i)\lambda}. \quad (28)$$

Используя (22), выражение (28) можно упростить

$$F_i(0) = \frac{\prod_{j=1}^i (1 - Z_j^*)}{(n-i)\lambda} = \frac{1 - Z_i}{(n-i)\lambda}. \quad (29)$$

Тогда из (26) следует

$$T = \frac{1}{\lambda} \sum_{i=0}^k \frac{(1 - Z_i)}{n-i}. \quad (30)$$

Выражение (30) позволяет определить значение среднего времени работы до отказа по известным значениям Z_i и λ .

Определим значение T для сети, представленной на рис. 1 при $\lambda=0,01$ (1/час)

$$T = 100 \left(\frac{1}{7} + \frac{1}{6} + \left(\frac{19}{21} \right) \frac{1}{5} + \left(\frac{21}{35} \right) \frac{1}{4} \right) = 100 * \frac{269}{420} \approx 64,047 (\text{час.})$$

Сравнение с известными результатами

В целях проверки полученного выражения определим среднее время работы до отказа системы, для которой известны аналитические оценки (рис. 3).

В [4] можно найти следующие выражения.

Вероятность безотказной работы системы из 2-х параллельно соединенных идентичных элементов

$$P_{(t)} = 1 - (1 - e^{-\lambda t})^2 = 2e^{-\lambda t} - e^{-2\lambda t}.$$

Вероятность безотказной работы системы состоящей из 3-х одинаковых, последовательно соединенных подсистем

$$P_{\bar{n}(t)} = (P_{(t)})^3$$

$$P_{\bar{n}(t)} = (2e^{-\lambda t} - e^{-2\lambda t})^3 = 8e^{-3\lambda t} - 12e^{-4\lambda t} + 6e^{-5\lambda t} - e^{-6\lambda t}.$$

Среднее время работы системы до отказа равно

$$T = \int_0^{\infty} P_{\bar{n}(t)} dt = \frac{1}{\lambda} \left(\frac{8}{3} - \frac{12}{4} + \frac{6}{5} - \frac{1}{6} \right) = \frac{1}{\lambda} \left(\frac{42}{60} \right) = 0,7 \frac{1}{\lambda}.$$

Для определения среднего времени до отказа с использованием выражения (30), необходимо определить значения и Z_i . Для рассматриваемой системы они равны: $Z_1=0,0$; $Z_2=3/15$; $Z_3=12/20$; $Z_4 = Z_5 = Z_6=1$.

Подставляя эти значения в выражение (30), получаем

$$T = \frac{1}{\lambda} \left(\frac{1}{6} + \frac{1}{5} + \left(\frac{12}{15} \right) \frac{1}{4} + \left(\frac{8}{20} \right) \frac{1}{3} \right) = \frac{1}{\lambda} \left(\frac{42}{60} \right) = 0,7 \frac{1}{\lambda}.$$

Данный пример также показывает, что предлагаемый метод можно использовать для определения среднего времени работы до отказа сложных последовательно-параллельных систем, состоящих из идентичных невосстанавливаемых элементов.

Пример анализа надежности сети состоящей из идентичных невосстанавливаемых элементов

Обозначим m – число узлов, n – число ребер. Рассмотрим сеть с параметрами $m=20$, $n=24$, (рис. 4). Значения Z_i этой сети могут быть определены путем полного перебора всех возможных состояний.

Предлагаемый метод можно использовать при других критериях работоспособности сети. Например, сеть считается работоспособной, если число связных узлов $\geq m-h$. Полученные результаты можно использовать и в этом случае, только необходимо внести соответствующие изменения в алгоритм определения значений Z_i . В табл. 6 приведены значения Z_i при различных значениях h для сети, представленной на рис. 4. Определение значений Z_i при $k>0$ осуществлялось методом Монте-Карло. Количество испытаний составляло 10^6 .

Таблица 6. Значения Z_i при различных значениях h для сети на рис. 4

i/h	0	2	4	6	8	10
1	0,0000000	0,00000	0,00000	0,00000	0,00000	0,00000
2	0,0434783	0,00000	0,00000	0,00000	0,00000	0,00000
3	0,1620553	0,01581	0,00000	0,00000	0,00000	0,00000
4	0,3841521	0,07980	0,01498	0,00435	0,00296	0,00000
5	0,7048748	0,25247	0,08813	0,03329	0,01644	0,00000
6	1,0000000	0,56194	0,27850	0,13070	0,05976	0,00324
7	1,0000000	0,86648	0,56942	0,33252	0,17912	0,04445
8	1,0000000	1,00000	0,82642	0,58123	0,36764	0,16783
9	1,0000000	1,00000	0,96544	0,79849	0,57894	0,34029

10	1,0000000	1,00000	1,00000	0,93211	0,76173	0,52593
11	1,0000000	1,00000	1,00000	0,98807	0,89262	0,69336
12	1,0000000	1,00000	1,00000	1,00000	0,96470	0,82566
13	1,0000000	1,00000	1,00000	1,00000	0,99360	0,91743
14	1,0000000	1,00000	1,00000	1,00000	1,00000	0,97046
15	1,0000000	1,00000	1,00000	1,00000	1,00000	0,99403
α	0,214850615	0,29501	0,354027	0,411813	0,476755	0,571528

$$\alpha = \sum_{i=0}^k \frac{(1-Z_i)}{n-i}$$

$$T = \alpha * \lambda$$

Заключение

Получены аналитические выражения для определения значений показателей надежности сетей, состоящих из идентичных элементов, которые имеют экспоненциальное распределение времени работы до отказа и времени восстановления. При этом можно считать абсолютно надежными как узлы, так и ребра сети. Достоверность полученного результата подтверждается путем расчета показателей надежности последовательно–параллельной системы, для которой известны аналитические оценки.

Литература

1. Вопросы математической теории надежности. Е.Ю. Барзилович, Ю.К. Беляев, В.А. Каштанов, И.Н. Коваленко, А.Д. Соловьев, И.А. Ушаков./Под ред. Б.В.Гнеденко, М., Радио и связь, 1983. -367стр. с илл.
2. **Ткачев О.А.** Использование цепей Маркова для анализа надежности систем со сложной структурой. Кибернетика, №5 1983, стр. 95-101.
3. **Ткачев О.А.** Анализ надежности сетей передачи данных. – Труды международной конференции «Распределенные компьютерные и телекоммуникационные сети: теория и приложения» (DCCN-2010) ISBN 978-5-9901871-2-2, Россия, Москва, 2010, стр.276-283.
4. Математические методы в теории надежности. Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. М.: Наука, 1965. – 524 стр. с илл.
5. Теория проектирования вычислительных машин, систем и сетей: Учебное пособие/В.И.Матов, Г.Т.Артамонов, О.М. Брехов и др.; Под ред. В.И.Матова. –М.: Изд-во МАИ, 1999. -460с.
6. **Tkachev O.** Analytical estimation of reliability of networks consisting of identical elements. Reliability – Theory & Application, ISSN 1932-2321, №2(21) 2011, p.9-20.
7. **Tkachev O.** Determination of mean time to failure of a network consisting of identical non-repairable elements. Reliability – Theory & Application, ISSN 1932-2321, №3(22) 2011, p. 43-46.

Tkachev O.A.

RELIABILITY ANALYSIS OF NETWORKS CONSISTING OF IDENTICAL ELEMENTS

The paper offers analytical models, which allows obtaining expressions for determining the reliability indices of networks consisting of identical elements. For networks consisting of recoverable elements, the mean time between failures and the mean time to repair in steady-state operation are considered as reliability indices. In assessing the reliability of networks of non-repairable elements, such an index is the mean time to failure.

Keywords: *reliability indices of networks, Markov processes, mean time to failure, mean time to repair.*

Introduction

Many modern engineering systems have a network structure. For example, telecommunications, energy and transportation systems have such a structure. In the design of similar systems, a lot of attention is paid to providing the high level of reliability.

The reliability of a network depends on several factors: the reliability of components, the topology and control algorithms used. This paper proposes a method of estimating the reliability indices of a network according to its topology.

In the analysis of networks reliability, determining the values of parameters describing the behavior of network states is of considerable interest. For networks consisting of recoverable elements, the mean time between failures and the mean time to repair in steady-state operation are considered as reliability indices. In assessing the reliability of networks of non-repairable elements, such an index is the mean time to failure.

These reliability indices of networks can be determined if the process of changing network states is represented in the form of Markov process, which states are described by the number of failed elements, and network states.

The simplest criterion of network operability is its connectivity. The network is connected if between any pair of nodes, there is at least one path.

Network connectivity will be used in considered examples as criterion of network operability, but the obtained expressions are valid when using other criteria of network operability.

Model of network reliability consisting of identical recoverable elements

Networks refer to the class of systems with a complex structure. A characteristic feature of such systems is that under a certain number of failed elements the system can be either in upstate or in failed state. For example, considering the network shown in Fig.1 we cannot say for sure whether it would be connected, if you remove two or three edges.

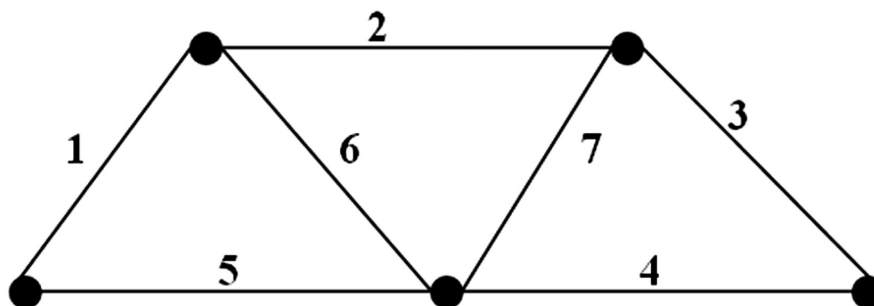


Fig. 1. Example of a network

We shall use the number of sections of power i as the main parameter that will allow us to determine the network reliability indices under consideration. We will denote this parameter as Y_i .

Let us determine the values of Y_i for the network shown in Fig. 1. Since the network under consideration is doubly connected, the removal of one edge cannot break its connectivity, therefore, $Y_1 = 0$. We shall consider all the possible states of the network after removing 2 and 3 edges respectively in order to determine the values of Y_2 and Y_3 .

As a result of the analysis of the network shown in Fig. 1, it is possible to determine that in this network there are two sections of power 2 and 14 sections of power 3, therefore, $Y_2 = 2$, $Y_3 = 14$. Any combination of i edges for $i > 3$ will be a section.

Knowing the values of Y_i , we can determine the values of the probability that with i edges failed, the network will turn out to be disconnected. We denote this index as Z_i .

The value of Z_i is equal to the ratio of Y_i to the total number of possible combinations of i elements out of n , where n is the number of edges in the network:

$$Z_i = \frac{Y_i}{\binom{n}{i}}. \quad (1)$$

Let us consider a Markov process, describing the change of network states in case of failure and restoration of its edges. Each state of the process is described by a particular combination of failed edges and the network status (connected and disconnected).

We denote the connected states and disconnected state of the network when i edges failed as (i') and (i'') respectively.

We shall denote a set of connected states of the network as E_+ , and a set of disconnected states of the network as E_- .

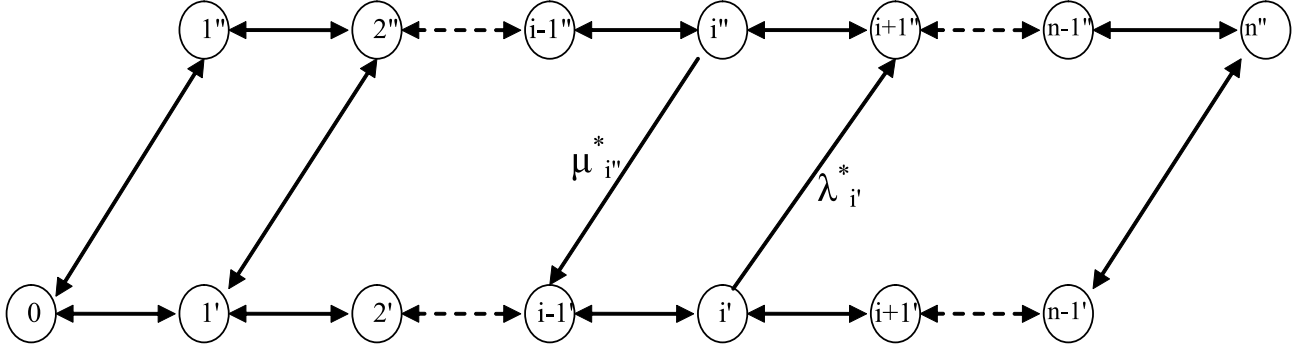


Fig. 2. Markov process of network states changes

In [1] it is shown that the mean stay time of a Markov process on the set of states E_+ to the first transition into one of the states of the set E_- can be determined from expression (2).

$$T_{E_+} = \frac{\sum_{i=0}^n P_i}{\sum_{i=0}^n P_i \lambda_{i'}^*} \quad (2)$$

The mean stay time of the process on the set of disconnected states E_- to the first transition into one of the states E_+ can be determined from expression (3).

$$T_{E_-} = \frac{\sum_{i=0}^n P_i}{\sum_{i=0}^n P_i \mu_{i''}^*}, \quad (3)$$

where P_i, P_i^* are the probabilities of states, and
 $\lambda_{i'}^*$ is the transition rate from the state (i') to the state $(i+1)''$;
 $\mu_{i''}^*$ is the transition rate from the state (i'') to the state $(i-1)'$.

The total failure rate of edges in the state i is equal to $(n-i) \lambda$, the total recovery rate is equal to $i \mu$; therefore:

$$\lambda_{i'}^* = (n-i) \lambda Z_i^* \quad (4)$$

$$\mu_{i''}^* = i \mu Z_{i'}^{**}, \quad (5)$$

where Z_i^* is the probability that at the failure of one edge the network will transit from a connected state (i') into a disconnected state $(i+1)''$;

$Z_{i'}^{**}$ is the probability that at the recovery of one edge the network will transit from a disconnected state (i'') into a connected state $(i-1)'$.

The relationship of values $Z_i^*, Z_{i'}^{**}$ and Z_i was established in the study [2].

The values Z_i^* and $Z_{i'}^{**}$ can be determined from expressions (6) and (7) respectively.

$$Z_i^* = \frac{Z_{i+1} - Z_i}{1 - Z_i} \quad (6)$$

$$Z_i^{**} = \frac{Z_{i-1}}{Z_i} \quad (7)$$

And by substituting the values λ_i^* and μ_i^* from expressions (4) and (5) into expressions (2) and (3) respectively, we will obtain the following:

$$T_{E_+} = \frac{\sum_{i=0}^n P_i}{\lambda \sum_{i=0}^n P_i (n-i) Z_i^*} \quad (8)$$

$$T_{E_-} = \frac{\sum_{i=0}^n P_i}{\mu \sum_{i=0}^n i P_i (1 - Z_i^{**})}. \quad (9)$$

The values of P_i , P_i^* may be determined as follows.

Since all edges are identical in terms of reliability, then all states with i failed edges are equiprobable. The probability that i edges will be in failure state in the network is equal

$$P_i = \frac{(\lambda / \mu)^i \binom{n}{i}}{(1 + \lambda / \mu)^n} \quad (10)$$

from the definition of Z_i we obtain the following:

$$P_i = (1 - Z_i) P_i \quad (11)$$

$$P_i^* = Z_i P_i. \quad (12)$$

The probability of the network stay in connected state at an arbitrary time point is the following:

$$R = \sum_{i=0}^n P_i. \quad (13)$$

The value of R may also be determined from the expression:

$$R = \frac{T_{E_+}}{T_{E_+} + T_{E_-}}. \quad (14)$$

Table 1. The values of $Y_i, Z_i, Z_i^*, Z_i^{**}$ for the network shown in Fig. 1

i		Y_i	Z_i	Z_i^*	Z_i^{**}
0	1	0	0	0	0
1	7	0	0	0,095238	0
2	21	2	0,095238	0,336842	0
3	35	14	0,4	1	0,238095
4	35	35	1	0	0,4
5	21	21	1	0	1
6	7	7	1	0	1
7	1	1	1	0	1

By substituting the values of $Y_i, Z_i, Z_i^*, Z_i^{**}$ from Table 1 in expression (8), (9), (14) for $\lambda = 0,1$ (1/h), and $\mu = 1$ (1/h), we obtain the following values of reliability indices under consideration.

$$T_{E_+} = 23,769 \text{ h.}$$

$$T_{E_-} = 0,469 \text{ h.}$$

$$R = 0,980645$$

Rough estimates of reliability indices

Analyzing the limits of the expressions obtained for $\lambda/\mu \rightarrow 0$, [3], it is possible to obtain rough estimates of reliability indices.

$$T_{E_+} = \frac{1}{\lambda(\lambda/\mu)^{s-1} * S * Y_s} \quad (15)$$

$$T_{E_-} = \frac{1}{s * \mu} \quad (16)$$

For the network shown in Fig. 1 $s=2, Y_s=2$

By substituting these values into expression 14,15,16 for $\lambda = 0,1$ (1/h) and $\mu = 1$ (1/h), we will obtain the following:

$$T_{E_+} = 25 \text{ h.}$$

$$T_{E_-} = 0,5 \text{ h.}$$

$$R = 0,980392$$

Comparison with known results

In order to verify the obtained expressions, we shall define the values of reliability indices under consideration for the system presented in Fig. 3, for which analytical estimates are known.

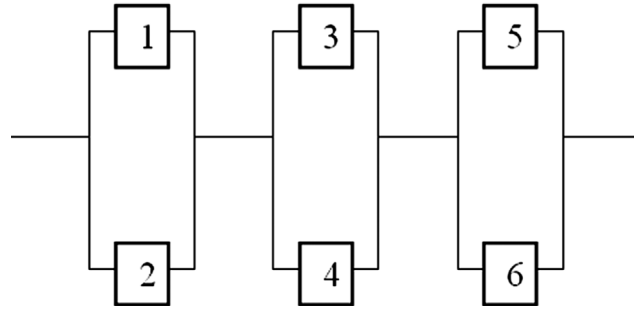


Fig. 3. A serial-parallel system

The following expressions can be found in [4].

For s identical elements connected in parallel with the parameters λ, μ .

$$t_{E_+} = \frac{1}{s * \mu} \left[\left(1 + \frac{\mu}{\lambda} \right)^s - 1 \right]$$

$$t_{E_-} = \frac{1}{s * \mu}$$

$$r = \frac{t_{E_+}}{t_{E_+} + t_{E_-}}$$

For k identical serially connected recoverable subsystems.

$$T_{E_+} = \frac{1}{k * (1/t_{E_+})}$$

$$R = r^k$$

$$T_{E_-} = T_{E_+} \frac{1-R}{R}$$

By substituting $s = 2, k = 3, \lambda = 0,1$ (1/h), $\mu = 1$ (1/h) in the above expressions, we will obtain the following:

$$T_{E_+} = 20,000 \text{ hours}$$

$$R = 0,975411$$

$$T_{E_-} = 0,504 \text{ hours}$$

To determine these reliability indices, using expressions (8), (9) and (14) it is necessary to define the values of Y_i and Z_i .

It is obvious that $Y_1 = 0$ and $Z_1 = 0.0$. Upon failure of two elements, three combinations lead to disconnection (downstate) of the system. These combinations are (1,2), (3,4), (5,6). The total number of possible combinations is 15, therefore, $Y_2 = 3$ and $Z_2 = 3 / 15$. To determine Y_3 and Z_3 , we shall consider all possible combinations out of three elements (see Table 2). From the results presented in Table 1, it follows that $Y_3 = 12$, and $Z_3 = 12/20$. In case of failure of four or more elements, the system will be disconnected, therefore, $Z_4 = Z_5 = Z_6 = 1$

Table 2. States of the system shown in Fig. 3 for failure of three elements

1	123	-	11	234	-
2	124	-	12	235	+
3	125	-	13	236	+
4	126	-	14	245	+
5	134	-	15	246	+
6	135	+	16	256	-
7	136	+	17	345	-
8	145	+	18	346	-
9	146	+	19	356	-
10	156	-	20	456	-

The results of other calculations are presented in Table 3.

Table 3. The results of characteristics calculation of the system presented in Fig. 3

i		Pi	Yi	Zi	Z*i	Z**i	Qi	Ri
0	1	0,5644739301	0	0	0	0	0,0000000000	0,5644739301
1	6	0,3386843580	0	0	0,2	0	0,0000000000	0,3386843580
2	15	0,0846710895	3	0,2	0,5	0	0,0169342179	0,0677368716
3	20	0,0112894786	12	0,6	1	0,33333	0,0067736872	0,0045157914
4	15	0,0008467109	15	1	0	0,6	0,0008467109	0,0000000000
5	6	0,0000338684	6	1	0	1	0,0000338684	0,0000000000
6	1	0,0000005645	1	1	0	1	0,0000005645	0,0000000000

By substituting the data from Table 3 in expression (26), (27), (37), we will obtain the following:

$$T_{E+} = 20,000 \text{ hours}$$

$$R = 0,975411$$

$$T_{E-} = 0,504 \text{ hour}$$

An example of reliability analysis of a network consisting of identical recoverable elements

Let us denote the number of nodes as $\mathbf{m}$ and the number of edges as $\mathbf{n}$. It should be noted that, for each pair of values of $\mathbf{n}$, $\mathbf{m}$, there is a topology that provides the highest level of reliability. Algorithms proposed by G.T. Artamonov in [5] were used to determine these topologies.

The network with the parameters $m = 20$, $n = 24$.

For achieving the maximal reliability, it is necessary to find the network with a minimum diameter and with the number of nodes equal to $2 \cdot (n - m)$ having the degree of 3, and evenly distribute the nodes of degree 2 over the edges of this network. As a result, the network presented in Fig. 4 will be obtained. The values of Y_i of the network can be determined by exhaustive search of all possible states. The results are presented in Tables 4a and 4b.

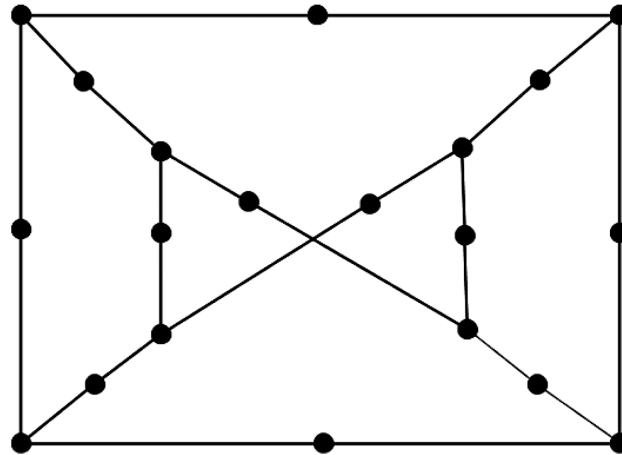


Fig.4 The network with parameters $m = 20$, $n = 24$

Table 4a. The values of Y_i and Z_i for the network shown in Fig. 4

i	1	2	3	4	5	$i \geq 6$
Y_i	0	12	328	4082	29960	
Z_i	0	0,043478	0,162055	0,384252	0,704875	1

Table 4b. The values of T_{E+} , T_{E-} , R for the network shown in Fig. 4

λ	T_{E+}	T_{E-}	R
0,1	2,13	0,3334	0,864576
0,01	390,86	0,4845	0,998762
0,001	41415,64	0,4986	0,999988

The use of other criteria of operability and models of network reliability

Up to this point, we have used connection of all nodes across the network as a criterion of its operability. However, it is appropriate to ask a question: can the loss of connection with one of the nodes be considered as a failure? If we consider the loss of connection with h nodes to be permissible, then it is possible to use the following criterion of network operability: the network is considered operable if the number of connected nodes $\geq m - h$. This criterion of network operability was analyzed in the study [6].

The obtained results can be used in this case, but it is only necessary to make appropriate changes to the algorithm determining the values Y_i . Table 5 shows the values T_{E+} and R , for different values of h in the network shown on figure 4.

Table 5. The values of T_{E+} and R for different values of h in the network shown in Fig. 4 ($\lambda=0,01$; $\mu=1$)

h	T_{E+}	R
1	5780,49	0,999943591
2	9843,50	0,999967012
3	31455,53	0,999990157

You can loosen the restriction on reliability equality of edges. Each edge can be presented as the serial connection of a certain number of elements with equal reliability. At that, dummy nodes are introduced into a network structure. The values of Z_i are determined after such changes. If one of the elements constituting an edge has failed, then this edge is removed from the network. Network connection is checked without dummy nodes.

It should be noted that the obtained results can be used when nodes have failed and edges are completely dependable. Node failure can be simulated by removing all the edges outgoing from that node.

This method of reliability analysis of networks can be used even in those cases when only those states are considered as operable ones, in which the quantity of certain network parameters, such as the transmission time or capacity, will satisfy the specified values.

For large-scale networks, the statistical estimation of values of Z_i can be determined using the Monte Carlo method. First, a random combination out of i failed elements is generated, and then the network operability is checked. The ratio of the number of tests, in which the network would be in downstate, to the total number of tests will be a statistical estimate of Z_i .

However, please note that in order to achieve the high accuracy of statistical evaluation of Z_i , the number of trials must be large enough (10^5 - 10^6).

Reliability model of network consisting of the identical non-recoverable elements

We assume that the network nodes are absolutely dependable, and the edges are identical in terms of reliability, and they failed independently of each other and have an exponential distribution of operation time to failure.

Let us consider a Markov chain, which describes the change of the network states in moments of failure of its elements.

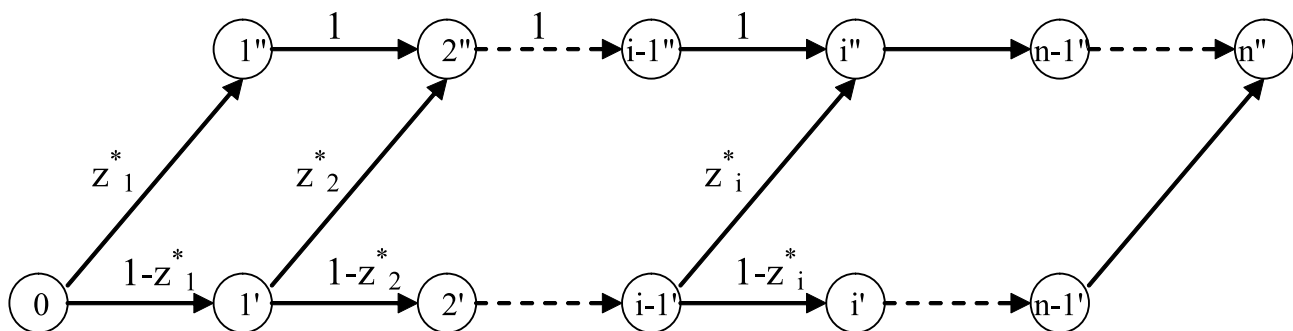


Fig. 5. The diagram of network state changes

If with $i-1$ of failed elements the network was operable, then in case of failure of the i -th element the network transits into downstate with the probability Z_i^* , or with the probability $1 - Z_i^*$ it will remain in upstate.

If with $i-1$ of failed elements the network was in downstate, then in case of failure of the i -th element, the network will remain in downstate with the probability equal to one.

Transition diagram of the process under consideration is shown in Fig. 5. The states i' corresponds to the network upstates, and the states i'' correspond to the network downstates when i elements failed.

We shall introduce the notation Q_i , as the probability of upstate, and $Q_{i''}$, as the probability of downstate of the network when i elements failed. From the definition of Z_i we have the following:

$$Q_{i'} = 1 - Z_i \quad (17)$$

$$Q_{i''} = Z_i \quad (18)$$

In accordance with the diagram of network state changes shown in Fig. 5 we can write the following:

$$Q_{i'} = Q_{(i-1)'} (1 - Z_i^*) \quad (19)$$

whence

$$Z_i^* = \frac{Q_{(i-1)'} - Q_{i'}}{Q_{(i-1)'}} \quad (20)$$

By substituting the values of $Q_{i'}$ and $Q_{i''}$ from (17) and (18) in (20), we will obtain

$$Z_i^* = \frac{Z_i - Z_{i-1}}{1 - Z_{i-1}} \quad (21)$$

Also, from expression (19) it follows

$$Q_{i'} = \prod_{j=1}^i (1 - Z_j^*) = 1 - Z_i. \quad (22)$$

To determine the mean time to failure, we shall consider the continuous Markov process that describes the behavior of a system over time. A number of failed elements and the state of the network [7] specify states of the process. State transition diagram of the process is shown in Fig. 6.

Let us denote the failure rate of elements by λ . Suppose that at some point in time there are i failed elements, and this network is operable. For an infinitely small time interval Δt , any of the following events can occur:

- The network will remain in upstate. The probability of this event is equal to $(1 - (n-i)\lambda \Delta t)$;
- One more element will fail, and the network transits into downstate. The probability of this event is equal to $(1 - (n-i)\lambda Z_{i+1}^* \Delta t)$;

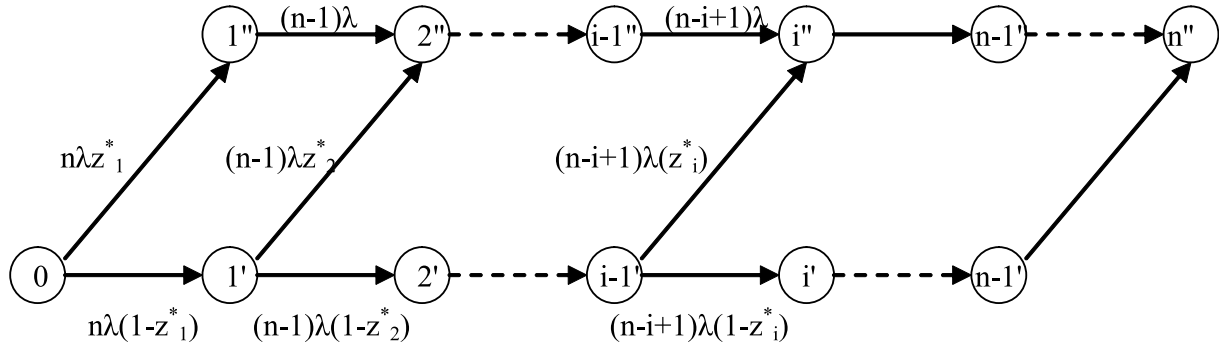


Fig. 6. Markov process of network state changes

- One more element will fail, but the network will remain in upstate. The probability of this event is equal to $(1-(n-i)\lambda (1-Z_{i+1}^*) \Delta t)$.

In order to simplify the analytical calculations, we shall replace a set of downstates by one absorbing state (see Fig. 7).

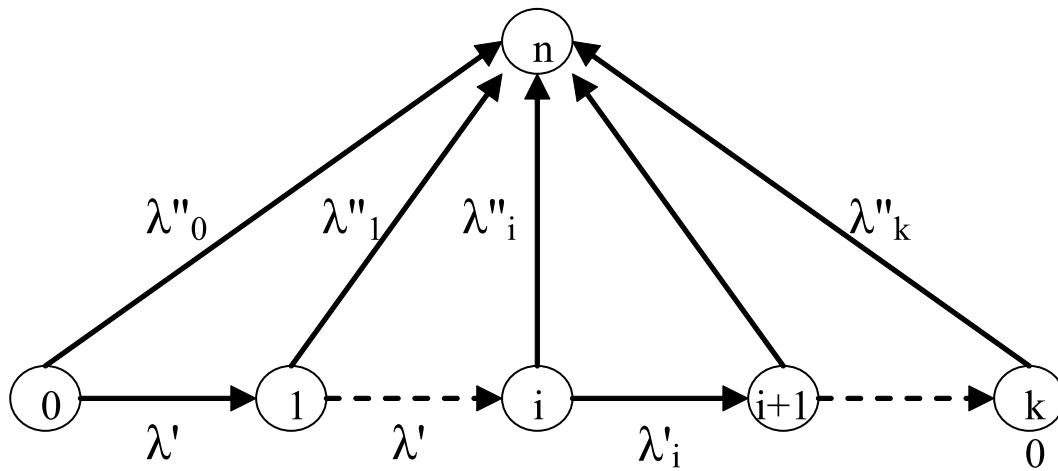


Fig. 7. Markov process of network state changes with absorbing state

The probabilities of process stay in different states at an arbitrary time point $P_i(t)$ may be found by solving the following system of differential equations:

$$\begin{aligned} \frac{\partial P_0(t)}{\partial t} &= -\lambda'_0 P_0(t) - \lambda''_0 P_0(t) = -\lambda_0 P_0(t) \\ \frac{\partial P_i(t)}{\partial t} &= \lambda'_{i-1} P_{i-1}(t) - \lambda'_i P_i(t) - \lambda''_i P_i(t) = \lambda'_{i-1} P_{i-1}(t) - \lambda_i P_i(t) \\ \frac{\partial P_n(t)}{\partial t} &= \sum_{i=0}^k \lambda''_i P_i(t), \end{aligned} \quad (23)$$

where $\lambda_i = (n-i)\lambda$, $\lambda'_i = (1 - Z_{i+1}^*) \lambda_i$

$\lambda''_i = Z_{i+1}^* \lambda_i$

k is the maximum number of elements after the failure of which the network can be in upstate.

Let us solve the system of differential equations (23), using the Laplace transform with the initial conditions $P_0(0)=1$, $P_i(0)=0 \quad \forall i \neq 0$.

We shall introduce the following notation $F(s) = \int_0^{\infty} P(t)e^{-st} dt$

Then the system of differential equations (23) is reduced to the system of algebraic equations with regard to $F(s)$.

$$\begin{aligned} sF_0(s) &= 1 - \lambda_0 F_0(s) \\ sF_i(s) &= \lambda'_{i-1} F_{i-1}(s) - \lambda_i F_i(s) \end{aligned} \quad (24)$$

$$sF_n(s) = \sum_{i=0}^k \lambda''_i F_i(s)$$

Hence, we have the following:

$$\begin{aligned} F_0(s) &= \frac{1}{s + \lambda_0} \\ F_i(s) &= \frac{\lambda'_{i-1}}{s + \lambda_i} F_{i-1}(s) \end{aligned} \quad (25)$$

$$F_n(s) = \frac{1}{s} \sum_{i=0}^k \lambda''_i F_i(s).$$

This solution allows obtaining the expression for the mean time to failure:

$$T = \sum_{i=0}^k F_i(s) \Big|_{s=0} \quad (26)$$

Expanding expressions (25) we will obtain

$$F_0(0) = \frac{1}{\lambda_0} = \frac{1}{n\lambda} \quad (27)$$

$$F_i(0) = \frac{\lambda'_{i-1}}{\lambda_i} F_{i-1}(0) = \frac{\prod_{j=1}^i (1 - Z_j^*)}{(n-i)\lambda}. \quad (28)$$

Using (22), expression (28) can be simplified as follows:

$$F_i(0) = \frac{\prod_{j=1}^i (1 - Z_j^*)}{(n-i)\lambda} = \frac{1 - Z_i}{(n-i)\lambda}. \quad (29)$$

Then from expression (26) it follows

$$T = \frac{1}{\lambda} \sum_{i=0}^k \frac{(1 - Z_i)}{n-i}. \quad (30)$$

The expression (30) allows determining the value of the mean time to failure by means of the known values of Z_i and λ .

Now we shall determine the value of T for the network shown in Fig. 1, at $\lambda = 0,01$ (1/h)

$$T = 100 \left(\frac{1}{7} + \frac{1}{6} + \left(\frac{19}{21} \right) \frac{1}{5} + \left(\frac{21}{35} \right) \frac{1}{4} \right) = 100 * \frac{269}{420} \approx 64,047(\text{hour}).$$

Comparison with known results

To verify the obtained expression, we should define the mean time to failure of the system, for which analytical estimates are known (see Fig. 3).

In [4], the following expressions can be found.

The probability of failure-free operation of the system consisting of two identical elements connected in parallel

$$P_{(t)} = 1 - (1 - e^{-\lambda t})^2 = 2e^{-\lambda t} - e^{-2\lambda t}.$$

The probability of failure-free operation of the system consisting of three identical serially connected subsystems.

$$P_{\tilde{n}(t)} = (P_{(t)})^3$$

$$P_{\tilde{n}(t)} = (2e^{-\lambda t} - e^{-2\lambda t})^3 = 8e^{-3\lambda t} - 12e^{-4\lambda t} + 6e^{-5\lambda t} - e^{-6\lambda t}$$

The mean time to failure of the system is equal to

$$T = \int_0^{\infty} P_{\tilde{n}(t)} dt = \frac{1}{\lambda} \left(\frac{8}{3} - \frac{12}{4} + \frac{6}{5} - \frac{1}{6} \right) = \frac{1}{\lambda} \left(\frac{42}{60} \right) = 0,7 \frac{1}{\lambda}.$$

To determine the mean time to failure by using expression (30), first, it is necessary to define the values of Z_i . For the system under consideration, they are as follows:

$$Z_1=0,0; Z_2=3/15; Z_3=12/20; Z_4=Z_5=Z_6=1.$$

By substituting these values into (30), we will obtain:

$$T = \frac{1}{\lambda} \left(\frac{1}{6} + \frac{1}{5} + \left(\frac{12}{15} \right) \frac{1}{4} + \left(\frac{8}{20} \right) \frac{1}{3} \right) = \frac{1}{\lambda} \left(\frac{42}{60} \right) = 0,7 \frac{1}{\lambda}$$

This example also shows that the proposed method can be used to determine the mean time to failure of complex serial-parallel systems consisting of identical non-recoverable elements.

An example of reliability analysis of the network consisting of identical non-recoverable elements

Let us denote by $\mathbf{m}$ the number of nodes and by $\mathbf{n}$ the number of edges. Now we shall consider a network with parameters $m = 20$, $n = 24$ (see Fig. 4). The values of $\mathbf{Z}_i$ of the network can be determined by exhaustive search of all possible states.

The proposed method can be used with other criteria of the network operability. For example, the network is considered operable if the number of connected nodes $\geq \mathbf{m} - \mathbf{h}$. The obtained results can be used in this case, but it is only necessary to make appropriate changes to the algorithm determining the values of $\mathbf{Z}_i$. Table 6 shows the values of $\mathbf{Z}_i$, for different values of h for the network shown in Fig. 4. Determination of $\mathbf{Z}_i$ for $k > 0$ was carried out by using the Monte Carlo method. The number of tests was 10^6 .

Table 6. The values of $\mathbf{Z}_i$ for different values of h for the network shown in Fig. 4

i / h	0	2	4	6	8	10
1	0,0000000	0,00000	0,00000	0,00000	0,00000	0,00000
2	0,0434783	0,00000	0,00000	0,00000	0,00000	0,00000
3	0,1620553	0,01581	0,00000	0,00000	0,00000	0,00000
4	0,3841521	0,07980	0,01498	0,00435	0,00296	0,00000
5	0,7048748	0,25247	0,08813	0,03329	0,01644	0,00000
6	1,0000000	0,56194	0,27850	0,13070	0,05976	0,00324
7	1,0000000	0,86648	0,56942	0,33252	0,17912	0,04445
8	1,0000000	1,00000	0,82642	0,58123	0,36764	0,16783
9	1,0000000	1,00000	0,96544	0,79849	0,57894	0,34029
10	1,0000000	1,00000	1,00000	0,93211	0,76173	0,52593
11	1,0000000	1,00000	1,00000	0,98807	0,89262	0,69336
12	1,0000000	1,00000	1,00000	1,00000	0,96470	0,82566
13	1,0000000	1,00000	1,00000	1,00000	0,99360	0,91743
14	1,0000000	1,00000	1,00000	1,00000	1,00000	0,97046
15	1,0000000	1,00000	1,00000	1,00000	1,00000	0,99403
α	0,214850615	0,29501	0,354027	0,411813	0,476755	0,571528

$$\alpha = \sum_{i=0}^k \frac{(1-Z_i)}{n-i}$$

$$T = \alpha * \lambda$$

Conclusion

The analytical expressions for determining the values of reliability indices of networks consisting of elements that have an exponential distribution of time to failure and recovery time have been obtained. At the same time, nodes and edges of the network can be considered as completely dependable. The accuracy of the obtained result is confirmed by calculating the reliability indices of a serial-parallel system for which analytical estimates are known.

References

1. Issues of the mathematical theory of reliability. E. Yu. Barzilovich, Yu.K. Belyaev, V.A. Kashtanov, I.N. Kovalenko, A.D. Soloviev, I.A. Ushakov. / Ed. by B.V.Gnedenko, Moscow, Radio and Communication, 1983. -367p.
2. **Tkachev O. A.** Using Markov chains to analyze reliability of systems with a complex structure. Cybernetics, # 5, 1983, pp. 95-101.
3. **Tkachev O. A.** Reliability analysis of data networks. – Proceedings of the International Conference “Distributed Computer and Telecommunication Networks: Theory and Applications” (DCCN-2.010) ISBN 978-5-9901871-2-2, Russia, Moscow, 2010, pp..276-283.
4. Mathematical Methods in Reliability theory. B.V. Gnedenko, Yu.K. Belyaev, A.D. Soloviev. Moscow: Nauka, 1965. – 524 p. with illustrations.
5. The theory of designing computers, systems and networks: Tutorial / V.I.Matov, G.T.Artamonov, O.M. Brekhov and others; ed. V.I.Matov. -M.: Publishing House of the Moscow Aviation Institute, 1999. -460 p.
6. **Tkachev O.** Analytical estimation of reliability of networks consisting of identical elements. Reliability – Theory & Application, ISSN 1932-2321, № 2 (21) 2011, p.9-20.
7. **Tkachev O.** Determination of mean time to failure of a network consisting of identical non-repairable elements. Reliability – Theory & Application, ISSN 1932-2321, № 3 (22) 2011, p. 43-46.

Федотова Г.А.

РЕЗЕРВИРОВАНИЕ КАК СОСТАВНАЯ ЧАСТЬ ПРОБЛЕМЫ НАДЁЖНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ

Статья посвящена проблеме резервирования генерирующих мощностей в Единой электроэнергетической системе (ЕЭС) России. Рассмотрены используемые в советский период и в настоящее время подходы к ее решению, особенности резервирования в рыночных условиях. Приведены общие принципы резервирования, используемые в России и за рубежом при вертикально-интегрированной иерархической структуре управления электроэнергетикой и в рыночной среде. Даны рекомендации по доработке отдельных нормативных документов, регламентирующих порядок выбора и размещения резервных мощностей в ЕЭС и разработке оптимизационных моделей для решения задач резервирования в многозонном энергообъединении.

Ключевые слова: электроэнергетика, резервирование генерирующих мощностей, балансовая надёжность, энергорынок, конкурентный отбор мощности.

Введение в проблему и основные принципы резервирования

Резервирование является одним из главных средств повышения надёжности в энергетике на всех временных уровнях управления электроэнергетическими системами (ЭЭС). Оно обеспечивает частичную компенсацию снижения надёжности в ЭЭС, возникающего вследствие отказов оборудования, нарушения топливоснабжения ТЭС и водоснабжения ГЭС, отклонения фактических условий функционирования ЭЭС от прогнозных. Задача определения оптимальной величины и размещения резервов мощности в объединенной электроэнергетической системе (ОЭС) с ограниченными пропускными способностями межсистемных электрических связей очень сложна. Несмотря на то, что этой проблемой занимаются уже более полувека, до настоящего времени не существует единого общепринятого подхода к ее решению [1-3]. При полностью централизованном управлении отраслью существует регулирующий орган или регулирующая вертикально-интегрированная компания, отвечающая за выбор и поддержание резерва генерирующей мощности, достаточного для обеспечения необходимого уровня надёжности. В рыночной среде сам рынок может решать, какой уровень резерва мощности нужно обеспечить для соблюдения нормативов надёжности и как его размещать в энергообъединении. Но и в таких моделях управление резервами не осуществляется без какого-либо административного вмешательства. В условиях энергорынка подходы к выбору и размещению резервов мощности в ОЭС меняются в зависимости от типа и структуры рынка.

В электроэнергетических системах с централизованным рынком мощности, к числу которых относится ЕЭС России, формирование резервов генерирующих мощностей производится посредством конкурентного отбора мощности (КОМ) в соответствии с требованиями и правилами энергорынка. Основные функции по формированию правил рынка мощности и требований к поддержанию надёжности ЕЭС России выполняет Системный оператор (СО) (ФЗ № 250 от 04.11.2007). При проведении конкурентного отбора мощности СО определяет потребность в мощности по зонам рынка и отбирает с учетом ограничений по пропускным способностям сети необходимые объемы генерирующей мощности, обеспечивающие достаточный уровень балансовой надёжности по минимальной стоимости. Основные экономические принципы обеспечения надёжности ЭЭС в России в условиях энергорынка определены Федеральным законом “Об электроэнергетике” (статьи 6, 9, 18, 20, 38, 39 [4]). В соответствии с этим законом управление надёжностью и резервами в электроэнергетике должно быть основано на распределении ответственности за их обеспеченность между субъектами отношений и координации этой ответственности на основе сочетания государственного регулирования и рыночных механизмов. Несмотря на большое разнообразие подходов, используемых для выбора и размещения резервов генерирующей мощности в мировой практике, все они основаны на следующих основных принципах.

1. Резервирование является технико-экономической проблемой, решение которой связано как с проведением технических мероприятий, так и с оптимизацией резервов мощности на основе математических моделей. Существует два основных подхода к решению задач оптимального резервирования: нормативный и затратный. Нормативный основан на выборе величины резерва мощности в энергообъединении и его размещении по ЭЭС с целью обеспечения нормативного уровня балансовой надёжности в ОЭС и надёжности электроснабжения потребителей. Затратный состоит в оптимизации резервов по экономическим критериям, включающим затраты на создание резервов и ущерб от недоотпуска электроэнергии потребителям, обусловленного дефицитом мощности. Поскольку обеспечение абсолютной надёжности экономически неэффективно, то при оптимизации резервов мощности в ЭЭС должен быть соблюден баланс между затратами на создание и поддержание резервов и ущербом потребителей от недопоставки электроэнергии. Как в России, так и за рубежом применяются оба подхода.

2. Задачи резервирования решаются взаимосогласованно на этапах планирования развития электроэнергетики и функционирования ЭЭС. Управление планированием развития отрасли предполагает создание резервов установленной мощности ЭЭС и выделение на их создание определённых финансовых средств. При функционировании ЭЭС резервы используются по своему прямому назначению – для обеспечения балансовой надёжности и надёжного снабжения потребителей электроэнергией требуемого качества. При этом, насколько эффективно резервы используются в условиях эксплуатации, настолько оправданы затраты на их создание на этапе планирования развития.

3. Для определения оптимальной величины и размещения резервов мощности в энергообъединении используются оценочные и вероятностные подходы. В мировой практике широкое использование получили вероятностные методы и модели. Они позволяют учитывать аварийность генерирующего и сетевого оборудования, случайные колебания нагрузки и ошибки её прогноза, перерывы топливоснабжения, отставания сроков ввода новых мощностей и другие случайные факторы, влияющие на надёжность.

4. Основную сложность в решении задач надёжности и резервирования в энергообъединении с ограниченными пропускными способностями межсистемных связей является учёт этих ограничений, разновременности прохождения максимумов нагрузок и различий их характерных графиков. Применительно к современным условиям функционирования и развития электроэнергетики России

Федеральным Законом “Об электроэнергетике” введено понятие зоны свободного перетока мощности (ЗСПМ). Наличие большого количества таких зон в ЕЭС, не всегда территориально совпадающих с региональными энергосистемами, усложнило проблему учёта указанных факторов.

При многозонном представлении энергообъединения используемые в мировой практике критерии выбора величины и размещения резервов мощности, а также показатели балансовой надёжности не являются в достаточной мере обоснованными и носят, как правило, эмпирический характер. Поэтому для решения задач резервирования в России не может использоваться в чистом виде какая-либо зарубежная методика. Необходим научно обоснованный подход, который бы учитывал фактическое состояние отрасли и современные требования к надёжности, специфику развития и функционирования ЭЭС в условиях энергорынка. До начала реформирования отрасли существовала иерархическая система управления надёжностью и резервами мощности в ЕЭС. Отношения между производителями и потребителями электроэнергии строились на выполнении обязательств, инструкций и указаний. Переход от централизованной системы управления электроэнергетикой к рынку с законодательной и имущественной ответственностью за уровень надёжности всех структур, связанных с производством, транспортом, распределением и потреблением электроэнергии, требует переосмысления принципов формирования резервов генерации в электроэнергетических системах, пересмотра подходов к обеспечению надёжности. Традиционные принципы обеспечения надёжности и действующая сегодня в России практика выбора и размещения резервов генерирующей мощности в ЕЭС должны быть скорректированы, в первую очередь в части критериев принятия управленческих решений в рыночных условиях, требований к видам и уровням резервов с учётом современного состояния оборудования электростанций и электрических сетей [5].

Выбор и размещение резервов генерирующей мощности в ЕЭС России на этапе планирования развития электроэнергетики

При управлении развитием электроэнергетики задачи выбора и размещения резервов установленной генерирующей мощности ЕЭС решаются в разных временных разрезах:

- при планировании развития электроэнергетики (с заблаговременностью 7 – 15 лет);
- при проектировании развития ЕЭС (с заблаговременностью 5-10 лет);
- при функционировании долгосрочного рынка мощности (с заблаговременностью 4 – 5 лет).

При планировании развития электроэнергетики формируется Генеральная схема размещения объектов электроэнергетики с детализацией по объединённым энергосистемам, которая корректируется не реже одного раза в 3 года. Разрабатываются схемы и программы развития ЕЭС, объединённых и региональных энергосистем, определяющие сбалансированные планы развития генерирующих мощностей и электрических сетей [6]. Одной из главных задач на этом этапе является выбор величины резервов установленной генерирующей мощности в энергосистемах или зонах свободного перетока мощности, обеспечивающих баланс между производством и потреблением электроэнергии и мощности. Её решение осуществляется на основе системы нормативов: на показатели балансовой надёжности; на пропускные способности межсистемных электрических связей, в том числе для реализации резервов мощностей; на запасы топлива на ТЭС, воды на ГЭС и т. д.

Для определения необходимого резерва генерирующей мощности на этом этапе оценивается величина необходимой дополнительной к исходному уровню установленной мощности в ЕЭС. При этом вводы дополнительной генерирующей мощности, её структура и размещение должны обеспечивать покрытие прогнозируемой нагрузки с учётом возможных превышений над ожидаемой величиной, возможность проведения плановых ремонтов генерирующего оборудования и компенсацию мощности, выведенной из работы по причине полных или частичных

отказов. Потребность во вводе дополнительной установленной мощности определяется при составлении перспективных балансов электрической мощности и энергии. При этом решаются задачи прогнозирования роста нагрузок и электропотребления; выбора оптимальной структуры вновь вводимой мощности; определения местоположения и её основных параметров, очередности строительства, расширения, реконструкции и технического перевооружения электростанций. Перспективные балансы мощности и энергии в ЕЭС разрабатываются с учётом условий совместной работы региональных энергосистем в ОЭС. При разделении ЕЭС на зоны свободного перетока мощности балансы составляются для ЕЭС в целом и для каждой зоны, которые затем согласуются и уточняются. Необходимые резервы мощности в региональных ЭЭС или ЗСПМ определяются с учётом сетевых ограничений. В результате для выполнения общего баланса мощности ЕЭС путём технико-экономических расчётов принимаются решения по планированию новых генерирующих мощностей в ЭЭС и усилению пропускных способностей межсистемных связей.

Значения необходимого резерва мощности в энергообъединениях при формировании Генеральной схемы размещения объектов электроэнергетики принимаются как доля (в процентах) от максимумов нагрузки. Они определены в Методических рекомендациях по проектированию развития энергосистем [7].

На этапе проектирования в связи с уменьшением заблаговременности принятия решений (5 – 10 лет) снижается степень неопределённости спроса на электрическую энергию и требуемого увеличения установленных мощностей для его удовлетворения. В этих условиях осуществляется корректировка уровня резерва генерирующих мощностей, структуры мощности, формирующей резерв, и его территориального размещения. При этом проводится проверка перспективных балансов мощности и энергии, внесение коррективов в проект развития в случае их нарушения, уточнение объёмов поставляемых энергоресурсов и при необходимости изменение мест их размещения, характеристик новых электростанций и сетей, корректировка пропускных способностей связей и оценка уровня балансовой надёжности.

Величина резерва мощности в энергосистемах на этом этапе рассчитывается на основе специальных оценочных расчётов при рассмотрении различных аварийных ситуаций с учётом функционального назначения его составляющих (оперативной, ремонтной и стратегической). При этом оперативный резерв должен обеспечивать нормативную надёжность покрытия нагрузок, оцениваемую вероятностью бездефицитной работы ЭЭС. Ремонтный резерв должен компенсировать снижение установленной мощности энергосистем, связанное с выводом генерирующего оборудования в плановые ремонты. Его величина определяется на период прохождения годового максимума нагрузки на основе характеристик и конструктивных особенностей оборудования с учётом нормативов на периодичность и длительность ремонтов. Стратегический резерв должен компенсировать нарушения баланса мощности из-за непредвиденных его отклонений от прогноза, связанные в основном с инерционностью энергетического строительства и/или с опережающим развитием смежных отраслей.

С заблаговременностью 4 – 5 лет при функционировании долгосрочного рынка мощности величины и размещение резервов мощности по ЗСПМ определяются Положением о порядке определения величины спроса на мощность и плановых коэффициентов резервирования мощности в зонах [8]. В соответствии с этим положением величина спроса на мощность определяется произведением величины прогнозируемого в год поставки максимального часового потребления электрической энергии в зоне и планового коэффициента резервирования мощности за вычетом объёмов производства электрической энергии генерирующими объектами, функционирующими на розничных

рынках. Максимальный часовой объем потребления электрической энергии в зоне определяется Системным оператором на основе прогноза потребления мощности по территориям субъектов Российской Федерации, включенного в программу развития ЕЭС. Плановый коэффициент резервирования мощности рассчитывается Системным оператором для ЗСПМ как сумма показателя 1,17, коэффициента прогнозного недоиспользования мощности и коэффициента, учитывающего экспорт электрической энергии. Коэффициент прогнозного недоиспользования мощности определяется отношением среднемесячного снижения мощности, обусловленного проведением внеплановых ремонтов генерирующего оборудования, к величине прогнозируемого максимального объема потребления в соответствующей зоне.

Действующая схема планирования резерва мощности в электроэнергетике России и используемые нормативные документы, регламентирующие порядок выбора величины необходимого резерва мощности и его размещения в ЕЭС, были разработаны для условий централизованного управления отраслью [6-8]. В Методических рекомендациях по проектированию развития энергосистем [7] значения оперативного резерва мощности, зависящего от структуры установленного оборудования электростанций, его типов, единичных мощностей и аварийности, величины вероятного отклонения баланса мощности системы от прогноза, вычисляются на основе нормативных значений этих показателей, принятых ещё в советское время. В Положении о порядке определения величины спроса на мощность и плановых коэффициентов резервирования мощности в ЗСПМ [8] выбор планового коэффициента резервирования не основан на непосредственном анализе балансовой надёжности. Эти документы требуют доработки в части учёта функционирования рынка мощности и современных требований к надёжности. В частности:

1. Используемая методика разбиения на ЗСПМ недостаточно обоснована в части выбора оптимального резерва в зонах с учётом надёжности при реализации полноценного конкурентного отбора мощностей.

2. Задание единого для всех зон рынка показателя 1,17 не обеспечивает оптимальность выбора величины и размещения резерва мощности по зонам, поскольку при этом не учитываются различия в зонах по составу и структуре генерирующих мощностей, единичным мощностям и аварийности, по связям с другими зонами и их пропускным способностям.

3. Использование оценочных подходов при выборе величины резервов мощности в ЕЭС не позволяет учитывать случайные факторы, влияющие на надёжность, нужны вероятностные методы и модели. Такие методы применялись в практике планирования развития энергосистем в нашей стране в советский период и широко используются за рубежом.

Следовательно, практика выбора и размещения резервов установленной мощности, сложившаяся в настоящее время в России, не обеспечивает в достаточной степени оптимальность решений по надёжности. Используемая методика не позволяет определить экономически обоснованные значения резервов мощности с учётом надёжности, новых экономических условий развития отрасли и современного состояния энергетического оборудования. Необходимы новые научно обоснованные подходы, соответствующие международным стандартам, учитывающие рыночные отношения в отрасли, современные формы управления электроэнергетикой и требования к надёжности [5, 11]. Они могут быть основаны на методах, разработанных в советский период, адаптированных к современным условиям. Подходы, разработанные и используемые в СССР, базировались на глубоко проработанных фундаментальных исследованиях и вполне соответствовали международным стандартам, но были ориентированы на вертикально-интегрированную централизованно управляемую электроэнергетику [9, 10]. В последние 20 лет они не получили необходимого развития и практического использования.

Содержательные постановки задач выбора и размещения резервов мощности

Как было отмечено ранее, выбор оптимальной величины резерва и его территориальное размещение в ЕЭС по зонам свободного перетока мощности должны быть основаны на компромиссе между стоимостью его создания и поддержания и ущербом у потребителей от недопоставки электроэнергии, обусловленной дефицитом мощности. Повышение надёжности энергосистем путем создания резервов мощности требует увеличения приведённых затрат, включающих капиталовложения и эксплуатационные расходы. При этом уменьшается ущерб потребителей от недоотпуска им электроэнергии.

В общем случае задача оптимизации резерва мощности в ЭЭС состоит в выборе такого резерва, который бы обеспечивал необходимую надёжность при минимальных затратах. На рис. 1 показаны зависимости затрат на создание и поддержание резерва мощности (А), ущерба от недопоставки электроэнергии потребителям (В) и суммарных приведенных затрат с учётом ущерба (С) от величины резерва располагаемой мощности [9]. Минимум кривой суммарных затрат С соответствует оптимальному уровню резерва мощности.

Критерий выбора резерва мощности в отдельной энергосистеме или зоне свободного перетока мощности может быть представлен функционалом:

$$C = C_R + M[Y] \rightarrow \min, \quad (1)$$

где: C – приведенные затраты; C_R – затраты на создание и поддержание резерва генерирующей мощности в зоне; $M[Y]$ – математическое ожидание ущерба от ненадёжности электроснабжения потребителей, обусловленного дефицитом мощности.

Задача выбора и размещения резервов мощности значительно усложняется в энергообъединении со слабыми межсистемными связями. Такое объединение может не отвечать требованиям надёжности при наличии в его составе дефицитных зон даже если отдельные энергосистемы или зоны свободного перетока мощности соответствуют требованиям надёжности или имеют избытки мощности. Недостаток мощности в дефицитных зонах покрыть невозможно из-за ограниченных пропускных способностей внешних связей. Чтобы привести это энергообъединение в соответствие со стандартом надёжности, необходимо либо ввести дополнительные мощности в определенных зонах, либо усилить связи между зонами. Для этого нужно знать, какие связи нужно усилить и в каких зонах при этом экономически целесообразно ввести дополнительные мощности по требованиям надёжности. Чтобы понять, как зависит уровень надёжности объединения от объёма резервирования в зонах и запасов пропускных способностей межсистемных связей, необходимы исследования по оценке балансовой надёжности в отдельных зонах и по объединению в целом с учетом пропускных способностей связей. Решение такой задачи в условиях энергорынка сопряжено с большими трудностями, особенно для крупного энергообъединения, каковым является ЕЭС России.

Для достижения необходимого уровня балансовой надёжности в многозональном энергообъединении со слабыми электрическими связями в качестве альтернативы увеличению резервов генерирующей мощности в зонах может рассматриваться соответствующее увеличение пропускной способности сети. Тогда задача оптимального резервирования заключается в одновременной оптимизации

резервов генерирующей мощности в зонах и запасов по пропускным способностям связей между зонами. В качестве критерия оптимизации может быть использован следующий функционал:

$$C_{\Sigma} = \sum_{\mu=1}^M C_{R\mu} + \sum_{l=1}^L C_l + \sum_{\mu=1}^M M_{\mu}[Y] \rightarrow \min, \quad (2)$$

где: M – количество зон в энергообъединении; L – количество связей между зонами; C_{Σ} – суммарные приведенные затраты в объединении; $C_{R\mu}$ – затраты на создание и поддержание резерва генерирующей мощности в μ -й зоне; C_l – затраты на усиление пропускной способности l -й связи; $M_{\mu}[Y]$ – математическое ожидание ущерба от ненадёжности электроснабжения потребителей в μ -й зоне.

Возможен и другой подход, когда критерием выбора и размещения резерва генерирующей мощности служит минимум суммарных приведенных затрат, включающих затраты на создание резервов генерирующей мощности и усиление связей, а необходимый уровень надёжности электроснабжения потребителей задается ограничением по нормативам. Тогда величина резерва мощности в каждой зоне многозонного объединения будет выбираться из условий экономически целесообразной и технически необходимой (нормативной) надёжности, а критерий выбора резервов мощности в энергообъединении и его размещения по ЗСПМ будет иметь следующий вид:

$$C_{\Sigma} = \sum_{\mu=1}^M C_{R\mu} + \sum_{l=1}^L C_l \rightarrow \min, \pi_{\mu} \geq \pi_{norm}, \quad (3)$$

где π_{μ} и π_{norm} – расчетная величина показателя надёжности электроснабжения потребителей в μ -й зоне и его нормативное значение соответственно.

Использование критерия (3) для выбора и размещения резервов генерирующей мощности ОЭС в рыночных условиях позволяет наиболее полно учитывать специфику отношений между субъектами энергорынка. При централизованном управлении электроэнергетикой России размещение резервов было основано на коллективном принципе взаимопомощи ЭЭС, когда между системами распределялся не только резерв, но и дефицит мощности. Тогда включение математического ожидания ущерба от недоотпуска электроэнергии потребителям в функционал (2) было правомочно. В рыночных условиях в избыточные энергосистемы не может быть распределен дефицит мощности других ЭЭС. Каждая энергосистема стремится в первую очередь обеспечить необходимый уровень собственной надёжности при минимальных затратах и получить максимальную прибыль. Во вторую – выполнить договорные обязательства перед смежными энергосистемами и только после этого выдать избыток мощности для покрытия дефицита мощности в других системах на коммерческой основе. При таком подходе необходимы нормативы надёжности электроснабжения потребителей. Попытка их получения была сделана в СССР [9], но с тех пор работы в этом направлении не ведутся, поэтому оптимизация резервов по критерию (3) пока проблематична.

Использование резервов генерирующей мощности при функционировании ЭЭС

При функционировании ЭЭС основное значение приобретают вопросы использования резервов с учётом их функционального назначения и таких свойств, как мобильность и экономичность.

На этом этапе смысл задачи состоит в уточнении величины резерва мощности в каждой зоне свободного перетока мощности и его перераспределении между зонами с целью обеспечения требуемого уровня надёжности в зонах и по энергообъединению в целом с учетом фактически сложившейся ситуации в энергосистемах. Такое перераспределение в современных условиях функционирования ЭЭС должно производиться через рынок мощности и системных услуг. При этом в каждой зоне должен быть предусмотрен оперативный резерв для покрытия собственной нагрузки с заданной степенью надёжности и ремонтный резерв – для замещения мощностей, выводимых в плановый ремонт и на реконструкцию. Тесная взаимосвязь оперативной и ремонтной составляющих резерва мощности позволяет за счет оптимизации сроков проведения ремонтов в процессе их планирования воздействовать на величину оперативной составляющей, обеспечивающей надёжность. Поэтому задача перераспределения резервов мощности должна решаться совместно с задачей планирования ремонтов генерирующего оборудования, связанных со снижением надёжности. Совместное планирование ремонтов оборудования электрических станций и сетей межсистемных связей дает дополнительные возможности повышения надёжности за счет использования системных эффектов [12].

В условиях энергорынка задача планирования ремонтов заслуживает особого внимания в контексте с проблемой резервирования при функционировании ЭЭС. Разделение собственности и введение рыночных механизмов в процесс управления электроэнергетикой привели к появлению независимых субъектов рынка, имеющих несовпадающие интересы, которые прямо или косвенно отражаются на подходах к планированию ремонтов. Генерирующие и сетевые компании заинтересованы в получении максимальной прибыли от эксплуатации оборудования, установленного на электростанциях и в сетях, находящихся в их собственности. Потребители заинтересованы в минимальной цене на электроэнергию, системный оператор – в обеспечении требуемой надёжности и получении прибыли и т. д. В условиях рынка независимо от выбранного критерия должен работать механизм, позволяющий при выборе сроков проведения плановых ремонтов согласовывать интересы всех субъектов рынка [13].

Перераспределение резервов генерирующей мощности между ЗСПМ в условиях функционирования ЭЭС может осуществляться с помощью оптимизационных математических моделей по критериям надёжности в предположении, что величина имеющихся в зонах резервов определена и экономически обоснована на стадии планирования развития [14]. В зависимости от условий работы энергообъединения и целей оптимизации возможно использование разных критериев надёжности, например, таких:

- Обеспечение равновозможной надёжности электроснабжения потребителей в зонах и во времени.
- Достижение равной вероятности работоспособного состояния энергосистем (зон свободного перетока мощности).
- Выравнивание оперативного резерва мощности между зонами и во времени пропорционально нагрузке.
- Обеспечение максимально возможной надёжности электроснабжения потребителей в энергообъединении с учётом нормативов надёжности в зонах.

Уровень надёжности при этом может оцениваться различными показателями, в том числе показателем относительной обеспеченности электроэнергией потребителей, вероятностью работоспособного состояния энергосистем и т.д. Выбранный показатель надёжности должен быть нормируемым, иметь простой физический смысл и быть достаточно чувствительным к различным возмущениям, приводящим к снижению надёжности (аварийное снижение мощности, случайный

рост нагрузки, вывод оборудования в ремонт) и к мероприятиям, повышающим надёжность (ввод нового оборудования, усиление пропускных способностей связей, резервирование).

Наряду с критериями надёжности теоретически возможно решение рассматриваемой задачи на основе затратных критериев. Тогда путем рационального использования резервов мощности можно обеспечить минимум суммарных затрат, включающих затраты на использование и содержание резервов мощности, на топливо и ремонт оборудования, а также ущерб от недоотпуска электроэнергии потребителям. Практически такой подход трудно реализуем и одна из главных проблем использования затратных критериев заключается в отсутствии необходимой экономической информации и/или в ее недоступности. Непростым делом является прогнозирование цен на топливо и ремонт, затрат на содержание резервов мощности, тарифов на электроэнергию и ущербов от недоотпуска электроэнергии потребителям в условиях энергорынка.

Заключение

Таким образом, существующие и используемые сегодня подходы и методы выбора и размещения резервов генерирующей мощности ЭЭС в России не соответствуют современной организационной структуре отрасли. На сегодняшний день сохраняют силу Методические рекомендации по проектированию развития энергосистем, основанные на едином подходе к проектированию развития энергосистем, в том числе на экономическом обосновании уровня резервов установленной мощности. Данные рекомендации разработаны в 2003 г. и ориентированы на вертикально-интегрированную иерархическую структуру отрасли с централизованным управлением. Требуют доработки рекомендуемые уровни резервов в ОЭС, входящих в состав ЕЭС, в связи с интенсивным старением оборудования электрических станций и сетей.

Необходима доработка Положения о порядке определения величины спроса на мощность, выбора и размещения резервов мощности в части деления ЕЭС на зоны свободного перетока мощности и определения планового коэффициента резервирования мощности в ЗСПМ с учётом требований надёжности.

Применительно к рыночной системе развития электроэнергетики отсутствует методология резервирования, основанная на принятых в мировой практике принципах и подходах. Для выбора величины и размещения резервов мощности, даже на этапе планирования развития ЕЭС, необходимо использование не оценочных подходов, а оптимизационных моделей, основанных

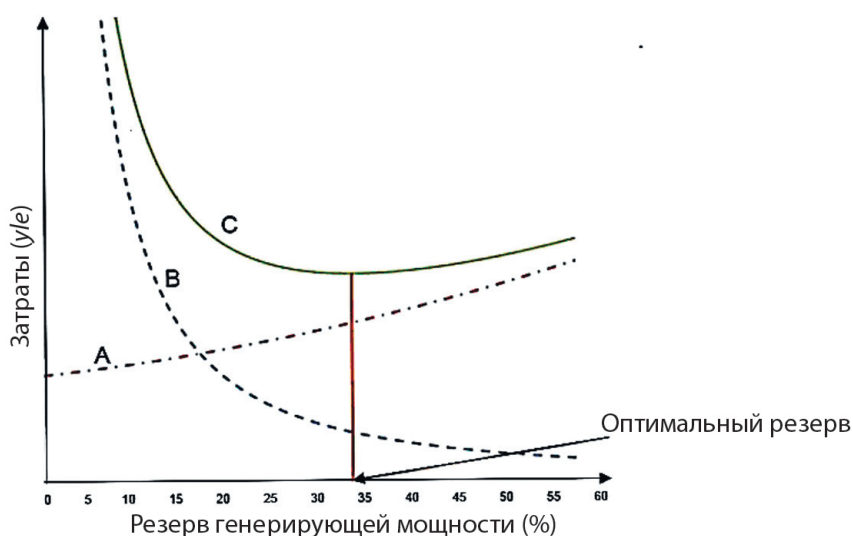


Рис. 1. Выбор оптимального резерва

на использовании вероятностных методов. Поскольку принципы выбора и размещения резервов мощности в России и за рубежом совпадают по основным позициям, то имеющиеся зарубежные разработки для решения рассматриваемой проблемы могут быть использованы в России при условии их адаптации к особенностям российского энергорынка.

Изложенные выше принципы и подходы к резервированию генерирующей мощности и обеспечению надёжности являются в основном традиционными. В настоящее время в условиях развития информационных технологий создаются новые подходы к развитию энергетики на основе современных методов и средств управления, направленных на уменьшение аварийности оборудования, отказов систем управления, на снижение вероятности системных аварий и требуемых резервов генерирующей мощности.

Литература

1. **Billington, Roy and Ronald N. Allan**, "Reliability Evaluation of Power Systems," Second Edition, Plenum Press, New York and London. 1996.
2. ABB, LOLE Resource Adequacy Methodology, Presentation to the New England Installed Capacity Requirement Stakeholder Meeting. November, 18, 2005. http://www.isonewengland.org/committees/comm_wkgrps/othr/icsp/mtrls/2005/nov182005/lole_resource_adequacy_methodology.pdf
3. **Johannes Pfeifenberger, Kathleen Spees, Adam Schumacher**, "A Comparison of PJM's RPM with Alternative Energy and Capacity Market Designs." A report by The Brattle Group prepared for PJM Interconnection. September, 2009.
4. Об электроэнергетике. Федеральный Закон РФ от 26.03.2003 № 35.
5. Концепция обеспечения надёжности в электроэнергетике. М.: Министерство энергетики РФ. 2011. 170 с.
6. О схемах и программах перспективного развития электроэнергетики. Постановление Правительства РФ от 17.10.2009 г. № 823.
7. Методические рекомендации по проектированию развития энергосистем. Приказ Министерства энергетики России от 30.06.03 № 281 (СО 153-34.20.118-2003).
8. Об утверждении Положения о порядке определения величины спроса на мощность для проведения долгосрочного отбора мощности на конкурентной основе на оптовом рынке электрической энергии (мощности) и порядке определения плановых коэффициентов резервирования мощности в зонах (группах зон) свободного перетока электрической энергии (мощности). Приказ Министерства энергетики РФ от 7 сентября 2010 г. N 431.
9. **Руденко Ю.Н., Чельцов М.Б.** Надёжность и резервирование в электроэнергетических системах. Новосибирск: Наука. 1974. 263 с.
10. **Руденко Ю.Н., Ушаков И.А.** Надёжность систем энергетики. Новосибирск: Наука. 1989. 328 с.
11. **Чукреев Ю.Я., Чукреев М.Ю.** Обеспечение надёжности при управлении развитием электроэнергетических систем для условий реформирования электроэнергетики. // Известия РАН. Энергетика. 2008. № 4. С. 39-48.
12. Надёжность систем энергетики и их оборудования. Справочник в 4 т. Т. 2. Надёжность электроэнергетических систем. М.: Энергоатомиздат. 2000. 568 с.
13. **Воропай Н.И., Федотова Г.А.** Планирование ремонтов электрогенерирующего оборудования в рыночной среде с учетом надёжности. // Автоматика и телемеханика. 2010. № 7. С. 179-184.
14. **Fedotova G., Voropai N.** Optimisation of reliability of power supply to consumers. //e-journal "Reliability: Theory & Applications". Vol. 2. June 2007. № 2. P. 57-68. Available: <http://www.gnedenko-forum.org/Journal/index.htm>

Fedotova G.A.

REDUNDANCY AS PART OF THE RELIABILITY PROBLEM IN ELECTRIC-POWER INDUSTRY

The paper is devoted to the problem of redundancy of generating capacities of the Unified Electric Power System (UES) of Russia. The paper has considered approaches to the solution of the problem used during the Soviet period, and now, peculiarities of redundancy in market conditions. General principles for redundancy used in Russia and abroad in a vertically integrated hierarchical structure of electric power management in a market environment are presented in this paper. Recommendations are given for completion of various individual norms regulating the procedure of selection and deployment of redundant capacities in the UES, and for the development of optimization models for solving problems of redundancy in a multiregional power systems association.

Keywords: *electric power engineering, redundancy of power generation capacity, balance dependability, energy market, competitive selection of power.*

Introduction to the problem and basic principles of redundancy

Redundancy is one of the most important means to improve the dependability of power systems at all temporary levels of control of electric power systems (EPS). It provides partial compensation for reduced dependability of EPS arising due to equipment failure, disorders of fuel supply of thermal power-station (TPS) and water supply of hydro power plants (HPP), the deviations of the actual operating conditions of EPS from predictable ones. The problem of determining the optimal size and placement of the power reserves in the united power system (UPS) with limited carrying capacity of intersystem electrical connections is very complex. Despite the fact that this issue has been dealt with more than half a century, to date there is no single standard approach to its solution [1-3]. With a fully centralized management of industry, there is a regulatory authority or regulatory vertically integrated company responsible for the selection and maintenance of redundancy for generating capacity sufficient to provide the required level of dependability. In a market environment, the market itself can decide what level of reserve capacity needed to ensure compliance with dependability regulations and how to deploy it in a power systems association. However, even in these models the redundancy management is not carried out without some kind of administrative interference. In terms of the energy market, approaches to selection and deployment of reserve power in the UPS vary depending on the type and structure of the market.

In electric power systems with a centralized market of power, which includes the UES of Russia, redundancy of generating capacity is accumulated by means of competitive selection of power (CSP),

in accordance with the requirements and regulations of the energy market. The main functions on the formation of the power market rules and requirements to support the dependability of the UES of Russia are performed by the System Operator (SO) (Federal Law # 250 dated 04.11.2007). In conducting competitive power take-off, SO determines the need of power according to market areas and takes off the necessary amount of generating power taking into account constraints of the network capacity ensuring a sufficient level of dependability with the least cost. Basic economic principles to ensure the dependability of electric power systems (EPS) in Russia in the energy market are determined by the Federal Law "On Electric Power Industry" (Article 6, 9, 18, 20, 38, 39 [4]). In accordance with this law, management of dependability and redundancy in electric power industry should be based on the allocation of responsibility for their provision between the entities of relationships and coordination of the liability based on combination of government regulation and market mechanisms. Despite the diversity of approaches used for the power take-off and deployment of generating power redundancy in the world practice, they are all based on the following principles.

1. Redundancy is a technical and economic challenge, which solution is associated with both technical activities and the optimization of power redundancies on the basis of mathematical models. There are two main approaches to solving the problems of optimal redundancy: normative and cost-based ones. The normative approach is based on the selection of a power redundancy value in a power system association and its deployment on electric power systems (EPS) in order to ensure the balance dependability of the regulatory level in the UPS and dependability of consumer power supply. The cost-based approach consists in the optimization of redundancies based on economic criteria, including costs for creation of redundancies and damage from undersupply of electricity to consumers due to power shortage. Since insuring absolute dependability is economically inefficient, then the optimization of power redundancies in the EPS should be a balance between the costs of building and maintaining redundancies and damage to consumers from electricity shortages. Both approaches are used in Russia and abroad.

2. Tasks of redundancy are solved in a mutually coordinated fashion at the planning stages of power industry development and EPS operation. Planning management of the industry development involves the creation of redundancies of rated capacity of EPS and allocation of certain funds for their creation. In the operation of EPS, the redundancies are used for their intended purpose to ensure balance dependability of reliable supply of consumers with electric power of required quality. In this case, as far as redundancies are used effectively in the service conditions, they justify the cost of creating them at the planning stage of development.

3. To determine the optimal value and power redundancy deployment in power systems, estimation and probabilistic approaches are used. In international practice, probabilistic methods and models have a widespread use. They allow one to take into account the accident rate of generating and network equipment, random fluctuations in the load and prediction of its error, interruption of fuel supply, delays in putting new capacities into operation and other random factors affecting dependability.

4. The main difficulty in solving the problems of dependability and redundancy in power systems with limited network capacity of intersystem connections is the consideration of these limitations, time difference of the passage of peak loads and differences in their specific schedules. With regard to the modern conditions of functioning and development of power industry in Russia, the Federal Law "On Electric Power Industry" introduced the concept of free power flow areas (FPFA). The large number of such areas in the UES not always coinciding geographically with regional power systems has complicated the problem of these factors accounting.

With multiregional representation of the power association, the criteria for selecting the size and deployment of the power redundancies used in world practice, as well as the indicators of balance dependability are not adequately substantiated and are, as a rule, empirical. Therefore, to solve the problems of redundancy in Russia, any foreign technique cannot be used in its pure form. The scientifically grounded approach that takes into account the actual state of the industry and modern requirements for dependability, the specific development and operation of EPS in terms of the energy market is necessary. Prior to the reform of industry, there was a hierarchical system of control dependability and power redundancies in the UES. The relationship between producers and consumers of electric power were based on the fulfillment of obligations, regulations and instructions. The transition from a centralized system of management of electric power to the market with the legal and financial liability for the dependability level of all the structures associated with the production, transport, distribution and consumption of electricity, requires a reconsideration of provisioning of electric power generation systems, the revision of approaches to dependability ensuring. The traditional principles of dependability insuring and practice of take-off and employment of reserve generating capacity in the UES existing today in Russia should be corrected in the first place, in terms of criteria for decision-making in market conditions, and the requirements for types and levels of redundancies, with the current state of power plant equipment and electrical power networks taken into account [5].

Selection and deployment of redundancies of generating capacity in the UES of Russia at the planning stage of development of electric power industry

In managing the development of power industry, the problems of the selection and deployment of installed generating capacity of UES redundancies are solved at different time sections:

- when planning the development of electric-power industry (with a lead time of 7-15 years);
- when designing the development of UES (with a lead time of 5-10 years);
- for long-term functioning of the market of power (with a lead time of 4-5 years).

When planning the development of electric-power industry, the General scheme of power generating facilities deployment with details on the integrated power system is formed, and it is adjusted at least once every 3 years. Schemes and programs of UES development, united and regional energy systems determining balanced plans of generating capacity and electrical networks are developed [6]. One of the main problems at this stage is the selection of the quantity of redundancies of installed generating capacity in power systems or in areas of free power flow, providing the balance between production and consumption of electricity and power. The solution of this problem is based on a system of standards, on the indicators of balance dependability, on the carrying capacity of intersystem electrical connections, including those which are needed for the implementation of power redundancies, on fuel stores for a thermal power station, on water stores for a hydropower plant, etc.

To determine the required redundancy of generating capacity at this stage, the value of the required additional capacity in the UES as to the original level of the installed capacity should be estimated. In this case, the deployments of additional generating capacity, its structure and allocation should enable covering the projected load, taking into account the possible excess above the expected value, the ability to carry out scheduled repairs of generating equipment and power compensation derived from work because of total or partial failures. The need to introduce an additional installed capacity is determined by preparing long-term balance of electric power and energy. At the same time, this helps to solve such problems as prediction of load growth and electricity consumption, selection of the optimal structure of

power newly set into operation, the determination of location and its basic parameters, sequence of construction, expansion, renovation and modernization of power plants. Prospective balances of power and energy in the UES are developed in view of conditions of regional energy power system joint operation in the UPS. In the separation of the UES into areas of free power flow, the balance sheets are made for the UES as a whole and for each region, which are then harmonized and specified. The required redundancies of power in regional EPS or free power flow areas (FPFA) are determined with network constraints taken into account. As a result, to meet the overall balance of UES power by technical and economic calculation, decisions are taken on the planning of new generating capacity in EPS and on strengthening of the carrying capacities of intersystem connections.

The values of the required redundancy of power in a power system association in the formation of the General layout of electric power facilities are taken by percentage of the load peaks. They are defined in the Methodological recommendations for the design of power systems development [7].

At the design stage, the degree of uncertainty in demand for electricity and the required increase in installed capacity to meet the demand is reduced due to the reduced lead-time decision making (5-10 years). In these circumstances, the adjustment of the level of the redundancy of generating capacities, power structures, generating redundancy and its spatial location is carried out. This involves checking prospective balance of power and energy, correcting the project of development in case of their violation; refinement of delivered energy volumes and, if necessary, change of their locations, refinement of characteristics of new power plants and network; correction of carrying capacity connections and assessment of the balance dependability level.

The value of power redundancy in power systems at this stage is calculated on the basis of special assessment calculations when considering various emergency situations with the functionality of its components (operational, repair and strategic) taken into account. In this case, the operational redundancy should provide normative dependability of load covering estimated by the probability of deficit-free operation of EPS. Repair redundancy should compensate the reduction of installed capacity of power systems associated with the withdrawal of the generating equipment to scheduled maintenance. Its value is determined by the period of the annual maximum load on the basis of the characteristics and design features of the equipment with the regulations on the frequency and duration of repairs. Strategic redundancy should compensate the imbalance of power because of its unexpected deviations from the prediction, mainly related to the inertia of energy construction and/or to advancing development of adjoining industries.

With the lead-time of 4-5 years during operation of long-term power market, the value and deployment of the power redundancies for FPFA are determined by the Regulations on the procedure for determining the value of demand for power and planned factors of power redundancy in the areas [8]. In accordance with this regulation, the value of demand for power is determined by the product of the projected annual supply of maximum hourly consumption of electricity in the area and the planned factor of redundant power after deduction of volumes of electric energy production by generating facilities that operate in the retail markets. Maximum hourly consumption of electricity in the area is defined by the System Operator based on the forecast of power consumption in the territories of the Russian Federation included in the program of UES development. The System Operator calculates the planned factor of power redundancy for FPFA as the sum of the indicator 1.17, the coefficient of under-utilization of capacity and the coefficient, taking into account the export of electric energy. Predictive factor of under-utilization of power is determined by the ratio of average monthly power reduction due to unscheduled repairs of generating equipment, to the value of the projected peak consumption in the corresponding area.

The current framework for planning power redundancy in Russia's power industry and the used norms regulating the procedure for selection of a value of necessary power redundancy and its deployment in

the UES have been developed for the conditions of the centralized management of the industry [6-8]. In methodical recommendations for the design of power systems [7], the values of operational power redundancy depending on the structure of the installed equipment in electric power stations, its types, and individual power and accident rate, the probable value of deviation of the power balance of power systems from forecast are calculated based on normative values of these indicators taken as early as in the Soviet era. In the Regulation on the procedure for determining the value of demand for power and planned power redundancy factors in FPFA [8], the selection of the planned factor of power redundancy is not based on the direct analysis of balance dependability. These documents need to be improved in terms of the recording of power market functioning and current requirements for dependability. In particular:

1. The method used to divide into FPFAs is not sufficiently justified in terms of selecting the optimal redundancy in areas considering the dependability in case of the implementation of full value competitive take-off of powers.

2. Assignment of common indicator 1.17 to all areas of the market does not provide for the optimal choice of the value and deployment of the power redundancies as to the areas, because this does not take into account the differences of composition and structure of generating power in the areas, single powers and accident rates, relations with other regions and their carrying capacity abilities.

3. The use of valuation approaches in choosing the magnitude of power redundancies in the EPS does not allow taking into account random factors affecting the dependability. This task needs probabilistic methods and models. Such methods were used in the practice of planning the development of energy systems in our country during the Soviet period and are widely used abroad.

Consequently, the practice of selecting and deployment of redundancies of installed capacity, currently prevailing in Russia, does not provide sufficiently optimal solutions in terms of dependability. The methodology used is not economically feasible to determine the value of the power redundancies, taking into account dependability, the new economic conditions of the industry and the current state of the power equipment. The new scientifically reasonable approaches that meet international standards, taking into account the market relations in the industry, the modern forms of management of electric power and dependability requirements [5, 11], are required. They may be based on methods developed in the Soviet period, adapted to modern conditions. The approaches developed and used in the Soviet Union was based on the well-developed fundamental researches and was quite consistent with international standards, but was focused on a vertically integrated power industry with centralized control [9, 10]. In the past 20 years, they have not received the necessary development and practical use.

Statement of tasks for selection and deployment of power redundancies

As noted earlier, the choice of the optimal amount of redundancy and its territorial distribution in the UES of Russia in the areas of free power flow must be based on a compromise between the cost of its creation and support and damage brought to consumers of electric power shortages due to power shortage conditioned by power deficit. Improving the dependability of power systems by creating a redundancy of power requires an increase in reduced costs, including capital and operating costs. In this case the damage to consumers from the undersupply of electricity to consumers is reduced.

In general, the problem of optimizing the power redundancy in EPS consists in selection of such a reserve, which would provide the required dependability at minimum cost. Fig. 1 shows the dependence of the cost on creating and maintaining the power redundancy (A), the damage from short supply of electric power to consumers (B) and total reduced costs, taking into account the damage (C) from the amount

of available redundancy of power. [9] The minimum of the curve of the total costs C corresponds to the optimal level of power redundancy.

The selection criterion for power redundancy in a single power supply system or in a free power flow area can be represented by a functional:

$$C = C_R + M[Y] \rightarrow \min, \quad (1)$$

where C is the reduced cost, C_R is the cost of creating and maintaining the redundancy of generating power in the area, $M[Y]$ is the expectation of damage from the uncertainty of power supply due to power shortage.

The task of selecting and deployment of power redundancies is much more complicated in power systems with poor inter-system connections. Such an association cannot meet the requirements of dependability in case of deficient areas present in its structure, even if the individual power systems or areas of free power flow meet the requirements of dependability or have power excess. The lack of power in deficient areas cannot be covered due to the limited capacity of external links. In order to bring this power system in accordance with the standard of dependability, it is necessary either to introduce additional powers in certain areas, or to strengthen the connection between areas. For this purpose you need to know what connections should be strengthened and in which areas it should be economically feasible to introduce additional powers according to requirements of dependability. To understand the dependence of the dependability level of power systems associations on redundancy volume in the areas and reserves of carrying capacity of inter-system connections, it is necessary to conduct studies to assess the balance dependability of the individual areas and in power systems associations as a whole taking into account the carrying capacities of links. The solution of this problem in condition of power market is associated with great difficulties, especially for large power systems associations, which is the case for the UES of Russia.

To achieve the required level of the balance dependability of a multiregional power system with poor electrical connections as an alternative to an increase in redundancies of generating power in the areas, the corresponding increase of network carrying capacity may be considered. Then the problem of optimal redundancy consists in the simultaneous optimization of redundancy of generating capacity in the areas and reserves of carrying capacity of connections between the areas. The following functional can be used as an optimization criterion:

$$C_{\Sigma} = \sum_{\mu=1}^M C_{R\mu} + \sum_{l=1}^L C_l + \sum_{\mu=1}^M M_{\mu}[Y] \rightarrow \min, \quad (2)$$

where: M is the number of areas in power system, L is the number of links between areas zones, C_{Σ} is the total reduced costs in the power systems association, $C_{R\mu}$ is the cost of creating and maintaining redundancy of generating power in the μ -th area, C_l is the cost of increased carrying capacity of the l -th link, $M_{\mu}[Y]$ is the expectation of loss from uncertainty of power supply to consumers in the μ -th area.

There is a possibility for another approach when the criterion for selection and deployment of redundancy generation capacity consists in the minimum of total discounted costs, including the costs of creating redundancy of generating capacity and the strengthening of links, and the required level of dependability of consumer power supply is given according to limitation of norms. Then the amount of the power redundancy in each area of a multiregional power system will be selected under conditions of

economically reasonable and technically necessary (regulatory) dependability, and selection criteria of power redundancy in power systems and its deployment on FPFA will have the following form:

$$C_{\Sigma} = \sum_{\mu=1}^M C_{R\mu} + \sum_{l=1}^L C_l \rightarrow \min, \pi_{\mu} \geq \pi_{norm}, \quad (3)$$

where π_{μ} and π_{norm} are the calculated value of the dependability index of power supply of consumers in the μ -th area and its normative value, respectively.

Using the criterion (3) for the selection and deployment of redundancy of generating power in the UPS in market conditions allows us to take most comprehensively into account the specifics of the relationship between the subjects of the energy market. With centralized management of power industry in Russia, the deployment of redundancies was based on the collective principle of mutual aid presented by EPS, when not only the redundancy of power, but the power shortage is distributed between power systems. Then the inclusion of the expectation of damage from undersupply of electricity to consumers in the functional (2) was qualified. In the market environment, the power shortage of other EPS cannot be distributed in power systems with excess energy. Each power system in the first place strives for ensuring the necessary level of its own dependability at the lowest cost and gaining maximize profit. Then it strives to fulfill contractual obligations to the adjacent power systems and only after that to give out the excess power to meet the power shortage in other systems on a commercial basis. With this approach, standards of dependability of power supply are required. Attempts to get them were made in the USSR [9], but since that time works in this direction are not carried out, therefore, optimization of redundancies according to the criterion (3) is still problematic.

Use of redundancies of generating power in the operation of EPS

In EPS operation, the issues of use of redundancies in view of their functionality and such properties as mobility and efficiency are of the main significance. At this stage the meaning of the problem consists in refining the redundancy of power in each region of free power flow and its redistribution between areas to provide the required level of dependability in the areas and in power system as a whole with the actual situation in power systems. Such redistribution in current conditions of EPS operation should be carried out through the market of power and system services. At the same time, operating redundancy to cover its own load with the required degree of dependability and repair redundancy to replace the power taken out for planned maintenance and reconstruction in each area should be provided. The close relationship of operational and maintenance components of the power redundancy allows affecting the value of the operational constituent ensuring dependability by optimizing the timing of repairs in the process of planning. Therefore, the task of redistribution of power redundancies should be solved together with the task of planning of generating equipment repairs associated with the reduction of dependability. Joint planning of repair of stations' electrical equipment and networks of inter-system connections provides additional opportunities to improve dependability through the use of system effects [12].

In conditions of the power market, the task of scheduling repairs deserves special attention in the context of the problem of redundancy in the operation of the power system. The separation of ownership and the introduction of market mechanisms in the process of management of electric power have led to the appearance of independent market entities with divergent interests that directly or indirectly affect the approaches to the planning of repairs. Power generating and distributing companies are interested in

maximizing profits from the operation of the equipment installed in power plants and networks under their ownership. Consumers are interested in the minimum price for electricity; the system operator is interested in insuring the required dependability and profit-making, etc. In conditions of the power market, regardless of the selected criteria, the mechanism has to work that allows at the choice of timing of the planned repairs to coordinate the interests of all market participants [13].

Redistribution of redundancies of power generating between FPFA in the UES can be carried out with the help of optimization mathematical models for dependability criteria under the assumption that the amount of available redundancies in areas is defined and economically feasible in the planning stages of development [14]. Depending on the operating conditions and power systems' association and optimization purposes it is possible to use different criteria of dependability, such as the following ones.

- Ensuring equally possible dependability of power supply to consumers in the areas and over time.
- Achieving equal probability of upstate of power systems (in free power flow areas).
- Leveling operating power redundancy between areas and over time in proportion to the load.
- Ensuring maximum possible dependability of power supply to consumers in a power systems association taking into account the standards of dependability in the areas.

At the same time the level of dependability can be estimated by various indicators, including the indicator of the relative provision of electricity to consumers, the probability of upstate of power systems, etc. The selected dependability index should be normalized, it should have a simple physical meaning and be sufficiently sensitive to various disturbances, leading to a decrease in dependability (emergency power reduction, casual load growth, taking out the equipment for repair) and to activities that increase the dependability (putting into operation of new equipment, increasing the carrying capacity of links, redundancy).

Along with the criteria of dependability, theoretically it is possible to find the solution of the problem considered on the basis of cost criteria. Then, through the efficient use of power redundancies, it is possible to provide a minimum of total costs, including the costs for the use and maintenance of power redundancies, the costs for fuel and repairs, as well as damage caused by undersupply of electricity to consumers. Practically, this approach is difficult to implement, and one of the main problems of the use of cost-based criteria is the lack of adequate economic information and/or its inaccessibility. Besides, the prediction of prices for fuel and repair, costs for the maintenance of power redundancies, electricity tariffs and damages from undersupply of electricity to consumers in the power market is a complicated task.

Conclusion

Thus, approaches and methods for selecting and deployment of redundancies generating power of EPS in Russia existing and used today do not meet a modern organizational structure of the industry. At present, the Guidelines for the design of power supply systems based on a common approach to the design of development of power systems, including economic justification redundancy level of installed power, remain in force. These guidelines were developed in 2003 and orientated on a vertically integrated hierarchical structure of the industry with centralized management. Recommended levels of redundancies in the UPS comprising the UES of Russia, due to heavy aging power plants equipment and networks, require further updating.

There is a need to refine the Regulations on the procedure for determining the amount of power demand, selection and deployment of power redundancies in the division of the UES into areas of free power flow and determining the planned factor of the power redundancy in PPFAs to meet the requirements of dependability.

With regard to the market system of power industry development, there is no methodology for power redundancy based on internationally accepted principles and approaches. To select the amount and deployment of the power redundancies even at the planning stage of UES development it is necessary to use not estimating approaches, but optimization models based on probabilistic methods. Since the principles of selection and deployment of power redundancies in Russia and abroad coincide on basic positions, the available international developments to address this issue can be used in Russia under condition of their adaptation to the peculiarities of the Russian power market.

The above stated principles and approaches to redundancy of generating power and ensuring dependability are mostly traditional. At present, under conditions of information technology developments, the new approaches are applied to power systems development based on modern methods and controls aimed at reducing the breakdown rate of equipment, failures of control systems, and the probability of system failures and required redundancies of generating power.

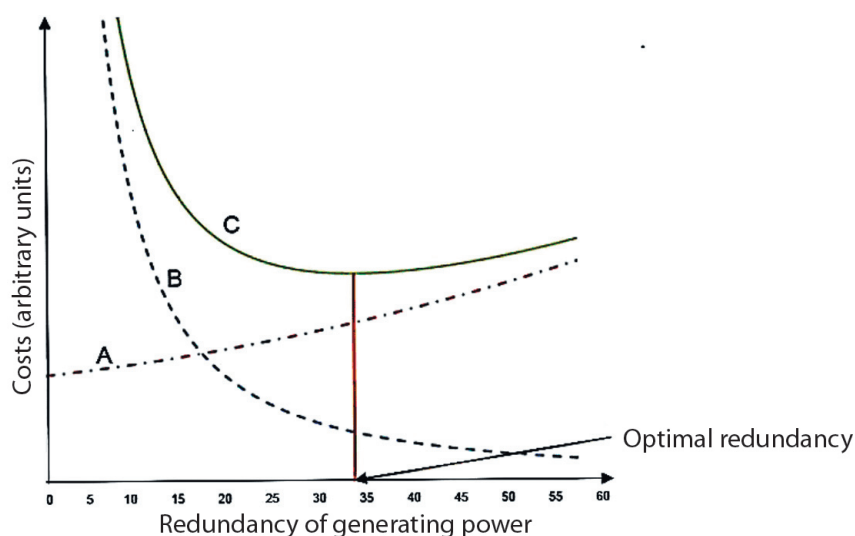


Fig. 1. Selection of optimal redundancy

References

1. **Billington, Roy and Ronald N. Allan.** Dependability Evaluation of Power Systems, Second Edition, Plenum Press, New York and London. 1996.
2. ABB, LOLE Resource Adequacy Methodology, Presentation to the New England Installed Capacity Requirement Stakeholder Meeting. November, 18, 2005. http://www.isonewengland.org/committees/comm_wkgrps/othr/icsp/mtrls/2005/nov182005/lole_resource_adequacy_methodology.pdf
3. **Johannes Pfeifenberger, Kathleen Spees, Adam Schumacher.** A Comparison of PJM's RPM with Alternative Energy and Capacity Market Designs. A report by The Brattle Group prepared for PJM Interconnection. September, 2009.
4. About power industry. Federal Law of the Russian Federation dated 26.03.2003 # 35.
5. The concept of dependability ensuring in power industry. Moscow: Russian Ministry of Energy, 2011. 170.
6. About designs and programs for the long-term development of power industry. Government regulation # 823 dated 17.10.2009.
7. Guidelines for the design of power systems. The Order of the Ministry of Energy of Russia # 281 dated 30.06.03 (SD 153-34.20.118-2003).

8. About approval of the Regulation on the procedure for determining the amount of power demand for long-term power take-off on a competitive basis in the wholesale market of electric power and the procedure for determining the planned coefficients of power redundancy in areas (groups of areas) of free flow of electrical power. The Order of the Ministry of Energy of the Russian Federation # 431 dated September 7, 2010.
9. **Rudenko Yu. N., Cheltsov M.B.** Dependability and redundancy in power systems. Novosibirsk: Nauka. 1974. p. 263.
10. **Rudenko Yu. N. Ushakov I.A.** The dependability of power systems. Novosibirsk: Nauka. 1989. p.328.
11. **Chukreev Yu., Chukreev M. Yu.** Ensuring dependability in managing the development of power systems for the conditions of the power industry reform. // Proceedings of the Russian Academy of Sciences. Energy. 2008. # 4. p. 39-48.
12. The dependability of power systems and their equipment. Reference book vol. 2. The dependability of electric power systems, Energoatomizdat. 2000. 568p.
13. **Voropai N.I., Fedotova G.A.** Planning for repairs of power generation equipment in the market environment, taking into account dependability. // Automation and telemechanics. 2010. # 7. p. 179-184.
14. **Fedotova G., Voropai N.** Optimization of dependability of power supply to consumers. // E-journal "Dependability: Theory & Applications". Vol. 2. June 2007. Number 2. P. 57-68. Available: <http://www.gnedenko-forum.org/Journal/index.htm>

Ададуров С.Е., Мальцев Г.Н., Ададуров А.С.

ДОСТОВЕРНОСТЬ ПЕРЕДАЧИ ОТВЕТСТВЕННЫХ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ СХЕМ ПОРОГОВОЙ ФРАГМЕНТАЦИИ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Исследована достоверность передачи ответственных сообщений управления железнодорожной автоматикой и обеспечением безопасности движения с использованием схем пороговой фрагментации и помехоустойчивого кодирования. Представлена схема реализации рассматриваемого метода передачи формализованных сообщений с выделением внешнего кодирования (формирование фрагментов сообщения по принципу схемы разделения секрета) и внутреннего кодирования (помехоустойчивое кодирование фрагментов). Проанализированы зависимости вероятностей пропуска сообщения и приема ложного сообщения от параметров схемы пороговой фрагментации и помехоустойчивых кодов с обнаружением и исправлением ошибок. Показано, что изменяя соотношение между параметрами внешнего и внутреннего кодирования, можно влиять на соотношение между вероятностями пропуска сообщения и приема ложного сообщения в соответствии с предъявляемыми к ним требованиями при передаче ответственных сообщений.

Ключевые слова: ответственные сообщения, схема пороговой фрагментации, помехоустойчивое кодирование, вероятность необнаруживаемых ошибок, защищенность от несанкционированного доступа.

Введение

В современных условиях управление процессом перевозок на транспорте обеспечивается развитой телекоммуникационной инфраструктурой связи автоматизированных диспетчерских центров (пунктов) управления со стационарными и подвижными абонентами [1]. На железнодорожном транспорте эти функции выполняют системы управления и обеспечения безопасности движения поездами (СУОБДП). Особенностью средств связи, используемых в составе СУОБДП, являются жесткие требования к достоверности передачи так называемых ответственных сообщений – команд управления и формализованных сообщений, непосредственно связанных с управлением железнодорожной автоматикой и обеспечением безопасности движения.

К числу ответственных сообщений относятся команды управления режимами движения и блокировкой перегонов, работой стрелочных участков, переездов и светофоров, а также формализованные сообщения диспетчерского управления подвижным составом. При задании требова-

ний к достоверности передачи таких сообщений наряду с общепринятым показателем – полной вероятностью ошибочного приема сообщения, в ряде случаев учитываются значения отдельных ее составляющих, в частности, вероятностей пропуска сообщения и приема ложного сообщения. При этом требуемые значения этих вероятностей (10^{-8} – 10^{-10} и ниже) соответствуют так называемой квазибезошибочной передаче [2]. Дополнительным требованием является защищенность от несанкционированного доступа к управлению железнодорожной автоматикой и имитации ложных сообщений [3].

Выполнение отмеченных требований в системах радиосвязи, составляющих в настоящее время основу СУОБДП, затруднено действием помех в радиоканалах передачи информации и их электромагнитной доступностью. Это приводит к необходимости разработки методов передачи ответственных сообщений, одновременно обеспечивающих высокую достоверность передачи информации в радиоканалах с помехами (помехоустойчивость) и защищенность от несанкционированного доступа к передаваемым сообщениям (информационную скрытность). В настоящей работе рассматривается один из таких методов, основанный на совместном использовании схем пороговой фрагментации и помехоустойчивого кодирования.

1. Описание метода фрагментированной передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования

Рассматриваемый метод фрагментированной передачи сообщений представляет собой сочетание схем пороговой фрагментации и помехоустойчивого кодирования с обнаружением или исправлением ошибок и позволяет одновременно повысить достоверность передачи сообщений в радиоканалах управления движением подвижного состава с помехами и защищенность от несанкционированного доступа. При этом информационная скрытность обеспечивается за счет преобразований исходного сообщения при фрагментации, передача избыточного числа фрагментов, позволяющего восстановить переданное сообщение по части из них, обеспечивает повышение достоверности при ошибочном приеме отдельных фрагментов, а суммарная вероятность ошибочного приема сообщения и ее составляющие зависят как от параметров помехоустойчивого канального кодирования фрагментов, так и от параметров схемы фрагментации, в соответствии с которой сообщения восстанавливаются по принятым фрагментам.

Используемые для деления передаваемого сообщения на фрагменты схемы пороговой фрагментации являются разновидностью криптографических схем разделения секрета [4]. Основной функцией схем разделения секрета в криптографии является распределенное управление доверием или совместный контроль за критичными действиями пользователей, который осуществляется по принципу участия (согласия) не менее V пользователей из общего их числа W ($V < W$). Схема разделения секрета между W пользователями называется схемой пороговой фрагментации (V, W) , если любая группа из V пользователей может восстановить секрет по имеющимся у них фрагментам (частям) секрета, в то время как никакая группа из меньшего числа пользователей не может получить никакой информации о секрете.

В общем случае схема пороговой фрагментации (V, W) формально задается пятеркой вида $\langle X_W, \Gamma(V), a_0, F, G \rangle$ и включает в себя следующие составляющие:

1. Множество участников схемы или абонентов $X_W = \{x_1, x_2, \dots, x_W\}$.

2. Множество абонентов $Y_Q = \{x_1, x_2, \dots, x_Q\}$, образующих структуру доступа

$$\Gamma(V) : [Y_Q = \{x_1, x_2, \dots, x_Q\} | (x_i \in X_W), (x_i \neq x_j, i \neq j), i = 1, 2, \dots, Q, \\ j = 1, 2, \dots, Q, V \leq Q \leq W].$$

3. Значение секрета a_0 , которое должно быть разделено между всеми участниками схемы.

4. Преобразование разделения секрета F , позволяющее вычислить фрагменты (доли секрета) $b_i, i=1, 2, \dots, W$, которые получают участники схемы в процессе разделения секрета a_0 . При этом $b_i = F(z_i, a_0)$, где z_i – характеристическое число i -го абонента, сопоставляемое ему в процессе разделения секрета.

5. Преобразование восстановления секрета G , позволяющее любому множеству участников $Y_Q = (x_1, x_2, \dots, x_Q) \in \Gamma(V)$, образующих структуру доступа, однозначно восстановить исходное значение секрета $a_0 = G(b_1, b_2, \dots, b_Q, z_1, z_2, \dots, z_Q)$.

Если в криптографии разделение информации на фрагменты используется для разграничения доступа к этой информации, то при передаче сообщений по линиям связи пороговая фрагментация обеспечивает повышение надежности и достоверности передачи. Фрагментация передаваемого сообщения (аналог секрета S_0) осуществляется таким образом, чтобы его можно было восстановить при объединении заданного числа фрагментов. Схема пороговой фрагментации (V, W) означает, что каждое сообщение передается в виде W фрагментов, и для его правильного выделения при приеме необходимо иметь не менее V фрагментов ($V < W$). Предполагается, что используется такой алгоритм формирования W фрагментов сообщения, что при объединении любых V или более неискаженных фрагментов можно однозначно восстановить переданное сообщение, тогда как объединение менее чем V любых неискаженных фрагментов не дает никакой информации о переданном сообщении. Такие схемы разделения секрета с возможностью его однозначного восстановления называются совершенными, и известны условия и доказательства их существования в частных случаях и для общего описания (произвольной структуры доступа) схемы пороговой фрагментации (V, W) [4].

Следует отметить, что в приведенном формальном определении схемы разделения секрета преобразования разделения секрета F и восстановления секрета G однозначно взаимосвязаны, но не симметричны. От этих преобразований зависит структура доступа $\Gamma(V)$, а также совершенство и другие свойства реализуемой с их помощью схемы «разделения секрета», в том числе информационная скрытность. Если фрагментированная передача направлена на предотвращение несанкционированного доступа к передаваемым сообщениям, то для нарушителя алгоритм формирования передаваемых фрагментов сообщений должен быть неизвестен.

Помехоустойчивое кодирование используется в рассматриваемом методе фрагментированной передачи сообщений в традиционном виде [5] канального кодирования фрагментов. Сформированные с использованием схем пороговой фрагментации фрагменты передаваемого сообщения кодируются блочными помехоустойчивыми кодами с обнаружением или исправлением ошибок и передаются по линии связи. При этом могут быть использованы любые (n, k) -коды, параметры которых (n – общее число символов, k – число информационных символов блочного кода) выбираются с учетом известных граничных условий, определяющих взаимосвязь этих параметров с кратностью обнаруживаемых q_o или исправляемых q_u ошибок. Свойством совершенных схем поро-

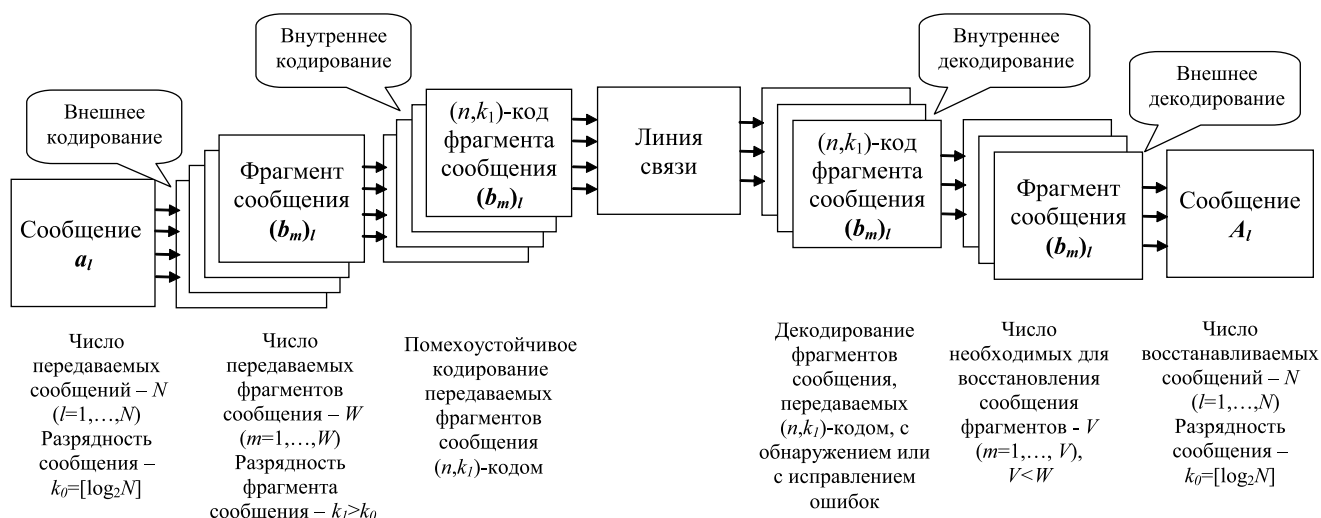


Рис. 1. Схема реализации метода передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования

говой фрагментации является условие, накладываемое на разрядность k_l формируемых фрагментов передаваемого сообщения (секрета). Она не может быть меньше, чем разрядность k_0 исходного сообщения: $k_l \geq k_0$, что обусловлено сложностью преобразований алгоритмов разделения секрета, позволяющих восстановить (выделить при приеме) передаваемое сообщение по меньшему, чем передавалось, числу фрагментов [4].

Схема реализации метода передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования представлена на рис. 1. В этой схеме формирование W фрагментов исходного сообщения a_l , $l=1, \dots, N$, с возможностью его выделения при приеме части фрагментов V ($V < W$) является внутренним кодированием, а кодирование фрагментов $(b_m)_l$, $m=1, \dots, W$, помехоустойчивым кодом – внешним кодированием. Соответственно формирование кодовых слов, соответствующих фрагментам передаваемого сообщения и его восстановление при приеме части фрагментов осуществляется в два этапа.

Первым этапом формирования последовательности кодовых слов, соответствующих фрагментам передаваемого l -го сообщения, является его фрагментация, состоящая в делении секрета на части. На этом этапе в соответствии с используемым алгоритмом разделения секрета формируются W кодовых слов – информационных блоков $(b_m)_l$, $m=1, \dots, W$, соответствующих фрагментам передаваемого сообщения a_l , $l=1, \dots, N$, которые в дальнейшем последовательно передаются по радиоканалу. В общем случае разрядность исходного сообщения a_l , составляет $k_0 = \lceil \log_2 N \rceil$, где $\lceil \cdot \rceil$ означает округление до ближайшего целого в сторону увеличения, а разрядность передаваемых кодовых слов $(b_m)_l$ составляет k_l . В общем случае вследствие отмеченного свойства совершенных схем пороговой фрагментации выполняется $k_l \geq k_0$. Вторым этапом формирования последовательности кодовых слов, соответствующих фрагментам передаваемого i -го сообщения, является помехоустойчивое кодирование сформированных на первом этапе W информационных блоков $(b_m)_l$, $m=1, \dots, W$, блочным помехоустойчивым (n, k_l) -кодом, после чего все они передаются по линии связи.

При приеме сообщений на первом этапе осуществляется декодирование последовательности блочных (n, k_l) -кодов с обнаружением или исправлением ошибок и выделение передаваемых информационных блоков $(b_m)_l$. На втором этапе по выделенным фрагментам $(b_m)_l$ в соответствии с используемым алгоритмом разделения секрета осуществляется восстановление переданного сообщения a_l . Правильное восстановление сообщения возможно при правильном приеме V и более фрагментов, причем $V < W$.

В дальнейшем будем полагать, что передаваемые фрагменты сообщения имеют разрядность $k=k_0=k_I$. Соответствующие схемы пороговой фрагментации называются идеальными, их существование определяется частными условиями идеальности конкретных преобразований разделения секрета F . Свойство идеальности позволяет передавать фрагменты сообщения с минимально возможным введением избыточности и с точки зрения затрат времени делает фрагментированную передачу эквивалентной обычному повторению сообщений. Частные условия идеальности связаны с наложением ограничений на разрядность передаваемых сообщений и параметров (коэффициентов), используемых при преобразовании разделения секрета. Кроме того, могут быть найдены более мягкие условия почти идеальных преобразований разделения секрета, для которых $k_I=k_0+1$.

2. Исследование достоверности фрагментированной передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования

Рассмотрим общий случай фрагментированной передачи сообщений с использованием схемы пороговой фрагментации (V, W) и помехоустойчивого кодирования фрагментов (n, k) -кодом, обнаруживающим q_o ошибок или исправляющим q_u ошибок. Взаимосвязь параметров помехоустойчивого кода n и k с кратностями гарантированно обнаруживаемых q_o и исправляемых q_u ошибок задается известной границей Хемминга [5]. При фиксированных n и k всегда выполняется $q_o > q_u$.

Исходной характеристикой линии связи, характеризующей условия передачи информации, является вероятность ошибочного приема информационного символа p_0 [2]. Достоверность передачи отдельных фрагментов помехоустойчивыми кодами в общем случае характеризуется вероятностями правильного приема P_{nn} , обнаруживаемой P_{oo} и необнаруживаемой $P_{но}$ ошибок.

При помехоустойчивом кодировании фрагментов (n, k) -кодом с обнаружением ошибок вероятности обнаруживаемой и необнаруживаемой ошибок определяются выражениями

$$P_{oo} = \sum_{i=1}^{q_o} C_n^i p_0^i (1-p_0)^{n-i}, \quad (1)$$

$$P_{но} = \sum_{i=q_o+1}^n C_n^i p_0^i (1-p_0)^{n-i}, \quad (2)$$

а вероятность правильного приема составляет: $P_{nn} = 1 - P_{oo} - P_{но}$.

При помехоустойчивом кодировании фрагментов (n, k) -кодом с исправлением ошибок возможны только необнаруживаемые ошибки. Вероятность необнаруживаемой ошибки определяется выражением

$$P_{но} = \sum_{i=q_u+1}^n C_n^i p_0^i (1-p_0)^{n-i}, \quad (3)$$

а вероятность правильного приема составляет: $P_{nn} = 1 - P_{но}$.

Выражения (1)–(3) соответствуют биномиальной модели ошибок в передаваемых фрагментах сообщений [5]. Определяемые с их помощью вероятности P_{oo} и $P_{но}$ и являются исходными для расчета показателей достоверности фрагментированной передачи сообщений с использованием схем пороговой фрагментации (V, W) . В качестве таких показателей будем рассматривать вероятность пропуска (недоставки) сообщения P_{np} и вероятность приема (выделения) ложного сообщения $P_{лс}$. Данные вероятности являются составляющими полной вероятности ошибочного приема сообщения и характеризуют наиболее опасные виды ошибок при передаче ответственных сообщений, связанных с управлением железнодорожной автоматикой и обеспечением безопасности движения.

Используя изложенную в работе [6] методику анализа процесса последовательной передачи по линии связи с помехами и выделения в приемном пункте фрагментов сообщения, сформированных с использованием схемы пороговой фрагментации (V, W) , получаем общие выражения для вероятностей пропуска сообщения и приема ложного сообщения:

$$P_{np} = \sum_{i=W-V+1}^W C_W^i (P_{oo} + P_{но})^i (1 - P_{oo} - P_{но})^{W-i}, \quad (4)$$

$$P_{лс} = \frac{P_{но}^V}{N^{V-1}} \left[1 + \sum_{i=1}^{W-V} C_{V+i-1}^i \left(1 - \frac{P_{но}}{N} \right)^i \right]. \quad (5)$$

Выражения (4) и (5) соответствуют помехоустойчивому кодированию фрагментов (n, k) -кодом как с обнаружением, так и с исправлением ошибок. В случае обнаружения ошибок вероятности P_{oo} и $P_{но}$ определяются выражениями (1) и (2) для кратности обнаруживаемых ошибок q_o . В случае исправления ошибок вероятность $P_{но}$ определяется выражением (3) для кратности исправляемых ошибок q_u , а вероятность P_{oo} полагается равной нулю $P_{oo}=0$.

Используя выражения (4) и (5) с учетом выражений (1) – (3) можно получить зависимости вероятностных характеристик достоверности фрагментированной передачи сообщений P_{np} и $P_{лс}$ от

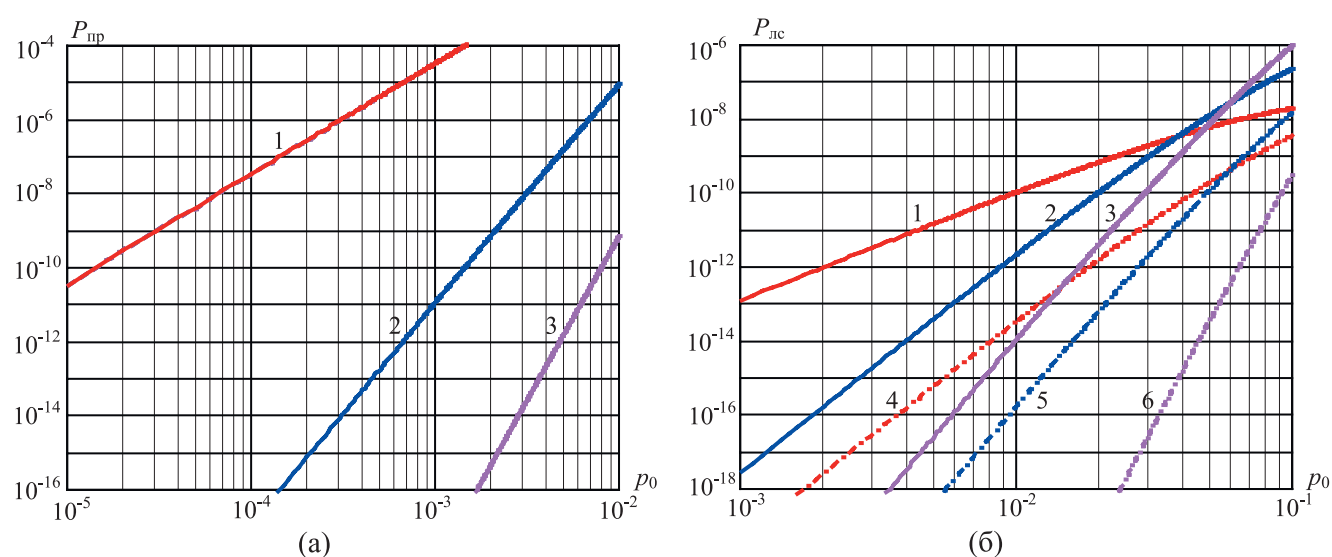


Рис. 2. Зависимости вероятностей пропуска сообщения (а) и приема ложного сообщения (б) от вероятности ошибочного приема информационного символа для схемы пороговой фрагментации (3,5) при использовании различных помехоустойчивых кодов

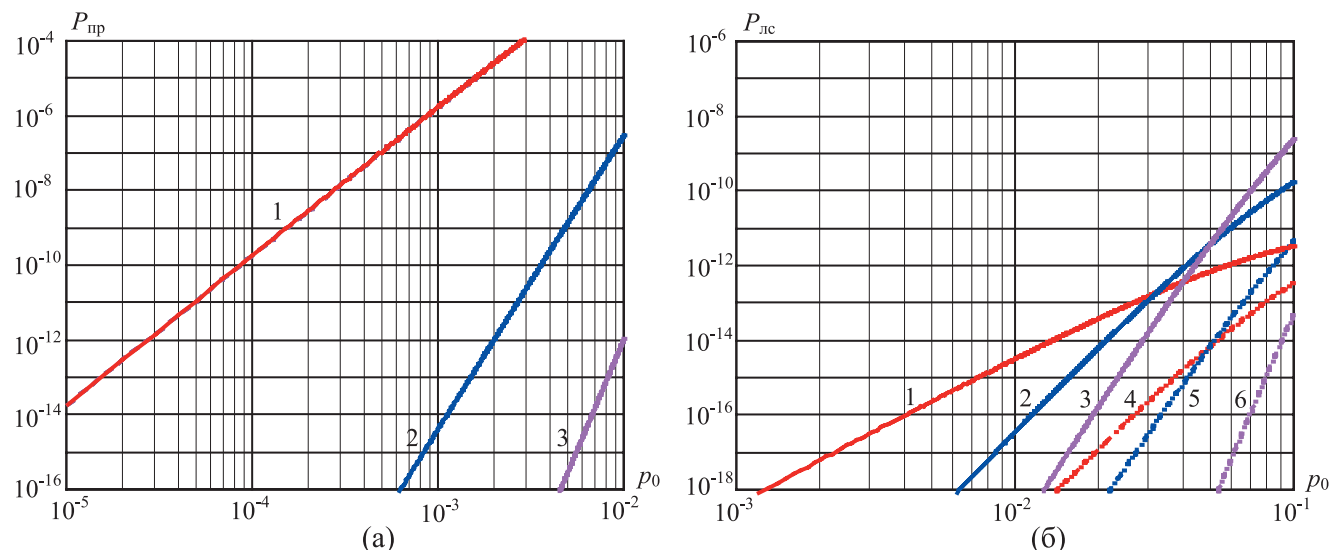


Рис. 3. Зависимости вероятностей пропуска сообщения (а) и приема ложного сообщения (б) от вероятности ошибочного приема информационного символа для схемы пороговой фрагментации (4,7) при использовании различных помехоустойчивых кодов

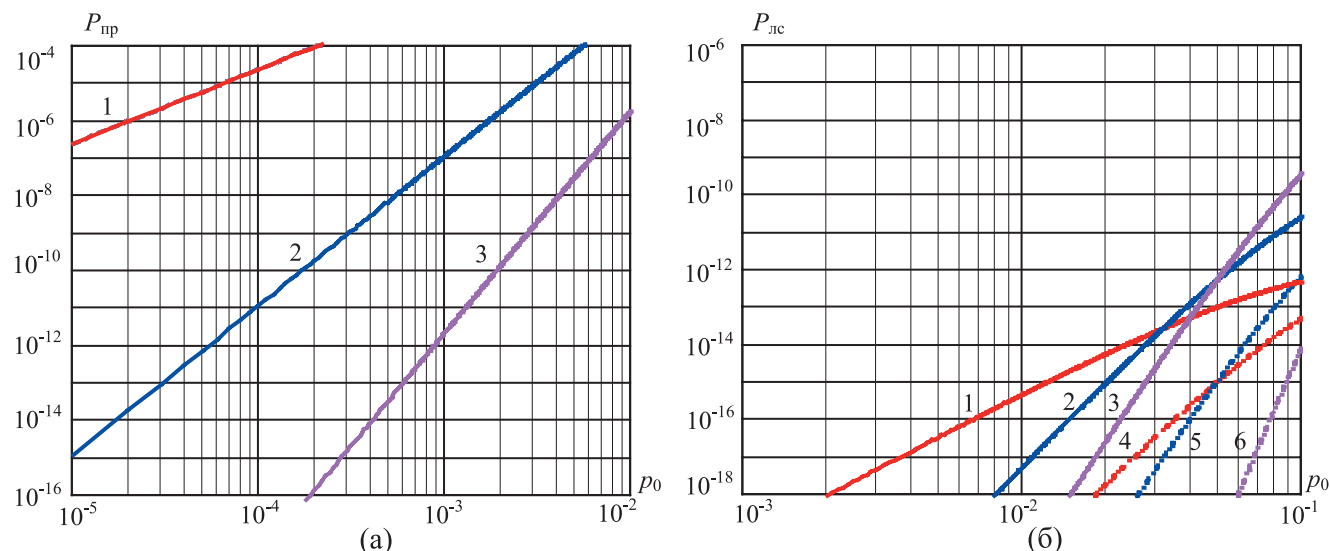


Рис. 4. Зависимости вероятностей пропуска сообщения (а) и приема ложного сообщения (б) от вероятности ошибочного приема информационного символа для схемы пороговой фрагментации (4,5) при использовании различных помехоустойчивых кодов

вероятностей ошибочного приема информационного символа в канале передачи информации p_0 и параметров схемы пороговой фрагментации (V, W) для различных (n, k) -кодов, используемых для передачи информационных блоков. Практический интерес представляет определение при заданных условиях связи параметров внешнего (схемы фрагментации) и внутреннего (помехоустойчивого кода) кодирования, обеспечивающих требуемые значения вероятностей пропуска сообщения $P_{пр}$ и приема ложного сообщения $P_{лс}$, что позволяет выбирать параметры схемы фрагментации и помехоустойчивого кода, обеспечивающие минимизацию одной из вероятностей $P_{пр}$ и $P_{лс}$ при максимально допустимых значениях другой вероятности.

На рис. 2–4 приведены результаты расчетов вероятностей пропуска сообщения $P_{пр}$ и приема ложного сообщения $P_{лс}$ в зависимости от вероятности ошибочного приема информационного символа p_0 при использовании схемы пороговой фрагментации с различными параметрами V и W

и помехоустойчивых (n,k) -кодов с различными значениями параметров q_o и q_u . Рассматривались следующие помехоустойчивые коды: код с проверкой на четность (15,14) с кодовым расстоянием $d=2$ с кратностью обнаруживаемых ошибок $q_o=1$ и с кратностью исправляемых ошибок $q_u=0$, код Хэмминга (15,11) с кодовым расстоянием $d=3$ с кратностью обнаруживаемых ошибок $q_o=2$ и с кратностью исправляемых ошибок $q_u=1$, циклический код (15,8) с кодовым расстоянием $d=5$ с кратностью обнаруживаемых ошибок $q_o=4$ и с кратностью исправляемых ошибок $q_u=2$. На рис. 2 приведены зависимости P_{np} (а) и $P_{лс}$ (б) от p_0 для схемы пороговой фрагментации (3,5), на рис. 3 – зависимости P_{np} (а) и $P_{лс}$ (б) от p_0 для схемы пороговой фрагментации (4,7), на рис. 4 – зависимости P_{np} (а) и $P_{лс}$ (б) от p_0 для схемы пороговой фрагментации (4,5). На рис. 2а, 3а, 4а кривые 1 соответствуют коду (15,14) при $q_u=0$ и $q_o=1$, коду (15,11) при $q_o=2$ и коду (15,8) при $q_o=4$, кривые 2 – коду (15,11) при $q_u=1$, кривые 3 – коду (15,8) при $q_u=2$. На рис. 2б, 3б, 4б кривые 1 соответствуют коду (15,14) при $q_u=0$, кривые 2 – коду (15,11) при $q_u=1$, кривые 3 – коду (15,8) при $q_u=2$, кривые 4 – коду (15,14) при $q_o=1$, кривые 5 – коду (15,11) при $q_o=2$, кривые 6 – коду (15,8) при $q_o=4$. Величина N , от которой зависит вероятность $P_{лс}$, определялась в виде $N=2^k$.

Совпадение кривых, соответствующих различным вариантам использования помехоустойчивых кодов с обнаружением ошибок обусловлено тем, что на величину вероятности пропуска сообщения P_{np} в соответствии с выражением (4) влияет сумма вероятностей обнаруживаемых P_{oo} и необнаруживаемых $P_{но}$ ошибок при передаче каждого фрагмента, которая для $q_o \geq 1$ оказывается одинаковой для всех вариантов использования помехоустойчивых кодов с обнаружением ошибок. На величину вероятности приема ложного сообщения $P_{лс}$ в соответствии с выражением (5) влияет величина вероятности необнаруживаемых ошибок $P_{но}$ при передаче каждого фрагмента, которая различается для всех рассматриваемых помехоустойчивых кодов и вариантов их использования для обнаружения и исправления ошибок.

Анализ приведенных зависимостей показывает, что рассмотренный метод фрагментированной передачи сообщений даже при достаточно большой вероятности ошибочного приема информационного символа в канале передачи информации ($p_0=10^{-2}$ - 10^{-4}) и при небольших значениях параметров схемы фрагментации V и W и за счет обнаружения и исправления ошибок и повторных передач обеспечивает достижение малых вероятностей пропуска сообщения P_{np} и приема ложного сообщения $P_{лс}$ на уровне до 10^{-12} - 10^{-16} . Значения P_{np} уменьшаются с увеличением q_u , значения $P_{лс}$ уменьшаются с увеличением q_o и q_u .

Семейства зависимостей на рис. 2 и рис. 3 соответствуют заданию параметров схемы фрагментации V и W , удовлетворяющих соотношению $V=[W/2]$, где $[\cdot]$ означает округление до ближайшего целого в сторону увеличения. В этих условиях при увеличении параметров схемы фрагментации V и W и сохранении соотношения между ними значения вероятностей P_{np} и $P_{лс}$ уменьшаются с увеличением V и W , причем всегда выполняется соотношение $P_{лс} < P_{np}$, поэтому при уменьшении вероятности пропуска сообщения одновременно уменьшается и вероятность приема ложного сообщения. При увеличении значений параметров схемы фрагментации V и W имеет место тенденция насыщения на некотором уровне значений вероятности пропуска сообщения P_{np} . Так, значения P_{np} для схемы (4,7) заметно ниже, чем значения P_{np} для схемы (3,5), но ненамного превышают значения P_{np} для схемы (5,8). В то же время значения вероятности приема ложного сообщения $P_{лс}$ при увеличении параметров схемы фрагментации V и W уменьшаются без какой-либо тенденции к насыщению. Как следует из выражения (5), величина $P_{лс}$ также уменьшается с увеличением числа передаваемых сообщений N . При этом в области больших значений вероятности ошибочного приема информационного символа p_0 влияние величины N на вероятность приема ложного сообщения $P_{лс}$ более заметное, чем влияние величин q_o и q_u . С уменьшением значений p_0 это влия-

ние практически исчезает и основным фактором, влияющим на величину $P_{лс}$ при фиксированном значении p_0 , является кратность обнаруживаемых q_o и исправляемых q_u ошибок при передаче фрагментов сообщения.

Семейства зависимостей на рис. 2 и рис. 4 соответствуют такому заданию параметров схемы фрагментации V и W , когда зафиксирован параметр W и увеличивается параметр V . В этих условиях с увеличением V одновременного уменьшения вероятностей P_{np} и $P_{лс}$ не происходит – вероятность P_{np} увеличивается, а вероятность $P_{лс}$ уменьшается, причем даже при увеличении параметра V на единицу и при фиксированном значении параметра W происходит заметное увеличение вероятности пропуска сообщения P_{np} и уменьшение вероятности приема ложного сообщения $P_{лс}$. Следовательно, изменяя соотношение между параметрами схемы фрагментации V и W можно влиять на соотношение между вероятностями P_{np} и $P_{лс}$ в соответствии с предъявляемыми к ним требованиями при передаче ответственных сообщений.

Следует отметить, что величина вероятности пропуска сообщения, определяемая выражением (4) совпадает с вероятностью пропуска сообщения при W -кратной передаче нефрагментированного сообщения и принятии решения по V совпадениям [7]. С точки зрения повышения достоверности передачи информации за счет введения при повторениях в передаваемые сообщения избыточности это эквивалентно использованию идеальной схемы пороговой фрагментации (V, W). Однако передача сообщений с простым повторением предполагает использование одной ступени кодирования, которое может обеспечивать только обнаружение или исправление ошибок за счет корректирующих способностей используемого помехоустойчивого кода, что соответствует внешнему кодированию фрагментов при фрагментированной передаче. Возможностями обеспечения информационной скрытности передаваемых сообщений многократная передача сообщений не обладает.

Заключение

Метод фрагментированной передачи ответственных сообщений анализировался, прежде всего, применительно к его использованию в системах радиосвязи, функционирующих в условиях помех и электромагнитной доступности. Повышение достоверности передачи сообщений достигается за счет введения значительной избыточности, связанной с многократной передачей фрагментов сообщения, эквивалентной по затратам времени их повторению. Однако при передаче формализованных сообщений управления движением и железнодорожной автоматикой, являющихся, по сути, малоинформативными, значительное введение избыточности вполне оправдано. Это, во-первых, позволяет достигнуть малых значений вероятностей пропуска сообщения и приема ложного сообщения (10^{-12} - 10^{-16}) в радиоканалах низкого качества с вероятностью ошибочного приема информационного символа 10^{-2} - 10^{-4} , во-вторых, одновременно повысить достоверность передачи сообщений в радиоканалах с помехами и защищенность от несанкционированного доступа

Помимо возможности использования в системах радиосвязи, рассмотренный метод хорошо согласуется с используемыми на железнодорожном транспорте технологиями передачи на подвижной состав сообщений (команд) сигнализации по тональным рельсовым цепям или с помощью расположенных между рельсами точечных радиопередатчиков (eurobalise) [6]. Обе технологии предполагают привязку передаваемых сообщений к прохождению подвижным составом так называемых блок-участков, на каждом из которых может передаваться один из фрагментов очередного сообщения.

Литература

1. Кудряшов В.А., Моченов А.Д. Транспортная связь. – М.: Маршрут, 2005. – 294с.
2. Тепляков И.М. Основы построения телекоммуникационных систем и сетей. – М.: Радио и связь, 2004. – 328 с.
3. Мальцев Г.Н., Ададунов А.С. Снижение угроз информационной безопасности систем радиосвязи // Автоматика. Связь. Информатика. – 2011. – №5. – С.22-24.
4. Введение в криптографию / В.В.Яценко, Н.П.Варновский, Ю.В.Нестеренко и др.; Под ред. В.В. Яценко. – М.:МЦНМО. – 1998. – 272 с.
5. Вернер М. Основы кодирования: Пер с нем.– М.: Техносфера, 2008.–288 с.
6. Яковлев В.А., Ададунов А.С. Способ безопасной передачи данных на локомотив на основе принципа «разделения секрета» с использованием дополнительных каналов // Надежность. – 2012. – №4. – С.95-104.
7. Мальцев Г.Н., Чернявский Е.В. Кодирование сообщений в системах радиопередачи без обратного информационного канала // Информационно-управляющие системы. – 2011. – №4. – С. 60-65.

Adadurov S.E., Maltsev G.N., Adadurov A.S.

ACCURACY OF VITAL MESSAGES TRANSMISSION USING THRESHOLD FRAGMENTATION METHODS AND ANTINOISE CODING

The paper studied the accuracy of transmission of vital messages for railway signalling and train controls systems using threshold fragmentation methods and antinoise coding. A scheme for the implementation of the transmission method of formalized messages with allocation of outer coding (generation of messages based on the principle of secret sharing) and internal coding (antinoise coding of fragments) is presented. The dependences of the probabilities of missing messages and receipt of a false report from the parameters of the fragmentation threshold scheme and antinoise coding with error detection and their correction are analyzed. It is shown that by changing the relation between the parameters of the external and internal encoding we can affect the relationship between the probability of missing a message and receiving a false report in accordance with the requirements made for the transmission of vital messages.

Keywords: *vital messages, threshold fragmentation method, antinoise coding, the probability of undetected errors, protection against unauthorized access.*

Introduction

Under present-day conditions, transportation process management is provided by advanced telecommunications infrastructure of centralized traffic control (CTC) centers with stationary and mobile users [1]. In rail transport, these functions are performed by automatic train control and train protection systems (ATC/ATP). Communication facilities used in ATC/ATP systems feature strict requirements for the accuracy of transmission of the so-called vital messages, i.e. command and control messages that are directly related to the management of railway automation and train safety.

Vital messages include commands for control of train movement and line blocking, operation of switch sections, crossings and signal lights as well as formalized messages of rolling stock dispatcher control. When we specify the requirements for the accuracy of transmission of vital messages, along with the generally accepted indicator, i.e. the total probability of erroneous reception of messages, in some cases we take into account the values of its individual components, in particular the probability of missing a vital message and receiving a false message. And the required values of these probabilities (10^{-8} - 10^{-10} and lower) correspond to the so-called quasi-error-free transmission [2]. An additional requirement is the protection against unauthorized access to railway signaling control and simulation of false messages [3].

Implementation of the requirements mentioned in the radio communication systems currently constituting the base of ATC/ATP systems is complicated by interference in radio channels of communication and their electromagnetic availability. This leads to the need to develop methods of vital messages transmission which both ensure the high accuracy of data transmission via radio channels with interference (noise immunity) and the protection against unauthorized access to messages (information security). In this paper we consider one such method based on the combined use of fragmentation threshold schemes and antinoise coding.

1. Description of the method of fragmented transmission of messages using threshold fragmentation schemes and antinoise coding

The considered method of fragmented message transmission is a combination of fragmentation threshold schemes and antinoise coding with error detection or error correction, and it can increase the accuracy of message transmission via train control radio channels with noise as well as the protection against unauthorized access. In this case, the information security is insured by transformation of the original message in the process of fragmentation. The transmission of the excess number of fragments, which allows to recover the transmitted message using only some of them, provides the increase of the accuracy of message transmission in case of the erroneous reception of individual fragments, and the overall probability of erroneous reception of a message and its components depends on the antinoise channel coding of fragments and the parameters of a fragmentation scheme, according to which the message is restored on the basis of the received fragments.

The schemes of threshold fragmentation used to divide a transmitted message into fragments are a type of cryptographic secret sharing schemes [4]. The main function of secret sharing schemes in cryptography is a distributed management of confidence or joint control over the vital actions of users, which is carried out on the principle of participation (consent) of at least V users out of their total number W ($V < W$). The scheme of secret sharing between W users is called a scheme of threshold fragmentation (V, W), if any group of V users can recover the secret according to available fragments (parts of a secret), while no group of a smaller number of users can get any information about the secret.

Generally, the threshold fragmentation scheme (V, W) formally is specified by a set of five users of the type $\langle X_W, \Gamma(V), a_0, F, G \rangle$ and includes the following components:

1. The set of scheme participants or subscribers $X_W = \{x_1, x_2, \dots, x_W\}$.
2. The set of subscribers $Y_Q = \{x_1, x_2, \dots, x_Q\}$, forming the access structure

$$\Gamma(V): [Y_Q = \{x_1, x_2, \dots, x_Q\} | (x_i \in X_W), (x_i \neq x_j, i \neq j), i = 1, 2, \dots, Q, \\ j = 1, 2, \dots, Q, V \leq Q \leq W].$$

3. The value of the secret a_0 , which is to be shared among all the members of the scheme.
4. The transformation of secret sharing F allowing to calculate the fragments (secret shares) $b_i, i=1, 2, \dots, W$, which is received by the participants of the scheme in the process of sharing the secret a_0 . In this case $b_i = F(z_i, a_0)$, where z_i is a characteristic number of the i -th subscriber correlated to him during the process of secret sharing.

5. The transformation of secret recovery G , which allows any set of the participants $Y_Q = (x_1, x_2, \dots, x_Q) \in \Gamma(V)$ forming the structure of access to unambiguously recover the original secret value a_0 . In this case $a_0 = G(b_1, b_2, \dots, b_Q, z_1, z_2, \dots, z_Q)$.

If in cryptography the fragmentation of information is used to restrict access to this information, for transmission of messages via communication links, threshold fragmentation provides higher reliability and accuracy of message transmission. The fragmentation of a transmitted message (secret analog S_0) is performed so that it can be restored by combining a predetermined number of fragments. A threshold fragmentation scheme (V, W) means that each message is transmitted in the form of W fragments, and to sort it out in a proper way when receiving you should have at least V ($V < W$) fragments. It is assumed that we use such an algorithm for the formation of W message fragments that when combining all V or more undistorted fragments we can uniquely reconstruct the transmitted message, whereas the combination of less than V of any undistorted fragments do not give any information about the transmitted message. Such secret sharing schemes with the possibility of their unique reconstruction are called perfect, and we know the conditions and the evidence of their existence in particular cases and for the general description (arbitrary access structures) of a threshold fragmentation scheme (V, W) [4].

It should be noted that in the above formal definition, the schemes of secret sharing, the transformation of secret sharing F and the recovery of secret G are unambiguously interrelated, but not symmetrical. The structure of access $\Gamma(V)$ as well as perfection, and other properties implemented by the "secret sharing" scheme, including information secrecy, depend on these transformations (conversions). If fragmented transmission is designed to prevent unauthorized access to transmitted messages, then the algorithm for the generation of transmitted message fragments must be unknown to an intruder.

Antinoise coding is used in this method of fragmented message transmission in the traditional form [5] of channel coding fragments. Fragments of a transmitted message generated using threshold fragmentation schemes are encoded by block noise-resistant codes with error detection or error correction and transmitted over the link. There may be used any (n, k) -codes, which parameters (n is the total number of characters, k is the number of data symbols of a block code) are selected based on the known boundary conditions defining the relationship between these parameters and the multiplicity of detected q_o , or corrected errors q_u . The property of perfect threshold fragmentation is the condition imposed on the number of digits k_l of the generated fragments of a transmitted message (secret). It can not be less than the number of digits of the original message k_0 : $k_l \geq k_0$, due to the complexity of transformations of secret sharing algorithms that enable to restore (select when receiving) a transmitted message by a smaller number fragments than it was transmitted [4].

The scheme of implementation of the method of message transmission using a threshold fragmentation scheme and antinoise coding is shown in Fig. 1. In this scheme, the generation of W fragments of the original message a_l , $l = 1, \dots, N$, with the possibility of its selection upon receipt of fragments share V ($V < W$), is inner coding, and the coding of fragments $(b_m)_l$, $m = 1, \dots, W$ using antinoise code is external coding. Accordingly, the generation of code words corresponding to fragments of a transmitted message and its restoration at the reception of a fragments share is carried out with two stages.

The first stage in generating the sequence of code words corresponding to the fragments of a transmitted l -th message consists in its fragmentation corresponding in terms of secret sharing to secret partition. At this stage in accordance with the applied secret sharing algorithm, W code words are generated, which are information blocks $(b_m)_l$, $m = 1, \dots, W$, corresponding to the fragments of a transmitted message a_l , $l = 1, \dots, N$, which are then serially transmitted via radio channel. In the general case the number of digits of the original message a_n makes up $k_0 = \lceil \log_2 N \rceil$, where $\lceil \cdot \rceil$ means rounding upward to the nearest integer,

and the number of digits of transmitted code words $(b_m)_l$ makes up k_l . In the general case, due to the marked property of perfect schemes of threshold fragmentation, the condition $k_l \geq k_0$ is satisfied. The second stage in generating the sequence of code words corresponding to the fragments of a transmitted i -th message is antinoise coding of W information blocks $(b_m)_l$, $m=1, \dots, W$ generated at the first stage, by using block noise-immune (n, k_l) -code, with all them being further transmitted via communication lines.

When receiving messages, the decoding of a sequence of block (n, k_l) -codes is carried out at the first stage, with error detection or error correction, and the selection of transmitted data blocks $(b_m)_l$ is performed. At the second stage, the restoration of a sent message is performed using selected fragments $(b_m)_l$, according to the applied algorithm of secret sharing. The proper restoration of messages is possible when V and more fragments are correctly received, with $V < W$.

In what follows we assume that the fragments of a transmitted message have the following number of digits $k=k_0=k_l$. The relevant schemes of threshold fragmentation are called ideal; their existence is determined by the particular conditions of ideality of specific transformations of secret sharing F . The property of ideality allows us to send the fragments of a message with the lowest possible introduction of redundancy and, in terms of time spent, makes fragmented transmission as equivalent to conventional repetition of messages. Specific conditions of ideality are associated with the imposition of restrictions on the number of digits of a transmitted messages and the parameters (coefficients) used in the transformation of secret sharing. Furthermore, there may be found more soft conditions of a nearly ideal transformation of secret sharing, for which $k_l = k_0 + 1$.

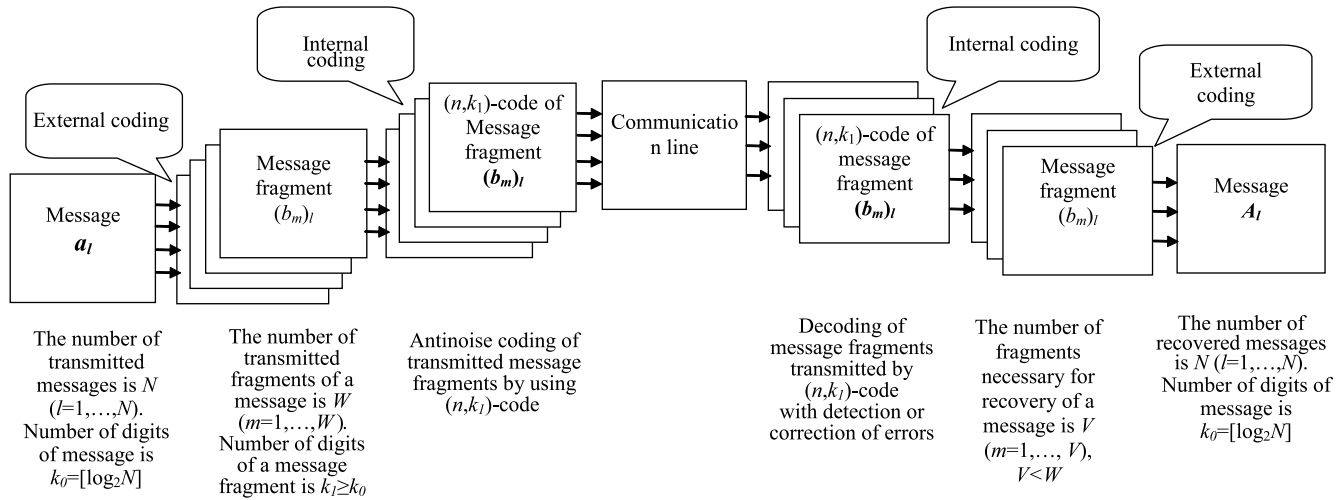


Fig. 1. The scheme of implementation of the method for transmission of messages using the scheme of threshold fragmentation and antinoise coding

2. Study of the accuracy of fragmented transmission of messages using schemes of threshold fragmentation and antinoise coding

Let us consider the general case of fragmented transmission of messages using a scheme of threshold fragmentation (V, W) and antinoise coding of fragments by (n, k) -code that detects q_o errors or corrects q_u errors. Interconnection of parameters of the noise-immune code n and k with multiplicities of known detected and corrected errors q_o , is given by the well-known Hamming boundary [5]. For fixed n and k , the following expression $q_o > q_u$ is always met.

The baseline characteristic of a communication line, which describes the conditions for information transmission, is the probability of erroneous reception of an information symbol p_0 [2]. The accu-

racy of the transmission of individual fragments by noise-immune codes is generally characterized by the probability of correct reception P_{nn} , the probability of detectable errors P_{oo} and undetectable errors P_{ho} .

In case of antinoise coding of fragments by (n,k) -code with error detection, the probabilities of detectable and undetectable errors are defined by the following expressions:

$$P_{oo} = \sum_{i=1}^{q_o} C_n^i p_0^i (1-p_0)^{n-i}, \quad (1)$$

$$P_{ho} = \sum_{i=q_o+1}^n C_n^i p_0^i (1-p_0)^{n-i}, \quad (2)$$

and the probability of correct reception makes up: $P_{nn} = 1 - P_{oo} - P_{ho}$.

In case of antinoise coding of fragments by (n,k) -code with error correction, only detectable errors are possible, and the probability of undetected error is defined by the following formula:

$$P_{ho} = \sum_{i=q_u+1}^n C_n^i p_0^i (1-p_0)^{n-i}, \quad (3)$$

and the probability of correct reception makes up: $P_{nn} = 1 - P_{ho}$.

Equations (1)–(3) correspond to the binomial model of errors in the fragments of transmitted messages [5]. It is the probabilities P_{oo} and P_{ho} defined with their help that are the starting point for the calculation of indicators for the accuracy of fragmented transmission of messages using the schemes of threshold fragmentation (V, W) . As these indicators, we will consider the probability of missing (non-delivering) a message P_{np} and the probability of receiving (sorting out) a dummy message. These probabilities are the constituents of the total probability of erroneous reception of a message and characterize the most dangerous types of errors in the transmission of vital messages related to the control of railway automation and train safety operation.

Using the methodology presented in [6] for analyzing the process of serial transmission via communication lines with interference and selection in a reception centre of message fragments generated with the help of the scheme of threshold fragmentation (V, W) , we obtain the general expression for the probability of missing messages and receiving a false message:

$$P_{np} = \sum_{i=W-V+1}^W C_W^i (P_{oo} + P_{ho})^i (1 - P_{oo} - P_{ho})^{W-i}, \quad (4)$$

$$P_{pc} = \frac{P_{ho}^V}{N^{V-1}} \left[1 + \sum_{i=1}^{W-V} C_{V+i-1}^i \left(1 - \frac{P_{ho}}{N} \right)^i \right]. \quad (5)$$

Expressions (4) and (5) correspond to the noise-immune coding of fragments by (n,k) -code with the detection and correction of errors. In case of error detection, the probabilities P_{oo} and P_{ho} are determined

by expressions (1) and (2) for the multiplicity of detected errors q_o . In case of error correction, the probability P_{no} is defined by expression (3) for the multiplicity of corrected errors q_u , and the probability P_{oo} is assumed to be zero: $P_{oo}=0$.

Using expressions (4) and (5) with expressions (1) – (3) taken into account, it is possible to obtain the dependences of probability characteristics of the accuracy of fragmented message transmission P_{np} and P_{nc} on the probabilities of erroneous reception of an information symbol in the information transmission channel p_o and the parameters of a threshold fragmentation scheme (V, W) for different (n, k) -codes used to transmit information blocks. Practical interest is in determination under specified conditions of parameters of external (fragmentation scheme) and internal (noise-immune code) coding, providing the required probabilities of missing a message P_{np} and receiving a false message, which allows us to choose the parameters of fragmentation schemes and noise-immune code that minimizes one of the probabilities P_{np} and P_{nc} at the maximum acceptable values of the other probability.

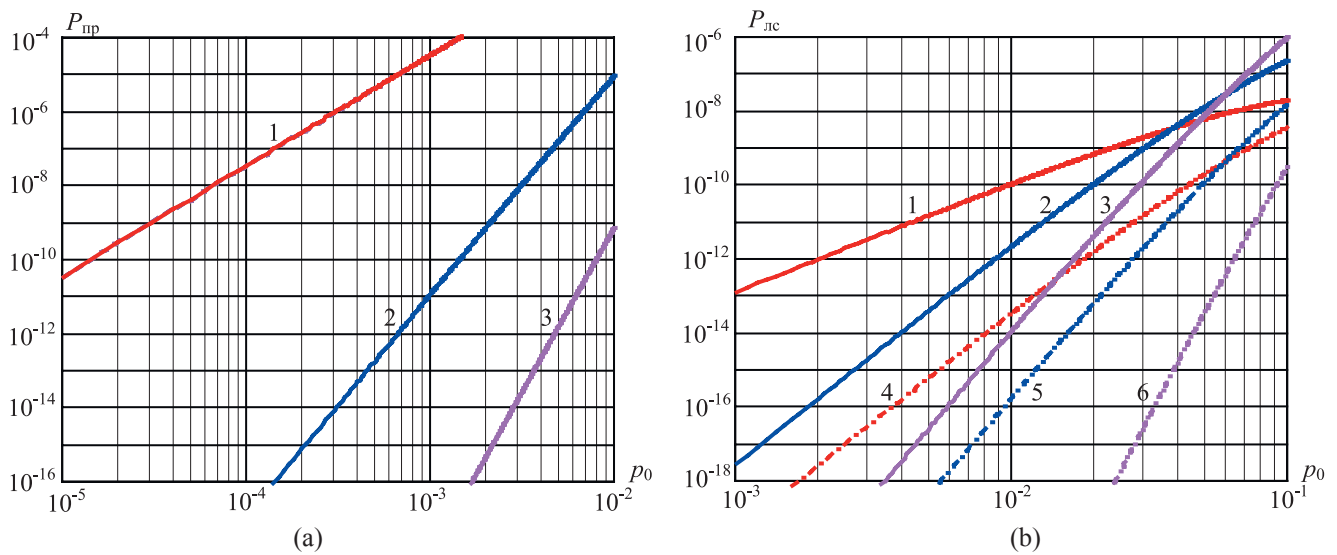


Fig. 2. Dependences of probabilities of missing a message (a) and receiving a false message (b) on the probability of erroneous reception of information symbol for the threshold fragmentation scheme (3,5) using a variety of noise-immune codes

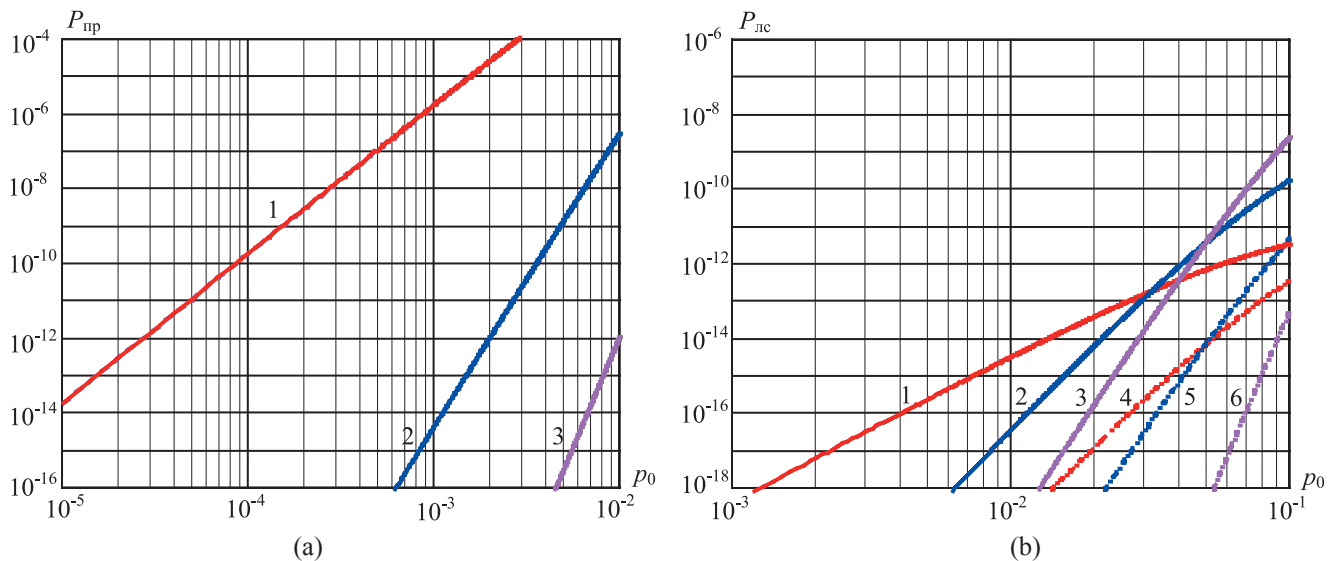


Fig. 3. Dependences of probabilities of missing a message (a) and receiving a false message (b) on the probability of erroneous reception of information symbol for the threshold fragmentation scheme (4,7) using a variety of noise-immune codes

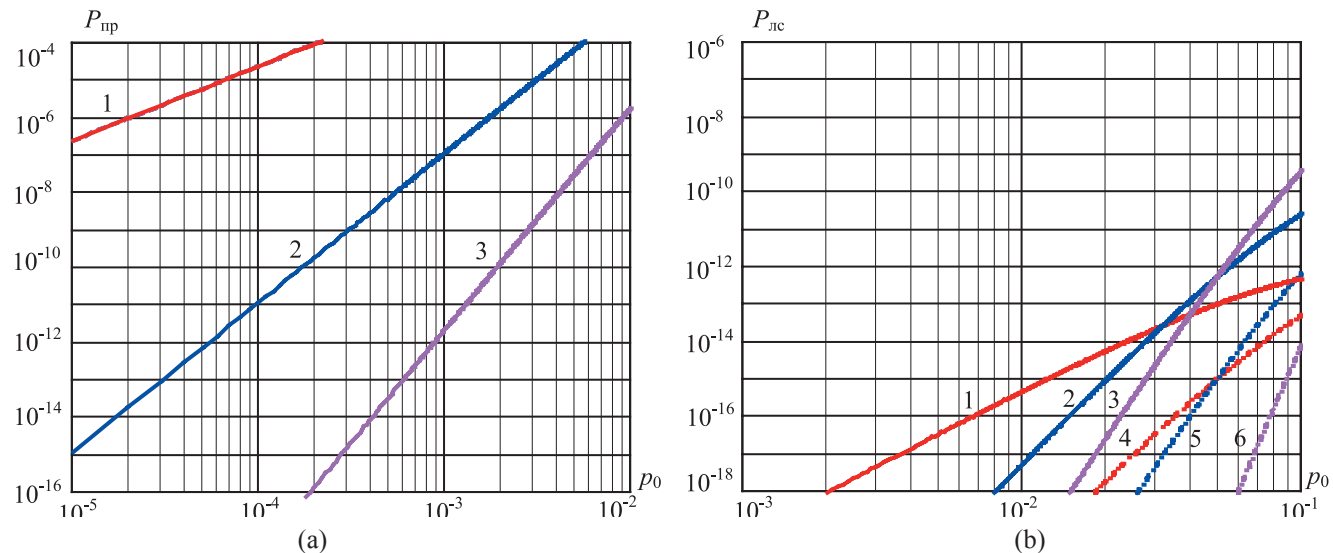


Fig. 4. Dependences of probabilities of missing a message (a) and receiving a false message (b) on the probability of erroneous reception of information symbol for the threshold fragmentation scheme (4,5) using a variety of noise-immune codes

Fig. 2-4 show the results of calculations of the probabilities of missing a message P_{np} and receiving a dummy message, depending on the probability of erroneous reception of the information symbol p_0 using the threshold fragmentation scheme with different parameters V and W , and noise-immune (n, k) -codes with different parameter values q_o and q_u . We considered the following noise-immune codes: code with even parity check (15,14) with code distance $d = 2$ with a multiplicity of detected errors $q_o=1$ and with a multiplicity of corrected errors $q_u=0$, the Hamming code (15,11) with code distance $d = 3$ with a multiplicity of detected errors $q_o=2$ and with a multiplicity of corrected errors $q_u=2$, the cyclic code (15,8) and minimum distance $d = 5$ with a multiplicity of detected errors $q_o = 4$, and with a multiplicity of corrected errors $q_u=2$. Figure 2 shows the dependences of P_{np} (a) and P_{nc} (b) on p_0 for the scheme of threshold fragmentation (3,5). Figure 3 shows the dependences of P_{np} (a) and P_{nc} (b) on p_0 for the scheme of threshold fragmentation (4,7). Figure 4 shows the dependences of P_{np} (a) and P_{nc} (b) on p_0 for the scheme of threshold fragmentation (4,5). Curves 1 in Fig. 2a, 3a, 4a correspond to the code (15,14) with $q_u=0$ and $q_o=1$, to the code (15,11) with $q_o=2$ and to the code (15,8) with $q_u=1$, curves 2 correspond to the code (15,11) when $q_o=1$, curves 3 correspond to the code (15,8) for $q_u=2$.

Curves 1 in Fig. 2b, 3b, 4b, correspond to the code (15,14) with $q_u=0$, curves 2 correspond to the code (15,11) with $q_u=1$, curves 3 correspond to the code (15,8) with $q_o=2$, curves 4 correspond to the code (15,14) with $q_o=1$, curves 5 correspond to the code (15,11) with $q_o=2$, curves 6 correspond to the code (15,8) with $q_o=4$. The value of N , which determines the probability P_{nc} , was determined as $N = 2^k$.

The coincidence of the curves corresponding to different alternatives of using noise-immune codes with error detection is conditioned by the fact that the value of the probability of missing a message P_{np} with error detection in accordance with expression (4) is effected by the sum of the probabilities of detectable errors P_{oo} and undetected errors P_{uo} at the transmission of each fragment, which for $q_o \geq 1$ is the same for all considered noise-immune codes with error detection. The magnitude of the probability of receiving a dummy message in accordance with expression (5) is affected by the value of the probability of undetected errors P_{uo} at the transmission of each fragment, which is different for all the considered noise-immune codes and alternatives of their use to detect and correct errors.

The analysis of presented dependences shows that the considered method of fragmented transmission of messages even with a sufficiently large probability of erroneous reception of an information symbol in a communication channel ($p_0=10^{-2}-10^{-4}$) and for small values of the parameters of the fragmentation

scheme V and W , as well as due to identification and correction of errors and repeated transmissions achieves a low probability of missing a message P_{np} and receiving a dummy message P_{nc} at the level up to 10^{-12} - 10^{-16} . The values P_{np} decrease with the increasing q_u , the values of P_{nc} decrease with increasing q_o and q_u .

The families of dependences in Fig. 2 and Fig. 3 correspond to the assignment of the parameters V and W of the fragmentation scheme, satisfying the ratio $V=\lceil W/2 \rceil$, where $\lceil \cdot \rceil$ is rounding upward to the nearest integer. Under these conditions, in case of increase of fragmentation scheme parameters V and W and retention of relationships between them, the probabilities P_{np} and P_{nc} decrease with the increasing V and W , and the ratio $P_{nc} < P_{np}$ is always satisfied, therefore in case of decrease of the probability of missing a message, the probability of receiving a dummy message decreases simultaneously. In case of increase of fragmentation scheme parameters V and W , there is a tendency of saturation at some level of the probability values of missing a message P_{np} . Thus, the values P_{np} for the scheme (4,7) are significantly lower than the values of P_{np} for the scheme (3,5) but slightly higher than the values for the scheme (5,8). At the same time, the values of the probability of receiving a dummy message P_{nc} , with increasing fragmentation scheme parameters V and W , are reduced, without any tendency to saturate. As follows from expression (5), the value P_{nc} also decreases with the increasing number of transmitted messages N . At the same time in the area of large values of the probability of erroneous reception of an information symbol p_o , the effect of the value N on the probability of receiving a dummy message is more noticeable than the effect of values q_o and q_u . With the decreasing values of p_o , the effect practically disappears and the main factor affecting the value of P_{nc} for a fixed p_o is the multiplicity of detected errors q_o and corrected errors q_u during transmission of message fragments.

The families of dependences in Fig. 2 and Fig. 4 correspond to such an assignment of fragmentation scheme parameters V and W , where the parameter W is fixed and the parameter V increases. Under these conditions, the increase of V does not lead to the simultaneous reduction of probabilities P_{np} and P_{nc} – the probability P_{np} increases and the probability P_{nc} decreases, and even with the increase of the V value per unit and a fixed value of W , there is an evident increase of the probability of missing a message P_{np} and reduction of the probability of receiving a dummy message P_{nc} . Therefore, by changing the relationship between the parameters of the fragmentation scheme V and W , it is possible to influence the ratio between the probabilities P_{np} and P_{nc} in accordance with the requirements imposed on them for transmission of vital messages.

It should be noted that the value of the probability of missing a message defined by expression (4) coincides with the probability of missing a message in case of W -multiple transmission of a non-fragmented message and decision making on V coincidences [7]. In terms of increasing the accuracy of information transmission by introducing redundancy into transmitted messages for repeated transmission, it is equivalent to using the ideal scheme of threshold fragmentation (V, W). However, transmission of messages with simple repetition involves the use of only one step of coding, which can provide only the detection or correction of errors at the expense of correcting abilities of a used noise-immune code that corresponds to the external coding of fragments in fragmented transmission. Multiple transmissions of messages do not have the abilities of information secrecy.

Conclusion

The method of fragmented transmission of vital messages has been analyzed primarily with reference to its use in radio communication systems operating in noisy environments and electromagnetic availability. The accuracy of message transmission is increased by means of introducing considerable redundancy connected with repeated transmission of message fragments, which is the equivalent to

the expense of time spent for their repeating. However, during transmission of formalized messages of train operation and railway automation control, which are, in fact, low informative, a significant introduction of redundancy is justified. First, it allows us to reach low values of the probability of missing messages and receiving false messages (10^{-12} - 10^{-16}) in radio channels of low quality with the 10^{-2} - 10^{-4} probability of erroneous reception of an information symbol, and second, it allows us to increase simultaneously the accuracy of message transmission via radio channels with interference and protection against unauthorized access.

Besides the possibility of using the considered method in radio communications systems, the method is well consistent with the technology of transmission of signaling messages (commands) to trains via audio frequency track circuits or through spot radio transponders (Eurobalizes) located between rails [6]. Both techniques involve the referencing of transmitted messages to the so-called block sections passed by a train, where one of the fragments of a next message can be transmitted.

References

1. **Kudryashov V.A., Mochenov A.D.** Transport communication. – M.: Route 2005. – p. 294.
2. **Tepliyakov I.M.** Fundamentals of telecommunication systems and networks. – M.: Radio and communication, 2004. – p.328.
3. **Maltsev G.N., Adadurov A.S.** Reduction of threats to information security of radio systems // Automation. Communication. Informatics. – 2011. – # 5. – p..22-24.
4. **Yaschenko V.V., Varnovsky N.P., Nesterenko Yu.V.** et alia. Introduction to Cryptography /Ed. By Yaschenko V.V. – Moscow: MCCME (Moscow Center for Continuous Mathematical Education) – 1998. – p.272.
5. **Werner M.** Coding Basics: Translated from German. – M: Technosphere, p. 2008.-288.
6. **Yakovlev V.A., Adadurov A.S.** Method for safe data transmission to train based on the “secret sharing” principle using additional channels //Dependability-2012. – # 4. – p..95-104.
7. **Maltsev, G. E., Chernyavsky E.V.** Message encryption in systems of radio control without reverse information channel //Information and control systems. – 2011. – # 4. – p.60-65.

Перегуда А. И.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАДЕЖНОСТИ КОМПЛЕКСА «ОБЪЕКТ ЗАЩИТЫ – СИСТЕМА БЕЗОПАСНОСТИ» ПРИ НЕЧЕТКОЙ ИСХОДНОЙ ИНФОРМАЦИИ

В данной работе рассматривается математическая модель надежности комплекса «объект защиты – система безопасности» с периодически контролируемой системой безопасности. При построении математической модели надежности, учитывающей неопределенность параметров модели, используется случайно-нечеткий процесс восстановления. Получена нечеткая оценка для математического ожидания наработки комплекса, а также приведен пример вычисления оценки средней наработки до аварии комплекса «объект защиты – система безопасности».

Ключевые слова: надежность, случайно-нечеткие величины, принцип расширения Заде, функция принадлежности, нечеткая средняя наработка, оценка характеристик надежности, дефаззификация.

Введение

Системы, состоящие из объекта защиты и системы безопасности, применяются там, где необходимо обеспечить безопасную эксплуатацию потенциально опасных объектов. В качестве примера можно привести атомную промышленность. Назначение системы безопасности – переводить аварийные ситуации при нарушении нормального функционирования объекта защиты в ранг неопасных, т.е. парирование отказов объекта защиты. Рассматриваемая система обладает следующими характерными особенностями: имеет место вертикальная соподчиненность – установка находится под контролем системы безопасности; система безопасности обладает правом вмешательства с тем, чтобы предотвращать потенциально опасные изменения в объекте защиты; имеет место взаимозависимость действий – успешность действия системы в целом зависит от поведения всех элементов системы. Из этого следует, что объект защиты и систему безопасности необходимо рассматривать в совокупности как единый автоматизированный технологический комплекс «объект защиты – система безопасности» (АТК ОЗ–СБ). Разработке математической модели надежности такого комплекса посвящены работы [1,2].

При анализе надежности систем может иметь место неопределенность результатов анализа, обусловленная различными причинами. В этой работе будем рассматривать неопределенность результатов анализа надежности, обусловленную неопределенностью исходных данных. Данная

разновидность неопределенности возникает, поскольку параметры математической модели, используемой при анализе надежности систем, могут быть точно неизвестны вследствие недостаточности данных и изменчивости характеристик.

Для моделирования различных аспектов неопределенности разработано несколько отличающихся друг от друга подходов, таких как теоретико-вероятностный подход, нечеткие множества и меры и некоторые другие. Обсуждение их различий и преимуществ можно найти в работе [3]. Здесь будем использовать комбинацию теоретико-вероятностного подхода и нечетких мер для построения математической модели надежности, учитывающей неопределенность параметров модели. Подобный подход изложен в ряде работ [4 – 8]. В данной работе, следуя Лю [4,5] будем использовать случайно-нечеткие величины, поскольку они позволяют наиболее просто создать математическую модель надежности АТК ОЗ–СБ, учитывающую неопределенность исходных данных. При анализе математической модели надежности мы переходим от случайных величин к случайно-нечетким величинам, а, следовательно, возникает необходимость в применении случайно-нечеткого процесса восстановления [9,10].

Формализация и решение задачи

При разработке математических моделей надежности общепринятым является подход, при котором наработки и времена восстановления описываются с помощью случайных величин. Например, можно рассматривать наработку до отказа χ , имеющую функцию распределения $F_{\chi}(t; \vec{\lambda})$, где $\vec{\lambda}$ – вектор параметров распределения. Однако, как правило, точные значения параметров λ в силу тех или иных причин неизвестны, а, следовательно, имеет место неопределенность параметров модели, что, в свою очередь, приводит к неопределенности значений искомых показателей надежности. Для количественного учета этой неопределенности воспользуемся математическим аппаратом случайно-нечетких величин [4,5]. Сущность используемого подхода заключается в том, что случайным величинам приписывается мера правдоподобия. Случайно-нечеткие наработки до отказа и времена восстановления мы будем определять, используя подход, рассмотренный в [4]. Чтобы задать случайно-нечеткую величину χ , укажем семейство вероятностных распределений $\{F_{\chi}(t; \vec{\lambda}(\theta)), \theta \in \Theta\}$ на вероятностном пространстве (Ω, A, P) , где $\vec{\lambda}$ – нечеткий вектор, определенный на пространстве правдоподобия (Θ, G, Cr) , которому соответствует функция принадлежности $\mu_{\vec{\lambda}}(\vec{x})$.

Для создания математической модели надежности комплекса «объект защиты – система безопасности» будем использовать вместо случайных величин случайные нечеткие величины. Сущность данного подхода заключается в том, что случайным величинам будем приписывать меру правдоподобия.

Будем считать, что величины χ_i – случайные нечеткие величины, каждая из которых задана на соответствующем пространстве правдоподобия (Θ_i, P_i, Cr_i) , причем все они независимы, положительны и одинаково распределены. Аналогично γ_i – случайные нечеткие величины, каждая из которых задана на соответствующем пространстве правдоподобия (Θ_i', P_i', Cr_i') , причем они также независимы, одинаково распределены и положительны. Номер цикла процесса функционирования объекта защиты, на котором произошла авария, обозначим v . Кроме этого, считаем, что v – положительное случайное нечеткое целое (т.е. случайная нечеткая величина, которая принимает только положительные целые значения), определенное на пространстве правдоподобия $(\Theta_i'', P_i'', Cr_i'')$. И, наконец, предположим, что последовательности $\{\chi_i, i \geq 1\}$ и $\{\gamma_i, i \geq 1\}$ взаимно независимы, а v независима от последовательностей $\{\chi_i, i \geq 1\}$ и $\{\gamma_i, i \geq 1\}$.

Наработку комплекса до первой аварии можно записать [2]:

$$\omega = \sum_{i=1}^{v-1} (\chi_i + \gamma_i) + \chi_v,$$

где χ_v – наработка на отказ на том цикле регенерации, на котором произошел отказ объекта защиты. Таким образом, ω – это случайная нечеткая величина, определенная на пространстве правдоподобия (Θ_i, P_i, Cr_i) , где $\Theta = \Theta'' \times (\Theta_1 \times \Theta_1') \times (\Theta_2 \times \Theta_2') \times \dots$, Cr – мера правдоподобия, определяется так [4,5]

$$Cr(A) = \begin{cases} \sup_{(\theta_1, \theta_2, \dots) \in A} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\}, & \text{если } \sup_{(\theta_1, \theta_2, \dots) \in A} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\} < \frac{1}{2}, \\ 1 - \sup_{(\theta_1, \theta_2, \dots) \in A^c} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\}, & \text{если } \sup_{(\theta_1, \theta_2, \dots) \in A} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\} \geq \frac{1}{2}. \end{cases}$$

Для каждого фиксированного θ величины $M\chi_i(\theta)$, $M\gamma_i(\theta)$, $Mv(\theta)$ и $M\omega(\theta)$ представляют собой математические ожидания случайных величин $\chi(\theta)$, $\gamma(\theta)$, $v(\theta)$ и $\omega(\theta)$ соответственно. Поскольку θ варьируется на множестве Θ , то мы рассматриваем уже нечеткие величины $M\chi_i(\theta)$, $M\gamma_i(\theta)$, $Mv(\theta)$, $M\omega(\theta)$. Для измерения нечеткой величины используют два критических значения (оптимистическое и пессимистическое значение) с заданным доверительным уровнем α [5]. Таким образом, мы можем рассматривать следующие α -пессимистические и α -оптимистические значения этих математических ожиданий:

$$(M\chi_i(\theta))_{\sup}(\alpha) = \sup \{r | Cr \{M\chi_i(\theta) \geq r\} \geq \alpha\},$$

$$(M\chi_i(\theta))_{\inf}(\alpha) = \inf \{r | Cr \{M\chi_i(\theta) \leq r\} \geq \alpha\},$$

$$(M\gamma_i(\theta))_{\sup}(\alpha) = \sup \{r | Cr \{M\gamma_i(\theta) \geq r\} \geq \alpha\},$$

$$(M\gamma_i(\theta))_{\inf}(\alpha) = \inf \{r | Cr \{M\gamma_i(\theta) \leq r\} \geq \alpha\},$$

$$(Mv(\theta))_{\sup}(\alpha) = \sup \{r | Cr \{Mv(\theta) \geq r\} \geq \alpha\},$$

$$(Mv(\theta))_{\inf}(\alpha) = \inf \{r | Cr \{Mv(\theta) \leq r\} \geq \alpha\},$$

$$(M\omega(\theta))_{\sup}(\alpha) = \sup \{r | Cr \{M\omega(\theta) \geq r\} \geq \alpha\},$$

$$(M\omega(\theta))_{\inf}(\alpha) = \inf \{r | Cr \{M\omega(\theta) \leq r\} \geq \alpha\}.$$

Для каждого $\theta \in \Theta$ имеет место равенство

$$M\omega(\theta) = M \left(\sum_{i=1}^{v(\theta)-1} (\chi_i(\theta) + \gamma_i(\theta)) + \chi_{v(\theta)}(\theta) \right).$$

Используя формулу полной вероятности и определение критических значений α , вычислим α -пессимистическое значение $M\omega(\theta)$. Тогда

$$\begin{aligned}(M\omega(\theta))_{\inf}(\alpha) &= M \left(\sum_{i=1}^{v(\cdot)-1} (\chi_i(\theta) + \gamma_i(\theta)) + \chi_{v(\theta)}(\theta) \right)_{\inf}(\alpha) = \\&= \sum_{k=1}^{\infty} \left(P(\theta) = k \sum_{i=1}^{k-1} (M\chi_i(\theta) + M\gamma_i(\theta)) + M\chi_k(\theta) \right)_{\inf}(\alpha) = \\&= \sum_{k=1}^{\infty} P(v(\theta) = k)_{\inf}(\alpha) \left(\sum_{i=1}^{k-1} (M\chi_i(\theta) + M\gamma_i(\theta)) + M\chi_k(\theta) \right)_{\inf}(\alpha) = \\&= \sum_{k=1}^{\infty} P(v(\theta) = k)_{\inf}(\alpha) \left(\sum_{i=1}^{k-1} ((M\chi_i(\theta))_{\inf}(\alpha) + (M\gamma_i(\theta))_{\inf}(\alpha)) + (M\chi_k(\theta))_{\inf}(\alpha) \right) = \\&= \left(M\chi(\theta) \sum_{k=1}^{\infty} P(v(\theta) = k) \right)_{\inf}(\alpha) + \left((M\chi(\theta) + M\gamma(\theta)) \sum_{k=1}^{\infty} (k-1)P(v(\theta) = k) \right)_{\inf}(\alpha) = \\&= ((M\chi(\theta))_{\inf}(\alpha) + (M\gamma(\theta))_{\inf}(\alpha))(Mv(\theta) - 1)_{\inf}(\alpha) + (M\chi(\theta))_{\inf}(\alpha).\end{aligned}$$

Аналогично показывается, что α -оптимистическое значение $M\omega(\theta)$ определяется соотношением

$$(M\omega(\theta))_{\sup}(\alpha) = ((M\chi(\theta))_{\sup}(\alpha) + (M\gamma(\theta))_{\sup}(\alpha))(Mv(\theta) - 1)_{\sup}(\alpha) + (M\chi(\theta))_{\sup}(\alpha).$$

Вычислим теперь среднее ожидаемое значение случайной нечеткой величины, которое определяется формулой $E[\xi] = \frac{1}{2} \int_0^1 (\xi_{\sup}(\alpha) + \xi_{\inf}(\alpha)) d\alpha$ [5,6], получим

$$\begin{aligned}E[M\omega(\theta)] &= \frac{1}{2} \int_0^1 ((M\chi)_{\inf}(\alpha)(Mv(\theta))_{\inf}(\alpha) + (M\gamma(\theta))_{\inf}(\alpha)(Mv(\theta) - 1)_{\inf}(\alpha)) d\alpha + \\&+ \frac{1}{2} \int_0^1 ((M\chi(\theta))_{\sup}(\alpha)(Mv(\theta))_{\sup}(\alpha) + (M\gamma(\theta))_{\sup}(\alpha)(Mv(\theta) - 1)_{\sup}(\alpha)) d\alpha = \\&= \frac{1}{2} \int_0^1 ((M\chi(\theta))_{\inf}(\alpha)(Mv(\theta))_{\inf}(\alpha) + (M\chi(\theta))_{\sup}(\alpha)(Mv(\theta))_{\sup}(\alpha)) d\alpha + \\&+ \frac{1}{2} \int_0^1 ((M\gamma(\theta))_{\inf}(\alpha)(Mv(\theta) - 1)_{\inf}(\alpha) + (M\gamma(\theta))_{\sup}(\alpha)(Mv(\theta) - 1)_{\sup}(\alpha)) d\alpha.\end{aligned}$$

Таким образом, получаем

$$E[M\omega(\theta)] = M\chi(\theta) + M\chi(\theta)(v(\theta) - 1) + M\gamma(\theta)(v(\theta) - 1). \quad (1)$$

Из определения среднего ожидаемого значения случайной нечеткой величины следует, что $M[\omega] = E[M\omega]$.

Практическое использование теории нечетких величин предполагает наличие функций принадлежности. При дальнейшем вычислении математического ожидания случайной нечеткой величины $M[\omega]$ необходимо вычислить функцию принадлежности.

Пусть наработка между отказами объекта защиты имеет экспоненциальное распределение, параметр которого является треугольной нечеткой величиной. Тогда наработка между отказами объекта защиты является случайной нечеткой величиной. Кроме этого предположим, что и время восстановления объекта защиты имеет экспоненциальное распределение, параметр которого также является треугольной нечеткой величиной. Полагаем, что номер цикла v , на котором произошла авария, также является случайной нечеткой величиной, причем вероятность аварии на одном цикле процесса функционирования комплекса равна q .

Таким образом, исходя из сделанных предположений, запишем:

$$P\{\chi(\theta) \leq t\} = \begin{cases} 1 - e^{-\lambda_{\chi}(\theta)t}, & \text{если } 0 \leq t < \infty, \\ 0, & \text{если } t < 0. \end{cases}$$

Замечая, что треугольная нечеткая величина $\lambda_{\chi}(\theta)$ представима тройкой четких чисел $(\lambda_{\chi}^{(1)}, \lambda_{\chi}^{(2)}, \lambda_{\chi}^{(3)})$, таких что $\lambda_{\chi}^{(1)} < \lambda_{\chi}^{(2)} < \lambda_{\chi}^{(3)}$, а функция принадлежности ее определяется выражением вида

$$\mu_{\lambda_{\chi}}(y_1) = \begin{cases} \frac{y_1 - \lambda_{\chi}^{(1)}}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(1)}}, & \text{если } y_1 \in [\lambda_{\chi}^{(1)}, \lambda_{\chi}^{(2)}], \\ \frac{y_1 - \lambda_{\chi}^{(3)}}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(3)}}, & \text{если } y_1 \in [\lambda_{\chi}^{(2)}, \lambda_{\chi}^{(3)}], \\ 0, & \text{если } y_1 \notin [\lambda_{\chi}^{(1)}, \lambda_{\chi}^{(3)}]. \end{cases}$$

Аналогично запишем для нечеткой величины $\lambda_{\gamma}(\theta)$

$$P\{\gamma(\theta) \leq t\} = \begin{cases} 1 - e^{-\lambda_{\gamma}(\theta)t}, & \text{если } 0 \leq t < \infty, \\ 0, & \text{если } t < 0 \end{cases}$$

$$\mu_{\lambda_{\gamma}}(y_2) = \begin{cases} \frac{y_2 - \lambda_{\gamma}^{(1)}}{\lambda_{\gamma}^{(2)} - \lambda_{\gamma}^{(1)}}, & \text{если } y_2 \in [\lambda_{\gamma}^{(1)}, \lambda_{\gamma}^{(2)}], \\ \frac{y_2 - \lambda_{\gamma}^{(3)}}{\lambda_{\gamma}^{(2)} - \lambda_{\gamma}^{(3)}}, & \text{если } y_2 \in [\lambda_{\gamma}^{(2)}, \lambda_{\gamma}^{(3)}], \\ 0, & \text{если } y_2 \notin [\lambda_{\gamma}^{(1)}, \lambda_{\gamma}^{(3)}]. \end{cases}$$

Поскольку рассматриваемый процесс функционирования объекта защиты является альтернирующим случайным процессом, то вероятность того, что авария произошла на k -м цикле регенерации равна

$$P\{v = k\} = (1 - q)^{(k-1)} q. \quad (2)$$

В этом случае не представляется возможным в явном виде записать выражение для функции принадлежности величины $M\omega$, однако вычислить $E[\omega]$ все же можно. Очевидно, что

$$M[\omega] = M\left[\frac{1}{q\lambda_x} + \frac{1-q}{q\lambda_y}\right] = \frac{1}{q} M\left[\frac{1}{\lambda_x}\right] + \frac{1-q}{q} M\left[\frac{1}{\lambda_y}\right].$$

В полученном выражении оказались неизвестными ожидаемые значения $M\left[\frac{1}{\lambda_x}\right]$ и $M\left[\frac{1}{\lambda_y}\right]$, которые нам предстоит вычислить. Математическое ожидание нечеткой величины $M\left[\frac{1}{\lambda_x}\right]$ будем вычислять следующим образом:

$$M\left[\frac{1}{\lambda_x}\right] = \int_0^{+\infty} Cr\left\{\theta \in \Theta / \frac{1}{\lambda_x(\theta)} \geq r\right\} dr.$$

Прежде чем вычислить $M\left[\frac{1}{\lambda_x}\right]$, сначала необходимо определить соответствующую функцию принадлежности:

$$\mu(y) = \sup_{y=\frac{1}{y_1}} \mu_{\lambda_x}(y_1) = \begin{cases} \frac{\frac{1}{y_1} - \lambda_x^{(1)}}{\lambda_x^{(2)} - \lambda_x^{(1)}}, & \text{если } y \in \left[\frac{1}{\lambda_x^{(2)}}, \frac{1}{\lambda_x^{(1)}}\right] \\ \frac{\frac{1}{y_1} - \lambda_x^{(3)}}{\lambda_x^{(2)} - \lambda_x^{(3)}}, & \text{если } y \in \left[\frac{1}{\lambda_x^{(3)}}, \frac{1}{\lambda_x^{(2)}}\right] \\ 0, & \text{если } y \notin \left[\frac{1}{\lambda_x^{(3)}}, \frac{1}{\lambda_x^{(1)}}\right] \end{cases}.$$

Тогда меру правдоподобия можно записать в виде

$$Cr\left\{\theta \in \Theta / \frac{1}{\lambda_{\chi}(\theta)} \geq r\right\} = \begin{cases} 1, & \text{если } r \leq \frac{1}{\lambda_{\chi}^{(3)}} \\ 1 - \frac{1}{2} \frac{\frac{1}{r} - \lambda_{\chi}^{(3)}}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(3)}}, & \text{если } r \in \left[\frac{1}{\lambda_{\chi}^{(3)}}, \frac{1}{\lambda_{\chi}^{(2)}}\right] \\ \frac{1}{2} \frac{\frac{1}{r} - \lambda_{\chi}^{(1)}}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(1)}}, & \text{если } r \in \left[\frac{1}{\lambda_{\chi}^{(2)}}, \frac{1}{\lambda_{\chi}^{(1)}}\right] \\ 0, & \text{если } r > \frac{1}{\lambda_{\chi}^{(1)}} \end{cases}.$$

Следовательно, получаем

$$M\left[\frac{1}{\lambda_{\chi}}\right] = \int_0^{+\infty} Cr\left\{\theta \in \Theta / \frac{1}{\lambda_{\chi}(\theta)} \geq r\right\} dr = \frac{1}{2} \frac{1}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(1)}} \ln\left(\frac{\lambda_{\chi}^{(2)}}{\lambda_{\chi}^{(1)}}\right) + \frac{1}{2} \frac{1}{\lambda_{\chi}^{(3)} - \lambda_{\chi}^{(2)}} \ln\left(\frac{\lambda_{\chi}^{(3)}}{\lambda_{\chi}^{(2)}}\right). \quad (3)$$

Математическое ожидание нечеткой величины $M\left[\frac{1}{\lambda_{\gamma}}\right]$ можно записать аналогично (3), а именно

$$M\left[\frac{1}{\lambda_{\gamma}}\right] = \frac{1}{2} \frac{1}{\lambda_{\gamma}^{(2)} - \lambda_{\gamma}^{(1)}} \ln\left(\frac{\lambda_{\gamma}^{(2)}}{\lambda_{\gamma}^{(1)}}\right) + \frac{1}{2} \frac{1}{\lambda_{\gamma}^{(3)} - \lambda_{\gamma}^{(2)}} \ln\left(\frac{\lambda_{\gamma}^{(3)}}{\lambda_{\gamma}^{(2)}}\right).$$

Определим теперь Mv . Поскольку v – дискретная случайная величина, то

$$Mv = \sum_{k=1}^{\infty} kq(1-q)^{k-1} = q.$$

Подставляем полученные выражения $M\left[\frac{1}{\lambda_{\gamma}}\right]$, $M\left[\frac{1}{\lambda_{\chi}}\right]$ и Mv в формулу $M[\omega]$ имеем

$$M[\omega] = \frac{1}{2q} \left\{ \frac{1}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(1)}} \ln\left(\frac{\lambda_{\chi}^{(2)}}{\lambda_{\chi}^{(1)}}\right) + \frac{1}{\lambda_{\chi}^{(3)} - \lambda_{\chi}^{(2)}} \ln\left(\frac{\lambda_{\chi}^{(3)}}{\lambda_{\chi}^{(2)}}\right) \right\} + \\ + \frac{1-q}{2q} \left\{ \frac{1}{\lambda_{\gamma}^{(2)} - \lambda_{\gamma}^{(1)}} \ln\left(\frac{\lambda_{\gamma}^{(2)}}{\lambda_{\gamma}^{(1)}}\right) + \frac{1}{\lambda_{\gamma}^{(3)} - \lambda_{\gamma}^{(2)}} \ln\left(\frac{\lambda_{\gamma}^{(3)}}{\lambda_{\gamma}^{(2)}}\right) \right\}.$$

Заметим, что если $\lambda_{\chi}^{(1)} = \lambda_{\chi}^{(2)} = \lambda_{\chi}^{(3)}$ и $\lambda_{\gamma}^{(1)} = \lambda_{\gamma}^{(2)} = \lambda_{\gamma}^{(3)}$ полученное выражение сводится к выражению для вычисления математического ожидания в случае, когда параметры распределений являются четкими величинами.

Для того чтобы вычислить $M\omega(\theta)$, как математическое ожидание нечеткой величины, нам необходимо получить соотношение для вероятности $q(\theta)$ при каждом фиксированном $\theta \in \Theta$, поскольку значения $M\chi(\theta)$ и $M\gamma(\theta)$ были вычислены выше. Рассмотрим более подробно процесс функционирования системы безопасности. Поскольку система безопасности функционирует в режиме ожидания отказа объекта защиты, то невозможно обнаружить ее отказы в момент их возникновения. Поэтому для обнаружения скрытых отказов вводится процедура периодического профилактического контроля системы безопасности. Период контроля исправности обозначим T , а его длительность – δ . Предполагаем, что во время периодического контроля система безопасности прекращает выполнять свои функции. Если система безопасности исправно функционировала время ξ_i на i -м цикле регенерации, то за это время было произведено $\left\lfloor \frac{\xi_i}{T+\delta} \right\rfloor$ ($[x]$, $\{x\}$ – соответственно целая и дробная часть числа x , $x^+ = \max(x, 0)$) периодов контрольной профилактики. Причем за это время система находилась в рабочем состоянии время $\left\lfloor \frac{\xi_i}{T+\delta} \right\rfloor T$. Отказ СБ обнаруживается лишь в моменты времени $\left(\left\lfloor \frac{\xi_i}{T+\delta} \right\rfloor + 1 \right) (T+\delta)$, т.е. в моменты времени окончания процедуры контроля. После проведения соответствующих ремонтно-восстановительных работ продолжительностью η_i система безопасности начинает снова исправно функционировать. Таким образом, процесс функционирования системы безопасности с контрольными профилактиками есть случайный процесс с периодом регенерации

$$\tau_{CB}(\xi, \eta) = (T+\delta) \left(\left\lfloor \frac{\xi}{T+\delta} \right\rfloor + 1 \right) + \eta.$$

Таким образом, авария комплекса происходит в том случае, когда отказ объекта защиты приходится на неработоспособное состояние системы безопасности. Моментами регенерации процесса функционирования комплекса будут моменты окончания восстановления объекта защиты.

Учитывая независимость рассматриваемых величин, соотношение (1) можно записать для каждого фиксированного $\theta \in \Theta$ так

$$\begin{aligned} E[\omega(\theta)] &= \frac{1}{q(\theta)} M\chi(\theta) + \frac{1-q(\theta)}{q(\theta)} M\gamma(\theta) = \\ &= \frac{1}{q(\theta)} \int_0^{\infty} (1 - F_{\chi}(t; \bar{\lambda}_{\chi}(\theta))) dt + \frac{1-q(\theta)}{q(\theta)} \int_0^{\infty} (1 - F_{\gamma}(t; \bar{\lambda}_{\gamma}(\theta))) dt, \end{aligned} \quad (4)$$

где $q(\theta)$ – вероятность аварии на цикле регенерации процесса функционирования комплекса, $F_{\chi}(t; \bar{\lambda}_{\chi}(\theta))$, $F_{\gamma}(t; \bar{\lambda}_{\gamma}(\theta))$ – вероятностные распределения для случайно-нечетких величин χ и γ соответственно.

Для вычисления вероятности $q(\theta)$ обозначим $Q^+(\theta)$ – множество моментов времени, на протяжении которых система безопасности способна парировать отказ объекта защиты и $Q^-(\theta)$ – множество моментов времени, на протяжении которых система безопасности не способна парировать отказ объекта защиты. Тогда вероятность $q(\theta)$ для каждого фиксированного $\theta \in \Theta$ будем вычислять следующим образом:

$$q(\theta) = \int_0^\infty P(t \in Q^-(\theta)) dF_\chi(t; \bar{\lambda}_\chi(\theta)).$$

Замечая, что

$$P(t \in Q^-(\theta)) = 1 - P(t \in Q^+(\theta)) = 1 - P^+(t; \theta).$$

Тогда в соответствии с формулой полной вероятности запишем

$$P^+(t; \theta) = \int_0^\infty \int_0^\infty P(t \in Q^+(\theta) | \xi(\theta) = x, \eta(\theta) = y) dF_\eta(y; \bar{\lambda}_\eta(\theta)) dF_\xi(x; \bar{\lambda}_\xi(\theta)).$$

Напомним, что ξ – случайная наработка до первого скрытого отказа СБ, а η – случайное время восстановления системы безопасности после первого скрытого отказа. При вычислении $P^+(t; \theta)$ возможны только два взаимоисключающих варианта: $\tau_{CB}(\xi, \eta) > t$ и $\tau_{CB}(\xi, \eta) \leq t$. Следовательно, представим $P^+(t)$ в виде суммы двух слагаемых [2]:

$$\begin{aligned} P^+(t; \theta) = & \iint_{\tau_{CB}(x, y) \leq t} P(t \in Q^+(\theta) | \xi(\theta) = x, \eta(\theta) = y) dF_\eta(y; \bar{\lambda}_\eta(\theta)) dF_\xi(x; \bar{\lambda}_\xi(\theta)) + \\ & + \iint_{\tau_{CB}(x, y) > t} P(t \in Q^+(\theta) | \xi(\theta) = x, \eta(\theta) = y) dF_\eta(y; \bar{\lambda}_\eta(\theta)) dF_\xi(x; \bar{\lambda}_\xi(\theta)) = I_1 + I_2. \end{aligned}$$

Вычислим сначала второе слагаемое. Условие $\tau_{CB}(x, y) > t$ означает, что момент регенерации процесса функционирования системы безопасности наступил после момента времени t . Учитывая это условие, I_2 преобразуем так:

$$\begin{aligned} I_2 = & \iint_{\tau_{CB}(x, y) > t} \left(\sum_{m=0}^{\left\lfloor \frac{x}{T+\delta} \right\rfloor - 1} J_{t \in [m(T+\delta), m(T+\delta)+T)} + J_{t \in \left[\left\lfloor \frac{x}{T+\delta} \right\rfloor (T+\delta), x \right)} \right) dF_\eta(y; \bar{\lambda}_\eta(\theta)) dF_\xi(x; \bar{\lambda}_\xi(\theta)) = \\ = & \int_0^\infty \left(\sum_{m=0}^{\left\lfloor \frac{x}{T+\delta} \right\rfloor - 1} J_{t \in [m(T+\delta), m(T+\delta)+T)} + J_{t \in \left[\left\lfloor \frac{x}{T+\delta} \right\rfloor (T+\delta), x \right)} \right) \left(1 - F_\eta \left(t - \left(\left\lfloor \frac{x}{T+\delta} \right\rfloor + 1 \right) (T+\delta); \bar{\lambda}_\eta(\theta) \right) \right) dF_\xi(x; \bar{\lambda}_\xi(\theta)), \end{aligned}$$

где $J_{t \in A}$ – индикатор события $t \in A$.

Опуская некоторые несложные, но громоздкие преобразования, приведем сразу конечный результат:

$$I_2 = \left(1 - F_{\xi}(t; \vec{\lambda}_{\xi}(\theta))\right) - \sum_{m=1}^{\infty} \left(1 - F_{\xi}(m(T+\delta); \vec{\lambda}_{\xi}(\theta))\right) \left(J_{(m-1)(T+\delta)+T \leq t} - J_{m(T+\delta) \leq t}\right).$$

Заметим, что $1 - \sum_{m=1}^{\infty} (1 - F_{\xi}(m(T+\theta)))(J_{(m-1)(T+\theta) \leq t} - J_{m(T+\theta) \leq t})$ представляет собой функцию распределения $F_{\zeta}(t)$ некоторой случайной величины ζ , что позволяет представить I_2 так

$$I_2 = F_{\zeta}(t; \vec{\lambda}_{\xi}(\theta)) - F_{\xi}(t; \vec{\lambda}_{\xi}(\theta)). \quad (5)$$

Рассмотрим теперь I_1 . При рассмотрении случая $\tau_{CB} \leq t$ будем учитывать, что после проведения соответствующих ремонтно-восстановительных работ в момент времени τ_{CB} система безопасности снова будет функционировать с теми же вероятностными характеристиками, что и в момент времени $t = 0$. Тогда

$$I_1 = \iint_{\tau_{CB}(x,y) \leq t} P^+(t - \tau_{CB}(x, y)) dF_{\eta}(y; \vec{\lambda}_{\eta}(\theta)) dF_{\xi}(x; \vec{\lambda}_{\xi}(\theta)) = \int_0^t P^+(t - z) dF_{\tau_{CB}}(z; \vec{\lambda}_{\eta}(\theta), \vec{\lambda}_{\xi}(\theta)). \quad (6)$$

Таким образом, суммируя (5) и (6) при каждом фиксированном $\theta \in \Theta$ получаем интегральное уравнение типа Вольтерра второго рода для вероятности $P(t \in Q^+(\theta))$:

$$P^+(t; \theta) = f(t; \theta) + \int_0^t P^+(t - z) dF_{\tau_{CB}}(z; \vec{\lambda}_{\eta}(\theta), \vec{\lambda}_{\xi}(\theta)), \quad (7)$$

$$\text{где } f(t; \theta) = F_{\zeta}(t; \vec{\lambda}_{\xi}(\theta)) - F_{\xi}(t; \vec{\lambda}_{\xi}(\theta)), \quad F_{\tau_{CB}}(z; \vec{\lambda}_{\eta}(\theta), \vec{\lambda}_{\xi}(\theta)) = P\left(\left(\left\lceil \frac{\xi(\theta)}{T+\delta} \right\rceil + 1\right)(T+\delta) + \eta(\theta) \leq z\right).$$

Так как уравнение (7) является уравнением в свертках, то для его решения используем преобразование Лапласа-Стилтьеса. Решение уравнения (7) в терминах преобразования Лапласа-Стилтьеса имеет вид

$$\tilde{P}^+(s; \theta) = \frac{\tilde{f}(s; \theta)}{1 - \tilde{F}_{\tau_{CB}}(s; \vec{\lambda}_{\eta}(\theta), \vec{\lambda}_{\xi}(\theta))} = \frac{Me^{-s\zeta(\theta)} - Me^{-s\xi(\theta)}}{1 - Me^{-s\tau_{CB}(\theta)}},$$

$$\text{где } \tilde{P}^+(s; \theta) = \int_0^{\infty} e^{-st} dP^+(t; \theta), \quad \tilde{F}_{\tau_{CB}}(s; \vec{\lambda}_{\eta}(\theta), \vec{\lambda}_{\xi}(\theta)) = \int_0^{\infty} e^{-st} dF_{\tau_{CB}}(t; \vec{\lambda}_{\eta}(\theta), \vec{\lambda}_{\xi}(\theta))$$

$$\text{и } \tilde{f}(s; \theta) = \int_0^{\infty} e^{-st} df(t; \theta) = \int_0^{\infty} e^{-st} dF_{\zeta}(t; \bar{\lambda}_{\xi}(\theta)) - \int_0^{\infty} e^{-st} dF_{\xi}(t; \bar{\lambda}_{\xi}(\theta)).$$

Из-за трудностей нахождения обратного преобразования Лапласа-Стилтьеса в аналитическом виде, найдем асимптотическое соотношение для $P^+(t; \theta)$, применив известное соотношение $\lim_{t \rightarrow \infty} P^+(t; \theta) = \lim_{s \rightarrow 0} \tilde{P}^+(s; \theta)$. Применяя указанное соотношение, получаем

$$\lim_{t \rightarrow \infty} P^+(t; \theta) = \frac{M\xi(\theta) - M\zeta(\theta)}{M\tau_{\bar{N}A}(\theta)}.$$

Очевидно, что теперь необходимо вычислить выражения для математических ожиданий $M\zeta(\theta)$, $M\xi(\theta)$ и $M\tau_{CB}(\theta)$. Поскольку $M\zeta(\theta) = \int_0^{\infty} (1 - F_{\zeta}(t; \bar{\lambda}_{\xi}(\theta))) dt$, то

$$\begin{aligned} M\zeta(\theta) &= \int_0^{\infty} \sum_{m=1}^{\infty} (1 - F_{\xi}(k(T+\delta); \bar{\lambda}_{\xi}(\theta))) (J_{(m+1)(T+\delta)+T \leq t} - J_{m(T+\delta) \leq t}) dt = \\ &= \sum_{k=0}^{\infty} k\delta (F_{\xi}((k+1)(T+\delta); \bar{\lambda}_{\xi}(\theta)) - F_{\xi}(k(T+\delta); \bar{\lambda}_{\xi}(\theta))) = \sum_{k=0}^{\infty} k\delta P\left(\left[\frac{\xi(\theta)}{T+\delta}\right] = k\right) = \delta M\left[\frac{\xi(\theta)}{T+\delta}\right]. \end{aligned}$$

Поскольку $\xi(\theta) \gg T + \delta$, то $\left[\frac{\xi(\theta)}{T+\delta}\right] \cong \frac{\xi(\theta)}{T+\delta} - \frac{1}{2}$ [1], что позволяет переписать $M\zeta(\theta)$ для каждого фиксированного $\theta \in \Theta$ так $M\zeta(\theta) = M\xi(\theta) \frac{\delta}{T+\delta} - \frac{\delta}{2}$. Тогда

$$M\xi(\theta) - M\zeta(\theta) = M\xi(\theta) \frac{T}{T+\delta} + \frac{\delta}{2} \text{ и } M\tau_{\bar{N}A}(\theta) = M\eta(\theta) + \frac{T+\delta}{2} + M\xi(\theta).$$

$$\lim_{t \rightarrow \infty} P^+(t; \theta) = \frac{M\xi(\theta) \frac{T}{T+\delta} + \frac{\delta}{2}}{M\xi(\theta) + \frac{T+\delta}{2} + M\eta(\theta)}.$$

Заметим, что $M\eta(\theta)$ и $M\xi(\theta)$ могут быть вычислены аналогично как математические ожидания $M\chi(\theta)$ и $M\gamma(\theta)$. Для вероятности $q(\theta)$ для каждого фиксированного $\theta \in \Theta$ можем записать следующую асимптотическую оценку:

$$q(\theta) \approx 1 - \lim_{t \rightarrow \infty} P^+(t; \theta) = \frac{M\xi(\theta) \frac{\delta}{T+\delta} + \frac{T}{2} + M\eta(\theta)}{M\xi(\theta) + \frac{T+\delta}{2} + M\eta(\theta)}.$$

Таким образом, мы получили соотношения для всех величин, входящих в (1). Теперь можем вычислить $M[\omega(\theta)]$ при каждом фиксированном $\theta \in \Theta$ по формуле

$$M[\omega(\theta)] = \frac{\left(M\xi(\theta) + \frac{T+\delta}{2} + M\eta(\theta)\right)M\chi(\theta) + \left(M\xi(\theta)\frac{T}{T+\delta} + \frac{\delta}{2}\right)M\gamma(\theta)}{M\xi(\theta)\frac{\delta}{T+\delta} + \frac{T}{2} + M\eta(\theta)},$$

где $M\chi(\theta) = \int_0^\infty (1 - F_\chi(t; \tilde{\lambda}_\chi(\theta)))dt$, $M\xi(\theta) = \int_0^\infty (1 - F_\xi(t; \tilde{\lambda}_\xi(\theta)))dt$, $M\gamma(\theta) = \int_0^\infty (1 - F_\gamma(t; \tilde{\lambda}_\gamma(\theta)))dt$ и $M\eta(\theta) = \int_0^\infty (1 - F_\eta(t; \tilde{\lambda}_\eta(\theta)))dt$.

Следовательно, в соответствии с определением функции от нечетких величин [4,5], мы задали нечеткое математическое ожидание наработки до первой аварии как функцию от нечетких параметров модели.

Используем принцип расширения Заде [6]:

$$\mu(x) = \sup_{x=f(x_1, x_2, \dots, x_n)} \min_{1 \leq i \leq n} \mu_i(x_i)$$

и запишем соотношение для функции принадлежности $M\omega(\theta)$:

$$\mu_{M\omega}(y) = \sup_{y=f(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4)} \min(\mu_{\tilde{\lambda}_\chi}(\tilde{x}_1), \mu_{\tilde{\lambda}_\gamma}(\tilde{x}_2), \mu_{\tilde{\lambda}_\xi}(\tilde{x}_3), \mu_{\tilde{\lambda}_\eta}(\tilde{x}_4)),$$

$$\text{где } f(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4) = \frac{\left(M\xi(\tilde{x}_3) + \frac{T+\delta}{2} + M\eta(\tilde{x}_4)\right)M\chi(\tilde{x}_1) + \left(M\xi(\tilde{x}_3)\frac{T}{T+\delta} + \frac{\delta}{2}\right)M\gamma(\tilde{x}_2)}{M\xi(\tilde{x}_3)\frac{\delta}{T+\delta} + \frac{T}{2} + M\eta(\tilde{x}_4)}.$$

Таким образом, нам удалось записать соотношение для функции принадлежности ожидаемого значения наработки комплекса до аварии через функции принадлежности параметров модели.

Рассмотрим теперь процедуру дефаззификации, т.е. преобразование нечеткого множества в четкое число, для чего воспользуемся определением среднего ожидаемого значения случайно-нечетких величин [6]:

$$M[\omega(\theta)] = \int_0^\infty Cr\{\theta \in \Theta \mid M\omega(\theta) \geq r\}dr - \int_{-\infty}^0 Cr\{\theta \in \Theta \mid M\omega(\theta) \leq r\}dr.$$

Найдем соответствующую меру правдоподобия, используя соотношение, связывающее меру правдоподобия и функцию принадлежности [5]:

$$Cr\{M\omega \in B\} = \frac{1}{2} \left(\sup_{y \in B} \mu_{M\omega}(y) + 1 - \sup_{y \in R \setminus B} \mu_{M\omega}(y) \right).$$

Тогда запишем

$$M[\omega] = \frac{1}{2} \int_0^\infty \left(\sup_{y \geq r} \mu_{M\omega}(y) + 1 - \sup_{y < r} \mu_{M\omega}(y) \right) dr.$$

Предполагая, что случайные нечеткие величины $\xi(\theta)$ и $\eta(\theta)$ распределены по экспоненциальному закону, параметры которых являются треугольными нечеткими величинами, замечаем, что ожидаемые значения $M[\xi(\theta)]$ и $M[\eta(\theta)]$ можно записать аналогично соотношению (3).

Пример. Пусть случайные нечеткие величины χ , ξ , γ и η распределены по экспоненциальным законам, т.е.

$$F_\chi\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\chi(\theta)t}, F_\xi\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\xi(\theta)t}, F_\gamma\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\gamma(\theta)t} \text{ и } F_\eta\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\eta(\theta)t}.$$

Здесь будем строить функцию принадлежности на основе доверительных интервалов параметров распределения методом, предложенным Бакли [8]. Его сущность заключается в том, что функция принадлежности искомого параметра распределения определяется своими множествами α -уровня. При этом в качестве множества α -уровня берется интервальная оценка искомого параметра распределения с уровнем доверия $(1-\alpha)$. Доверительные границы для интенсивности отказов рассчитываются по следующим формулам [12]:

$$\lambda_i = \frac{\chi^2(1-\alpha_1, 2d)}{2nt_0}, \lambda_{\bar{a}} = \frac{\chi^2(\alpha_2, 2d)}{2nt_0},$$

где d – количество отказов за время t_0 , n – общее количество элементов данного наименования, t_0 – период эксплуатации (в часах). В данном случае $t_0 = 289080$ ч, λ_i – нижняя граница доверительного интервала, $\lambda_{\bar{a}}$ – верхняя граница доверительного интервала, α_1 – вероятность события $\lambda \geq \lambda_i$, α_2 – вероятность события $\lambda \leq \lambda_{\bar{a}}$, $\alpha = \alpha_1 + \alpha_2 - 1$ – вероятность события $\lambda_i \leq \lambda \leq \lambda_{\bar{a}}$, $\chi^2(s, r)$ – квантиль χ^2 распределения с параметром s числом степеней свободы r .

В этом случае функцию принадлежности ожидаемого значения наработки комплекса до аварии комплекса запишем так:

$$\mu_{M\omega}(y) = \sup_{y=f(x_1, x_2, x_3, x_4)} \min(\mu_{\lambda_\chi}(x_1), \mu_{\lambda_\gamma}(x_2), \mu_{\lambda_\xi}(x_3), \mu_{\lambda_\eta}(x_4)),$$

$$\text{где } f(x_1, x_2, x_3, x_4) = \frac{1}{q(x_3, x_4)} \frac{1}{x_1} + \frac{1 - q(x_3, x_4)}{q(x_3, x_4)} \frac{1}{x_2}, \quad q(x_3, x_4) \approx \frac{\frac{1}{x_3} \frac{\delta}{T + \delta} + \frac{T}{2} + \frac{1}{x_4}}{\frac{1}{x_3} + \frac{T + \delta}{2} + \frac{1}{x_4}}.$$

Простейшими методами дефаззификации являются: метод центра тяжести, метод центра площадей, метод левого модального значения, метод правого модального значения [11].

Причем $\mu_{\lambda_{\chi}}(x) = \Delta(1 \times 10^{-6} \text{ч}^{-1}, 1.5 \times 10^{-6} \text{ч}^{-1}, 2 \times 10^{-6} \text{ч}^{-1})$, $\mu_{\lambda_{\gamma}}(x) = \Delta(1 \text{ч}^{-1}, 1.5 \text{ч}^{-1}, 2 \text{ч}^{-1})$, $\mu_{\lambda_{\eta}}(x) = \Delta(1 \times 10^{-4} \text{ч}^{-1}, 1.5 \times 10^{-4} \text{ч}^{-1}, 2 \times 10^{-4} \text{ч}^{-1})$, $\mu_{\lambda_{\xi}}(x) = \Delta(1 \text{ч}^{-1}, 1.5 \text{ч}^{-1}, 2 \text{ч}^{-1})$, $T = 500 \text{ч}$, $\delta = 0.1 \text{ч}$. Здесь Δ обозначает треугольную функцию принадлежности. Тогда

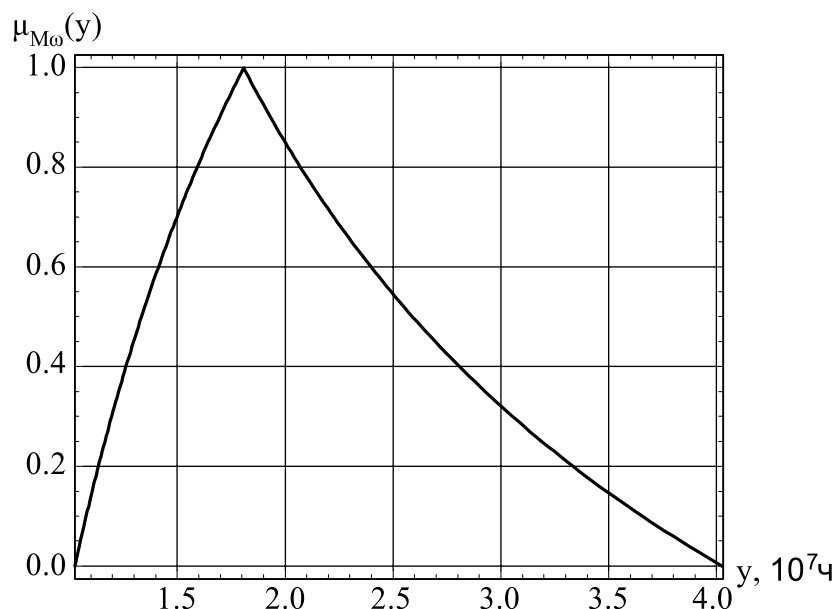


Рис. 1. Функция принадлежности средней наработки до аварии комплекса

При этом значение $M\omega$, вычисленное классическим способом, составляет $1.808 \times 10^7 \text{ч}$, что совпадает с максимумом функции принадлежности, а значение $M[\omega]$, полученное в результате процедуры дефаззификации, составляет $2.029 \times 10^7 \text{ч}$, что отражает асимметричность полученной функции принадлежности. Также оценили вклад каждого из нечетких параметров в неопределенность результата в соответствии с [8]. Так для параметра λ_{χ} получили 0.506858, для λ_{γ} – 0.4×10^{-7} , для λ_{ξ} – 0.491839, а для λ_{η} получили 0.00130296.

Заключение

Таким образом, в данной работе предложен подход к оценке средней наработки до аварии комплекса «объект защиты – система безопасности» с учетом неопределенности в задании неопределенностью исходных данных. Рассматривая процесс функционирования комплекса как случайно-нечеткий процесс восстановления, получены соотношения, позволяющие записать функцию принадлежности для средней наработки до аварии комплекса. Зная функцию принадлежности параметров комплекса, применяя процедуру дефаззификации, оценена средняя наработка до аварии комплекса.

Литература

1. Малашнин И.И., Перегуда А.И. Расчет и оптимизация надежности систем аварийной защиты ядерных реакторов. – М.: Энергоатомиздат, 1985 – 112 с.

2. **Перекуда А. И., Тимашов Д. А.** Математическая модель процесса функционирования автоматизированного технологического комплекса «объект защиты – система безопасности» с восстанавливаемыми элементами и периодическим контролем системы безопасности // Известия вузов. Ядерная энергетика. – 2007. – №3, вып. 2. – С. 101-109.
3. **Пытьев Ю. П.** Возможность как альтернатива вероятности. Математические и эмпирические основы, применение. – М.: Физматлит, 2007 – 464 с.
4. **Liu B.** Uncertainty Theory. – 2nd edition. – Berlin: Springer-Verlag, 2007. – 255 pp.
5. **Liu B.** Uncertainty Theory: An Introduction to Its Axiomatic Foundations. – Berlin: Springer-Verlag, 2004. – 411 pp.
6. **Kwakernaak H.** Fuzzy random variables – I. Definitions and theorems // Information Sciences. – 1978. – Vol. 15 – Pp. 1-29.
7. **Hanss M.** Applied Fuzzy Arithmetic: An Introduction with Engineering Applications. – Springer-Verlag, 2005. – 256 pp.
8. **Buckley J. J.** Fuzzy Probability and Statistics. – Springer-Verlag, 2006. – 270 p.
9. **Zhao R., Tang W., Yun H.** Random fuzzy renewal process // European Journal of Operational Research. – 2006. – Vol. 169. – Pp. 189-201.
10. **Shen Q., Zhao R., Tang W.** Random fuzzy alternating renewal processes // Soft Computing. – 2008. – Vol. 13, no. 2. – Pp. 139-147.
11. **Леоненко А.В.** Нечеткое моделирование в среде Matlab и fuzzyTECH. – СПб.: БХВ – Петербург, 2005. – 736 с.
12. **Байхельт Ф., Франкен П.** Надежность и техническое обслуживание. Математический подход: Пер. с нем. – М.: Радио и связь, 1988. – 392 с.

Pereguda A.I.

MATHEMATICAL MODEL OF DEPENDABILITY FOR A COMPLEX “FACILITY OF PROTECTION – SAFETY SYSTEM” IN CASE OF FUZZY INITIAL INFORMATION

The given paper considers the mathematical model of dependability for a complex “facility of protection – safety system” with a periodically controlled safety system. A random fuzzy process of recovery is used for construction of a dependability mathematical model, which takes into account the uncertainty of model parameters. A fuzzy estimation has been obtained for the mathematical expectation of a complex’s failure-free operating life, and the calculation of mean time to failure of a complex “facility of protection – safety system” has been exemplified.

Keywords: *dependability, random fuzzy variables, Zadeh’s extension principle, membership function, fuzzy mean time, estimation of dependability performance, defuzzification.*

Introduction

The complexes consisting of a protected facility and a safety system are applied where it is necessary to provide safe operation of potentially hazardous facilities. As an example, it is possible to consider the nuclear industry. A safety system is intended to shift emergencies into non-emergencies in case of violation of normal operation of a protected facility, i.e. to parry a protected facility failure. The considered system possesses the following typical features: it has a vertical hierarchy – the facility is under the control of a safety system; the safety system possesses the right of intervention to prevent potentially hazardous changes in a facility of protection; there is an interdependence of actions – the success of system actions as a whole depends on the behavior of all system elements. Whence it follows that a facility of protection and a safety system should be considered as a whole, as a common automated technological complex “facility of protection – safety system” (ATC FP-SS). Works [1, 2] are devoted to the development of a dependability mathematical model of such complex.

Uncertainty of analysis results caused by various reasons can take place when analyzing system dependability. In this work, we shall consider the uncertainty of results of dependability analysis caused by uncertainty of initial data. The given type of uncertainty arises as parameters of a mathematical model used for the analysis of system dependability cannot be precisely known owing to insufficiency of data and variability of characteristics.

Several approaches differing from each other have been developed for modeling various aspects of uncertainty, such as a theoretical probabilistic approach, fuzzy sets and measures, and some other methods. Discussion of their distinctions and advantages can be found in study [3]. Here we shall use a combination of a theoretical probabilistic approach and fuzzy measures for construction of a dependability mathematical model considering uncertainty of model parameters. The similar approach is stated in a number of studies [4 – 8]. In the present study following Lu [4, 5], we shall use random fuzzy variables as they allow to create in a most simple fashion the mathematical model of dependability of ATC FP-SS considering uncertainty of initial data. At the analysis of a dependability mathematical model, we switch over from random variables to random fuzzy variables, and, hence, there is a necessity for consideration of random fuzzy process of recovery, which is examined in works [9, 10].

Formalization and task solution

In development of dependability mathematical models, an approach is generally accepted when operating times and recovery times are described by means of random variables. For example, it is possible to consider time to failure χ with the function of distribution $F_\chi(t; \vec{\lambda})$, where $\vec{\lambda}$ is a vector of distribution parameters. However, as a rule, exact values of parameters $\vec{\lambda}$ by virtue of those or other reasons are not known, and there is uncertainty of model parameters that in turn leads to uncertainty of values of a required dependability parameter. For the quantitative account of this uncertainty, we shall take advantage of the mathematical tool of random fuzzy variables [4,5]. The essence of the used approach consists in the fact that the measure of likelihood is attributed to random variables. We shall define random fuzzy times to failure and recovery times using the approach considered in [4]. To set a random fuzzy variable χ , we shall specify the family of probabilistic distributions $\{F_\chi(t; \vec{\lambda}(\theta)), \theta \in \Theta\}$ on a probabilistic space (Ω, A, P) , where $\vec{\lambda}$ is a fuzzy vector defined on the space of likelihood (Θ, Π, Cr) to which the membership function $\mu_{\vec{\lambda}}(\vec{x})$ corresponds.

We shall use random fuzzy variables instead of random variables for construction of the dependability mathematical model of a complex "facility of protection – safety system". The essence of the given approach consists in the fact that we shall attribute a measure of likelihood to random variables.

Let us consider that values χ_i are random fuzzy quantities, each of which is specified on a corresponding space of likelihood (Θ_i, P_i, Cr_i) , and all of them are independent, positive and equally distributed. Similarly, γ_i is random fuzzy quantities, each of which is specified on a corresponding space of likelihood (Θ'_i, P'_i, Cr'_i) , and they are also independent, equally distributed and positive. The number of a process cycle of protected facility operation when there was a failure (an accident) we shall designate as v . Besides, we consider that v is a positive random fuzzy integer (i.e. a random fuzzy quantity which possesses only positive integers), defined on a space of likelihood (Θ'', P'', Cr'') . And, finally, let us suppose that sequences $\{\chi_i, i \geq 1\}$ and $\{\gamma_i, i \geq 1\}$ are mutually independent, and v is independent on sequences $\{\chi_i, i \geq 1\}$ and $\{\gamma_i, i \geq 1\}$.

The mean time to the first failure of a complex can be written as follows [2]:

$$\omega = \sum_{i=1}^{v-1} (\chi_i + \gamma_i) + \chi_v,$$

where χ_v is the time to failure on that cycle of regeneration on which a protected facility failed. Thus, ω is the random fuzzy quantity defined on a space of likelihood (Θ, P, Cr) where $\Theta = \Theta'' \times (\Theta_1 \times \Theta'_1) \times (\Theta_2 \times \Theta'_2) \times \dots$, and where Cr is the measure of likelihood defined as shown below [4,5]

$$Cr(A) = \begin{cases} \sup_{(\theta_1, \theta_2, \dots) \in A} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\}, & \text{if } \sup_{(\theta_1, \theta_2, \dots) \in A} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\} < \frac{1}{2}, \\ 1 - \sup_{(\theta_1, \theta_2, \dots) \in A^c} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\}, & \text{if } \sup_{(\theta_1, \theta_2, \dots) \in A} \inf_{1 \leq k \leq \infty} Cr_k \{\theta_k\} \geq \frac{1}{2} \end{cases}$$

For every fixed θ , the quantities $M\chi_i(\theta)$, $M\gamma_i(\theta)$, $Mv(\theta)$ and $M\omega(\theta)$ represent expectations of random variables $\chi(\theta)$, $\gamma(\theta)$, $v(\theta)$ and $\omega(\theta)$ respectively. As θ varies on the set Θ , then we already consider fuzzy quantities $M\chi_i(\theta)$, $M\gamma_i(\theta)$, $Mv(\theta)$, $M\omega(\theta)$. For measurement of a fuzzy quantity, two critical values (optimistic and pessimistic values) with the specified confidential level α are used [5]. Thus, we can consider the following α -pessimistic and α -optimistic values of these expectations:

$$(M\chi_i(\theta))_{\sup}(\alpha) = \sup \{r \mid Cr \{M\chi_i(\theta) \geq r\} \geq \alpha\},$$

$$(M\chi_i(\theta))_{\inf}(\alpha) = \inf \{r \mid Cr \{M\chi_i(\theta) \leq r\} \geq \alpha\},$$

$$(M\gamma_i(\theta))_{\sup}(\alpha) = \sup \{r \mid Cr \{M\gamma_i(\theta) \geq r\} \geq \alpha\},$$

$$(M\gamma_i(\theta))_{\inf}(\alpha) = \inf \{r \mid Cr \{M\gamma_i(\theta) \leq r\} \geq \alpha\},$$

$$(Mv(\theta))_{\sup}(\alpha) = \sup \{r \mid Cr \{Mv(\theta) \geq r\} \geq \alpha\},$$

$$(Mv(\theta))_{\inf}(\alpha) = \inf \{r \mid Cr \{Mv(\theta) \leq r\} \geq \alpha\},$$

$$(M\omega(\theta))_{\sup}(\alpha) = \sup \{r \mid Cr \{M\omega(\theta) \geq r\} \geq \alpha\},$$

$$(M\omega(\theta))_{\inf}(\alpha) = \inf \{r \mid Cr \{M\omega(\theta) \leq r\} \geq \alpha\}.$$

For each $\theta \in \Theta$, the following equality is true

$$M\omega(\theta) = M \left(\sum_{i=1}^{v(\theta)-1} (\chi_i(\theta) + \gamma_i(\theta)) + \chi_{v(\theta)}(\theta) \right).$$

Using the formula of total probability and definition of critical values α , we shall calculate α -pessimistic value $M\omega(\theta)$. Then

$$\begin{aligned}
 (M\omega(\theta))_{\inf}(\alpha) &= M \left[\sum_{i=1}^{v(\cdot)-1} (\chi_i(\theta) + \gamma_i(\theta)) + \chi_{v(\theta)}(\theta) \right]_{\inf}(\alpha) = \\
 &= \sum_{k=1}^{\infty} \left(P(\theta) = k \sum_{i=1}^{k-1} (M\chi_i(\theta) + M\gamma_i(\theta)) + M\chi_k(\theta) \right)_{\inf}(\alpha) = \\
 &= \sum_{k=1}^{\infty} P(v(\theta) = k)_{\inf}(\alpha) \left(\sum_{i=1}^{k-1} (M\chi_i(\theta) + M\gamma_i(\theta)) + M\chi_k(\theta) \right)_{\inf}(\alpha) = \\
 &= \sum_{k=1}^{\infty} P(v(\theta) = k)_{\inf}(\alpha) \left(\sum_{i=1}^{k-1} ((M\chi_i(\theta))_{\inf}(\alpha) + (M\gamma_i(\theta))_{\inf}(\alpha)) + (M\chi_k(\theta))_{\inf}(\alpha) \right) = \\
 &= \left(M\chi(\theta) \sum_{k=1}^{\infty} P(v(\theta) = k) \right)_{\inf}(\alpha) + \left((M\chi(\theta) + M\gamma(\theta)) \sum_{k=1}^{\infty} (k-1) P(v(\theta) = k) \right)_{\inf}(\alpha) = \\
 &= ((M\chi(\theta))_{\inf}(\alpha) + (M\gamma(\theta))_{\inf}(\alpha))(Mv(\theta) - 1)_{\inf}(\alpha) + (M\chi(\theta))_{\inf}(\alpha).
 \end{aligned}$$

It can be similarly shown that α -optimistic value $M\omega(\theta)$ is defined by the following ratio

$$(M\omega(\theta))_{\sup}(\alpha) = ((M\chi(\theta))_{\sup}(\alpha) + (M\gamma(\theta))_{\sup}(\alpha))(Mv(\theta) - 1)_{\sup}(\alpha) + (M\chi(\theta))_{\sup}(\alpha).$$

Let us calculate now the average expected value of a random fuzzy quantity which is defined by the formula $E[\xi] = \frac{1}{2} \int_0^1 (\xi_{\sup}(\alpha) + \xi_{\inf}(\alpha)) d\alpha$ [5,6], and we shall obtain the following

$$\begin{aligned}
 E[M\omega(\theta)] &= \frac{1}{2} \int_0^1 ((M\chi)_{\inf}(\alpha)(Mv(\theta))_{\inf}(\alpha) + (M\gamma(\theta))_{\inf}(\alpha)(Mv(\theta) - 1)_{\inf}(\alpha)) d\alpha + \\
 &+ \frac{1}{2} \int_0^1 ((M\chi(\theta))_{\sup}(\alpha)(Mv(\theta))_{\sup}(\alpha) + (M\gamma(\theta))_{\sup}(\alpha)(Mv(\theta) - 1)_{\sup}(\alpha)) d\alpha = \\
 &= \frac{1}{2} \int_0^1 ((M\chi(\theta))_{\inf}(\alpha)(Mv(\theta))_{\inf}(\alpha) + (M\chi(\theta))_{\sup}(\alpha)(Mv(\theta))_{\sup}(\alpha)) d\alpha + \\
 &+ \frac{1}{2} \int_0^1 ((M\gamma(\theta))_{\inf}(\alpha)(Mv(\theta) - 1)_{\inf}(\alpha) + (M\gamma(\theta))_{\sup}(\alpha)(Mv(\theta) - 1)_{\sup}(\alpha)) d\alpha.
 \end{aligned}$$

Thus, we obtain

$$E[M\omega(\theta)] = M\chi(\theta) + M\chi(\theta)(v(\theta) - 1) + M\gamma(\theta)(v(\theta) - 1). \quad (1)$$

From the definition of the average expected value of a random fuzzy quantity it follows that $M[\omega] = E[M\omega]$.

Practical use of the theory of fuzzy quantities assumes presence of membership functions. At the further calculation of the expectation of random fuzzy quantity $M[\omega]$, it is necessary to determine a membership function.

Let the mean time between failures of a facility of protection have an exponential distribution which parameter is a triangular fuzzy quantity. Then the mean time between failures of a facility of protection is a random fuzzy quantity. In addition to that, we shall assume that recovery time of a facility of protection has also an exponential distribution which parameter is a triangular fuzzy quantity. We believe that the number of a cycle v on which there was a failure, also is a casual fuzzy quantity, and the probability of a failure on one cycle of operation process of a complex is equal to q .

Thus, proceeding from the assumptions made above, we shall write down:

$$P\{\chi(\theta) \leq t\} = \begin{cases} 1 - e^{-\lambda_\chi(\theta)t}, & \text{if } 0 \leq t < \infty, \\ 0, & \text{if } t < 0. \end{cases}$$

Let us note that a triangular fuzzy quantity $\lambda_\chi(\theta)$ can be represented by a group of three discrete numbers $(\lambda_\chi^{(1)}, \lambda_\chi^{(2)}, \lambda_\chi^{(3)})$ in such a way that $\lambda_\chi^{(1)} < \lambda_\chi^{(2)} < \lambda_\chi^{(3)}$, and its membership function is defined by expression of the following form

$$\mu_{\lambda_\chi}(y_1) = \begin{cases} \frac{y_1 - \lambda_\chi^{(1)}}{\lambda_\chi^{(2)} - \lambda_\chi^{(1)}}, & \text{if } y_1 \in [\lambda_\chi^{(1)}, \lambda_\chi^{(2)}], \\ \frac{y_1 - \lambda_\chi^{(3)}}{\lambda_\chi^{(2)} - \lambda_\chi^{(3)}}, & \text{if } y_1 \in [\lambda_\chi^{(2)}, \lambda_\chi^{(3)}], \\ 0, & \text{if } y_1 \notin [\lambda_\chi^{(1)}, \lambda_\chi^{(3)}]. \end{cases}$$

Let us similarly write down the expression for a fuzzy quantity $\lambda_\gamma(\theta)$

$$P\{\gamma(\theta) \leq t\} = \begin{cases} 1 - e^{-\lambda_\gamma(\theta)t}, & \text{if } 0 \leq t < \infty, \\ 0, & \text{if } t < 0 \end{cases}$$

$$\mu_{\lambda_\gamma}(y_2) = \begin{cases} \frac{y_2 - \lambda_\gamma^{(1)}}{\lambda_\gamma^{(2)} - \lambda_\gamma^{(1)}}, & \text{if } y_2 \in [\lambda_\gamma^{(1)}, \lambda_\gamma^{(2)}], \\ \frac{y_2 - \lambda_\gamma^{(3)}}{\lambda_\gamma^{(2)} - \lambda_\gamma^{(3)}}, & \text{if } y_2 \in [\lambda_\gamma^{(2)}, \lambda_\gamma^{(3)}], \\ 0, & \text{if } y_2 \notin [\lambda_\gamma^{(1)}, \lambda_\gamma^{(3)}]. \end{cases}$$

As the considered process of protected facility operation is an alternating random process, then the probability of the failure occurring on the k -th cycle of regeneration is equal as shown below

$$P\{v = k\} = (1 - q)^{(k-1)} q. \quad (2)$$

In this case, it is not possible to explicitly write the expression for a membership function of the quantity $M\omega$, however it is possible to calculate $E[\omega]$. It is obvious that

$$M[\omega] = M\left[\frac{1}{q\lambda_\chi} + \frac{1-q}{q\lambda_\gamma}\right] = \frac{1}{q} M\left[\frac{1}{\lambda_\chi}\right] + \frac{1-q}{q} M\left[\frac{1}{\lambda_\gamma}\right].$$

In the obtained expression, there were unknown expected values $M\left[\frac{1}{\lambda_\chi}\right]$ and $M\left[\frac{1}{\lambda_\gamma}\right]$ which should be calculated. The expectation of a fuzzy quantity $M\left[\frac{1}{\lambda_\chi}\right]$ shall be calculated as follows:

$$M\left[\frac{1}{\lambda_\chi}\right] = \int_0^{+\infty} Cr \left\{ \theta \in \Theta / \frac{1}{\lambda_\chi(\theta)} \geq r \right\} dr.$$

Before to calculate $M\left[\frac{1}{\lambda_\chi}\right]$, first it is necessary to define the corresponding membership function:

$$\mu(y) = \sup_{y=\frac{1}{y_1}} \mu_{\lambda_\chi}(y_1) = \begin{cases} \frac{\frac{1}{y_1} - \lambda_\chi^{(1)}}{\lambda_\chi^{(2)} - \lambda_\chi^{(1)}}, & \text{if } y \in \left[\frac{1}{\lambda_\chi^{(2)}}, \frac{1}{\lambda_\chi^{(1)}}\right] \\ \frac{\frac{1}{y_1} - \lambda_\chi^{(3)}}{\lambda_\chi^{(2)} - \lambda_\chi^{(3)}}, & \text{if } y \in \left[\frac{1}{\lambda_\chi^{(3)}}, \frac{1}{\lambda_\chi^{(2)}}\right] \\ 0, & \text{if } y \notin \left[\frac{1}{\lambda_\chi^{(3)}}, \frac{1}{\lambda_\chi^{(1)}}\right] \end{cases}.$$

Then the measure of likelihood can be written down in the following form

$$Cr\left\{\theta \in \Theta / \frac{1}{\lambda_{\chi}(\theta)} \geq r\right\} = \begin{cases} 1, & \text{if } r \leq \frac{1}{\lambda_{\chi}^{(3)}} \\ 1 - \frac{1}{2} \frac{\frac{1}{r} - \lambda_{\chi}^{(3)}}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(3)}}, & \text{if } r \in \left[\frac{1}{\lambda_{\chi}^{(3)}}, \frac{1}{\lambda_{\chi}^{(2)}}\right] \\ \frac{1}{2} \frac{\frac{1}{r} - \lambda_{\chi}^{(1)}}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(1)}}, & \text{if } r \in \left[\frac{1}{\lambda_{\chi}^{(2)}}, \frac{1}{\lambda_{\chi}^{(1)}}\right] \\ 0, & \text{if } r > \frac{1}{\lambda_{\chi}^{(1)}} \end{cases}.$$

Consequently, we obtain

$$M\left[\frac{1}{\lambda_{\chi}}\right] = \int_0^{+\infty} Cr\left\{\theta \in \Theta / \frac{1}{\lambda_{\chi}(\theta)} \geq r\right\} dr = \frac{1}{2} \frac{1}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(1)}} \ln\left(\frac{\lambda_{\chi}^{(2)}}{\lambda_{\chi}^{(1)}}\right) + \frac{1}{2} \frac{1}{\lambda_{\chi}^{(3)} - \lambda_{\chi}^{(2)}} \ln\left(\frac{\lambda_{\chi}^{(3)}}{\lambda_{\chi}^{(2)}}\right). \quad (3)$$

The expectation of a fuzzy quantity $M\left[\frac{1}{\lambda_{\gamma}}\right]$ can be written down similarly to (3), that is

$$M\left[\frac{1}{\lambda_{\gamma}}\right] = \frac{1}{2} \frac{1}{\lambda_{\gamma}^{(2)} - \lambda_{\gamma}^{(1)}} \ln\left(\frac{\lambda_{\gamma}^{(2)}}{\lambda_{\gamma}^{(1)}}\right) + \frac{1}{2} \frac{1}{\lambda_{\gamma}^{(3)} - \lambda_{\gamma}^{(2)}} \ln\left(\frac{\lambda_{\gamma}^{(3)}}{\lambda_{\gamma}^{(2)}}\right).$$

Let us now define Mv . As v is a discrete random variable, then

$$Mv = \sum_{k=1}^{\infty} kq(1-q)^{k-1} = q.$$

We substitute the obtained expressions $M\left[\frac{1}{\lambda_{\gamma}}\right]$, $M\left[\frac{1}{\lambda_{\chi}}\right]$ and Mv in the formula $M[\omega]$ and obtain the following

$$M[\omega] = \frac{1}{2q} \left\{ \frac{1}{\lambda_{\chi}^{(2)} - \lambda_{\chi}^{(1)}} \ln\left(\frac{\lambda_{\chi}^{(2)}}{\lambda_{\chi}^{(1)}}\right) + \frac{1}{\lambda_{\chi}^{(3)} - \lambda_{\chi}^{(2)}} \ln\left(\frac{\lambda_{\chi}^{(3)}}{\lambda_{\chi}^{(2)}}\right) \right\} + \\ + \frac{1-q}{2q} \left\{ \frac{1}{\lambda_{\gamma}^{(2)} - \lambda_{\gamma}^{(1)}} \ln\left(\frac{\lambda_{\gamma}^{(2)}}{\lambda_{\gamma}^{(1)}}\right) + \frac{1}{\lambda_{\gamma}^{(3)} - \lambda_{\gamma}^{(2)}} \ln\left(\frac{\lambda_{\gamma}^{(3)}}{\lambda_{\gamma}^{(2)}}\right) \right\}.$$

It should be noted that if $\lambda_{\chi}^{(1)} = \lambda_{\chi}^{(2)} = \lambda_{\chi}^{(3)}$ and $\lambda_{\gamma}^{(1)} = \lambda_{\gamma}^{(2)} = \lambda_{\gamma}^{(3)}$, the obtained expression is reduced to expression for calculation of an expectation in case when parameters of distributions are discrete quantities.

To calculate $M\omega(\theta)$, as mathematical expectation of a fuzzy quantity, it is necessary to obtain a ratio for the probability $q(\theta)$ at each fixed $\theta \in \Theta$ since values $M\chi(\theta)$ and $M\gamma(\theta)$ have been calculated above. Let us consider the operation process of a safety system in more detail. As a safety system operates in a protected facility failure expectation mode of expectation, it is impossible to detect its failures during the moment of their occurrence. Therefore, for detection of latent failures, the procedure of the periodic preventive control of a safety system is introduced. We shall designate the period of the control of a safety system's operability as T , and its duration as δ . We assume that during the periodic control, a safety system stops to carry out its functions. If a safety system has regularly operated over the time ξ_i on the i -th cycle of regeneration, then for this period of time there has been made $\left\lfloor \frac{\xi_i}{T+\delta} \right\rfloor$ ($[x]$, $\{x\}$ are the integer and the fractional part of the number x , $x^+ = \max(x, 0)$ respectively) periods of control preventive maintenance. And for this time, the system has been in upstate for the time equal to $\left\lfloor \frac{\xi_i}{T+\delta} \right\rfloor T$. A failure F is detected only during the moments of time $\left(\left\lfloor \frac{\xi_i}{T+\delta} \right\rfloor + 1 \right) (T + \delta)$, i.e. during the moments of control procedure termination. After carrying out corresponding repair-and-renewal operations with the duration η_i a safety system starts again to function regularly. Thus, the process of safety system functioning with control preventive maintenance is a random process with the period of regeneration

$$\tau_F(\xi, \eta) = (T + \delta) \left(\left\lfloor \frac{\xi}{T + \delta} \right\rfloor + 1 \right) + \eta.$$

Thus, the failure of a complex occurs in case when a protected facility's failure falls down on a downstate of a safety system. The moments of regeneration of a complex's operation process will be the moments of the termination of protected facility recovery.

Considering the independence of examined quantities, the ratio (1) can be written down for each fixed $\theta \in \Theta$ in the following form

$$\begin{aligned} E[\omega(\theta)] &= \frac{1}{q(\theta)} M\chi(\theta) + \frac{1-q(\theta)}{q(\theta)} M\gamma(\theta) = \\ &= \frac{1}{q(\theta)} \int_0^\infty (1 - F_\chi(t; \tilde{\lambda}_\chi(\theta))) dt + \frac{1-q(\theta)}{q(\theta)} \int_0^\infty (1 - F_\gamma(t; \tilde{\lambda}_\gamma(\theta))) dt, \end{aligned} \quad (4)$$

where $q(\theta)$ is the probability of a failure on a cycle of a complex's operation process regeneration $F_\chi(t; \tilde{\lambda}_\chi(\theta))$, $F_\gamma(t; \tilde{\lambda}_\gamma(\theta))$ are probabilistic distributions for random fuzzy variables χ and γ respectively.

For calculation of the probability $q(\theta)$, we shall designate the set of the moments of time during which the safety system is capable to parry failures of a facility under protection as $Q^+(\theta)$ and the set of the moments of time during which the safety system is not capable to parry failures of a facility under protection as $Q^-(\theta)$. Then we shall calculate the probability $q(\theta)$ for each fixed $\theta \in \Theta$ as follows:

$$q(\theta) = \int_0^{\infty} P(t \in Q^-(\theta)) dF_{\chi}(t; \vec{\lambda}_{\chi}(\theta)).$$

Noticing that

$$P(t \in Q^-(\theta)) = 1 - P(t \in Q^+(\theta)) = 1 - P^+(t; \theta).$$

Then, according to the formula of total probability, we shall write down

$$P^+(t; \theta) = \int_0^{\infty} \int_0^{\infty} P(t \in Q^+(\theta) | \xi(\theta) = x, \eta(\theta) = y) dF_{\eta}(y; \vec{\lambda}_{\eta}(\theta)) dF_{\xi}(x; \vec{\lambda}_{\xi}(\theta)).$$

Let us remind that ξ is a random operating time to the first latent failure of a safety system, and η is the random time of a safety system's recovery after the first latent failure. For calculation of $P^+(t; \theta)$, there are only two possible mutually exclusive alternatives: $\tau_{CB}(\xi, \eta) > t$ and $\tau_F(\xi, \eta) \leq t$. Therefore, we shall present $P^+(t)$ in the form of the sum of two summands [2]:

$$P^+(t; \theta) = \iint_{\tau_{CB}(x, y) \leq t} P(t \in Q^+(\theta) | \xi(\theta) = x, \eta(\theta) = y) dF_{\eta}(y; \vec{\lambda}_{\eta}(\theta)) dF_{\xi}(x; \vec{\lambda}_{\xi}(\theta)) + \\ + \iint_{\tau_{CB}(x, y) > t} P(t \in Q^+(\theta) | \xi(\theta) = x, \eta(\theta) = y) dF_{\eta}(y; \vec{\lambda}_{\eta}(\theta)) dF_{\xi}(x; \vec{\lambda}_{\xi}(\theta)) = I_1 + I_2.$$

At first, let us calculate the second summand I_2 . The condition $\tau_F(x, y) > t$ means that the moment of regeneration of a safety system's operation process has come after the moment of time t . Taking into account this condition, we shall transform I_2 as follows:

$$I_2 = \iint_{\tau_{CB}(x, y) > t} \left(\sum_{m=0}^{\left\lceil \frac{x}{T+\delta} \right\rceil - 1} J_{t \in [m(T+\delta), m(T+\delta)+T)} + J_{t \in \left[\left\lceil \frac{x}{T+\delta} \right\rceil (T+\delta), x \right)} \right) dF_{\eta}(y; \vec{\lambda}_{\eta}(\theta)) dF_{\xi}(x; \vec{\lambda}_{\xi}(\theta)) = \\ = \int_0^{\infty} \left(\sum_{m=0}^{\left\lceil \frac{x}{T+\delta} \right\rceil - 1} J_{t \in [m(T+\delta), m(T+\delta)+T)} + J_{t \in \left[\left\lceil \frac{x}{T+\delta} \right\rceil (T+\delta), x \right]} \right) \left(1 - F_{\eta} \left(t - \left(\left\lceil \frac{x}{T+\delta} \right\rceil + 1 \right) (T+\delta); \vec{\lambda}_{\eta}(\theta) \right) \right) dF_{\xi}(x; \vec{\lambda}_{\xi}(\theta)),$$

where $J_{t \in A}$ is the indicator of event $t \in A$.

Omitting some simple but bulky transformations, we shall give the result at once:

$$I_2 = \left(1 - F_{\xi}(t; \bar{\lambda}_{\xi}(\theta))\right) - \sum_{m=1}^{\infty} \left(1 - F_{\xi}(m(T+\delta); \bar{\lambda}_{\xi}(\theta))\right) \left(J_{(m-1)(T+\delta)+T \leq t} - J_{m(T+\delta) \leq t}\right).$$

It should be noted that $1 - \sum_{m=1}^{\infty} (1 - F_{\xi}(m(T+\theta))) (J_{(m-1)(T+\theta) \leq t} - J_{m(T+\theta) \leq t})$ represents the distribution function $F_{\zeta}(t)$ of some random variable ζ that allows one to present I_2 in the following form

$$I_2 = F_{\zeta}(t; \bar{\lambda}_{\xi}(\theta)) - F_{\xi}(t; \bar{\lambda}_{\xi}(\theta)). \quad (5)$$

Now let us consider I_1 . When considering the case $\tau_F \leq t$, we shall take into account that after carrying out corresponding repair-and-renewal operations during the moment of time τ_F , a safety system will again function with the same probabilistic characteristics, as during the moment of time $t = 0$. Then

$$I_1 = \iint_{\tau_{CB}(x,y) \leq t} P^+(t - \tau_{CB}(x,y)) dF_{\eta}(y; \bar{\lambda}_{\eta}(\theta)) dF_{\xi}(x; \bar{\lambda}_{\xi}(\theta)) = \int_0^t P^+(t - z) dF_{\tau_{CB}}(z; \bar{\lambda}_{\eta}(\theta), \bar{\lambda}_{\xi}(\theta)). \quad (6)$$

Thus, by summarizing (5) and (6), for each fixed $\theta \in \Theta$, we obtain the Volterra type integrated equation of the second kind for the probability $P(t \in Q^+(\theta))$:

$$P^+(t; \theta) = f(t; \theta) + \int_0^t P^+(t - z) dF_{\tau_F}(z; \bar{\lambda}_{\eta}(\theta), \bar{\lambda}_{\xi}(\theta)), \quad (7)$$

where $f(t; \theta) = F_{\zeta}(t; \bar{\lambda}_{\xi}(\theta)) - F_{\xi}(t; \bar{\lambda}_{\xi}(\theta))$,

$$F_{\tau_F}(z; \bar{\lambda}_{\eta}(\theta), \bar{\lambda}_{\xi}(\theta)) = P\left(\left[\left[\frac{\xi(\theta)}{T+\delta}\right] + 1\right](T+\delta) + \eta(\theta) \leq z\right).$$

As equation (7) is a convolution equation, then for its solution we use the Laplace-Stieltjes transform. The solution of equation (7) in terms of the Laplace-Stieltjes transform has the following form

$$\tilde{P}^+(s; \theta) = \frac{\tilde{f}(s; \theta)}{1 - \tilde{F}_{\tau_F}(s; \bar{\lambda}_{\eta}(\theta), \bar{\lambda}_{\xi}(\theta))} = \frac{Me^{-s\zeta(\theta)} - Me^{-s\xi(\theta)}}{1 - Me^{-s\tau_F(\theta)}},$$

where $\tilde{P}^+(s; \theta) = \int_0^{\infty} e^{-st} dP^+(t; \theta)$, $\tilde{F}_{\tau_F}(s; \bar{\lambda}_{\eta}(\theta), \bar{\lambda}_{\xi}(\theta)) = \int_0^{\infty} e^{-st} dF_{\tau_F}(t; \bar{\lambda}_{\eta}(\theta), \bar{\lambda}_{\xi}(\theta))$ and $\tilde{f}(s; \theta) = \int_0^{\infty} e^{-st} df(t; \theta) = \int_0^{\infty} e^{-st} dF_{\zeta}(t; \bar{\lambda}_{\xi}(\theta)) - \int_0^{\infty} e^{-st} dF_{\xi}(t; \bar{\lambda}_{\xi}(\theta))$.

Due to the difficulty of finding a reverse conversion of the Laplace-Stieltjes transform in the analytical form, it is not possible, so we shall find an asymptotic ratio for $P^+(t; \theta)$ applying a known ratio $\lim_{t \rightarrow \infty} P^+(t; \theta) = \lim_{s \rightarrow 0} \tilde{P}^+(s; \theta)$. Applying the specified ratio, we obtain

$$\lim_{t \rightarrow \infty} P^+(t; \theta) = \frac{M\xi(\theta) - M\zeta(\theta)}{M\tau_F(\theta)}.$$

It is obvious that now it is necessary to calculate expressions for expectations $M\zeta(\theta)$, $M\xi(\theta)$ and $M\tau_F(\theta)$. And $M\zeta(\theta) = \int_0^\infty (1 - F_\zeta(t; \bar{\lambda}_\xi(\theta))) dt$, then

$$\begin{aligned} M\zeta(\theta) &= \int_0^\infty \sum_{m=1}^\infty (1 - F_\xi(k(T + \delta); \bar{\lambda}_\xi(\theta))) (J_{(m+1)(T+\delta)+T \leq t} - J_{m(T+\delta) \leq t}) dt = \\ &= \sum_{k=0}^\infty k\delta (F_\xi((k+1)(T + \delta); \bar{\lambda}_\xi(\theta)) - F_\xi(k(T + \delta); \bar{\lambda}_\xi(\theta))) = \sum_{k=0}^\infty k\delta P\left(\left\lfloor \frac{\xi(\theta)}{T + \delta} \right\rfloor = k\right) = \delta M\left[\frac{\xi(\theta)}{T + \delta}\right]. \end{aligned}$$

As $\xi(\theta) \gg T + \delta$, $\left\lfloor \frac{\xi(\theta)}{T + \delta} \right\rfloor \cong \frac{\xi(\theta)}{T + \delta} - \frac{1}{2}$ [1] that allows to rewrite $M\zeta(\theta)$ for each fixed $\theta \in \Theta$. Therefore, we have $M\zeta(\theta) = M\xi(\theta) \frac{\delta}{T + \delta} - \frac{\delta}{2}$. Then

$$M\xi(\theta) - M\zeta(\theta) = M\xi(\theta) \frac{T}{T + \delta} + \frac{\delta}{2} \text{ And } M\tau_F(\theta) = M\eta(\theta) + \frac{T + \delta}{2} + M\xi(\theta).$$

$$\lim_{t \rightarrow \infty} P^+(t; \theta) = \frac{M\xi(\theta) \frac{T}{T + \delta} + \frac{\delta}{2}}{M\xi(\theta) + \frac{T + \delta}{2} + M\eta(\theta)}.$$

It should be noted that $M\eta(\theta)$ $M\xi(\theta)$ can be calculated similarly to expectations $M\chi(\theta)$ and $M\gamma(\theta)$. For the probability $q(\theta)$ for each fixed $\theta \in \Theta$, we can write down the following asymptotic estimation:

$$q(\theta) \approx 1 - \lim_{t \rightarrow \infty} P^+(t; \theta) = \frac{M\xi(\theta) \frac{\delta}{T + \delta} + \frac{T}{2} + M\eta(\theta)}{M\xi(\theta) + \frac{T + \delta}{2} + M\eta(\theta)}.$$

Thus, we have obtained the ratio for all quantities in equation (1). Now we can calculate $M[\omega(\theta)]$ for each fixed $\theta \in \Theta$ under the formula

$$M[\omega(\theta)] = \frac{\left(M\xi(\theta) + \frac{T+\delta}{2} + M\eta(\theta)\right)M\chi(\theta) + \left(M\xi(\theta)\frac{T}{T+\delta} + \frac{\delta}{2}\right)M\gamma(\theta)}{M\xi(\theta)\frac{\delta}{T+\delta} + \frac{T}{2} + M\eta(\theta)},$$

where $M\chi(\theta) = \int_0^\infty (1 - F_\chi(t; \tilde{\lambda}_\chi(\theta)))dt$, $M\xi(\theta) = \int_0^\infty (1 - F_\xi(t; \tilde{\lambda}_\xi(\theta)))dt$, $M\gamma(\theta) = \int_0^\infty (1 - F_\gamma(t; \tilde{\lambda}_\gamma(\theta)))dt$

and $M\eta(\theta) = \int_0^\infty (1 - F_\eta(t; \tilde{\lambda}_\eta(\theta)))dt$.

Consequently, according to the definition of fuzzy values function [4,5], we have given a fuzzy expectation of mean operating time to the first failure as function of model fuzzy parameters.

Now we shall take advantage of Zadeh's extension principle [6]:

$$\mu(x) = \sup_{x=f(x_1, x_2, \dots, x_n)} \min_{1 \leq i \leq n} \mu_i(x_i)$$

and write down a ratio for the membership function $M\omega(\theta)$:

$$\mu_{M\omega}(y) = \sup_{y=f(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4)} \min(\mu_{\tilde{\lambda}_\chi}(\tilde{x}_1), \mu_{\tilde{\lambda}_\gamma}(\tilde{x}_2), \mu_{\tilde{\lambda}_\xi}(\tilde{x}_3), \mu_{\tilde{\lambda}_\eta}(\tilde{x}_4)),$$

Where

$$f(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4) = \frac{\left(M\xi(\tilde{x}_3) + \frac{T+\delta}{2} + M\eta(\tilde{x}_4)\right)M\chi(\tilde{x}_1) + \left(M\xi(\tilde{x}_3)\frac{T}{T+\delta} + \frac{\delta}{2}\right)M\gamma(\tilde{x}_2)}{M\xi(\tilde{x}_3)\frac{\delta}{T+\delta} + \frac{T}{2} + M\eta(\tilde{x}_4)}.$$

Thus, we have managed to write down a ratio for membership function of the expected value of a complex's operating time to failure through membership functions of model parameters.

Now let us consider the defuzzification procedure, i.e. the transformation of a fuzzy set into a discrete quantity. For this purpose, we shall take advantage of the definition of the average expected value of random fuzzy variables [6]:

$$M[\omega(\theta)] = \int_0^\infty Cr\{\theta \in \Theta \mid M\omega(\theta) \geq r\}dr - \int_{-\infty}^0 Cr\{\theta \in \Theta \mid M\omega(\theta) \leq r\}dr.$$

Let us find a corresponding measure of likelihood using a ratio connecting a measure of likelihood and a membership function [5]:

$$Cr\{M\omega \in B\} = \frac{1}{2} \left(\sup_{y \in B} \mu_{M\omega}(y) + 1 - \sup_{y \in R \setminus B} \mu_{M\omega}(y) \right).$$

Then we shall write down

$$M[\omega] = \frac{1}{2} \int_0^\infty \left(\sup_{y \geq r} \mu_{M\omega}(y) + 1 - \sup_{y < r} \mu_{M\omega}(y) \right) dr.$$

Assuming that random fuzzy quantities $\xi(\theta)$ and $\eta(\theta)$ are distributed according to the exponential law which parameters are triangular fuzzy quantities, we can see that expected values $M[\xi(\theta)]$ and $M[\eta(\theta)]$ can be written down similarly to ratio (3).

An example

Let random fuzzy quantities χ , ξ , γ and η be distributed according to the exponential law; i.e.

$$F_\chi\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\chi(\theta)t}, \quad F_\xi\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\xi(\theta)t}, \quad F_\gamma\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\gamma(\theta)t} \quad \text{and} \\ F_\eta\{t; \lambda(\theta)\} = 1 - e^{-\lambda_\eta(\theta)t}.$$

Here we shall construct a membership function based on distribution parameters' confidential intervals using the method offered by J. Buckley [8]. Its essence consists in the fact that the membership function of a required distribution parameter is defined by its sets of α -level. In this case the interval estimation of the required parameter of distribution with a confidence level $(1 - \alpha)$ is taken as a set of α -level. Confidence limits for a failure rate are calculated under the following formulas [12]:

$$\lambda_i = \frac{\chi^2(1 - \alpha_1, 2d)}{2nt_0}, \quad \lambda_{\hat{a}} = \frac{\chi^2(\alpha_2, 2d)}{2nt_0},$$

where d is the number of failures over the time t_0 , n is the total number of elements of the given name, t_0 is the time of operation (in hours). In this case $t_0 = 289080$ h, λ_i is the lower limit of the confidential interval, $\lambda_{\hat{a}}$ is the upper limit of the confidential interval, α_1 is the probability of the event $\lambda \geq \lambda_i$, α_2 is the probability of the event $\lambda \leq \lambda_{\hat{a}}$, $\alpha = \alpha_1 + \alpha_2 - 1$ is the probability of event $\lambda_i \leq \lambda \leq \lambda_{\hat{a}}$, $\chi^2(s, r)$ is the quantile of χ^2 distribution with a parameter s and the number of degrees of freedom r .

In this case, the membership function of the expected value of a complex operating time before failure we shall write down as follows:

$$\mu_{M\omega}(y) = \sup_{y=f(x_1, x_2, x_3, x_4)} \min(\mu_{\lambda_\chi}(x_1), \mu_{\lambda_\gamma}(x_2), \mu_{\lambda_\xi}(x_3), \mu_{\lambda_\eta}(x_4)),$$

$$\text{where } f(x_1, x_2, x_3, x_4) = \frac{1}{q(x_3, x_4)} \frac{1}{x_1} + \frac{1 - q(x_3, x_4)}{q(x_3, x_4)} \frac{1}{x_2}, \quad q(x_3, x_4) \approx \frac{\frac{1}{x_3} \frac{\delta}{T + \delta} + \frac{T}{2} + \frac{1}{x_4}}{\frac{1}{x_3} + \frac{T + \delta}{2} + \frac{1}{x_4}}.$$

The elementary methods of defuzzification are: the method of the centre of gravity, the method of the center of areas, the method of the left modal value and the method of the right modal value [11].

In this case $\mu_{\lambda_x}(x) = \Delta(1 \times 10^{-6} h^{-1}, 1.5 \times 10^{-6} h^{-1}, 2 \times 10^{-6} h^{-1})$, $\mu_{\lambda_\gamma}(x) = \Delta(1 h^{-1}, 1.5 h^{-1}, 2 h^{-1})$, $\mu_{\lambda_\xi}(x) = \Delta(1 \times 10^{-4} h^{-1}, 1.5 \times 10^{-4} h^{-1}, 2 \times 10^{-4} h^{-1})$, $\mu_{\lambda_\eta}(x) = \Delta(1 h^{-1}, 1.5 h^{-1}, 2 h^{-1})$, $T = 500h$, $\delta = 0.1h$. Here Δ designates a triangular membership function. Then we have

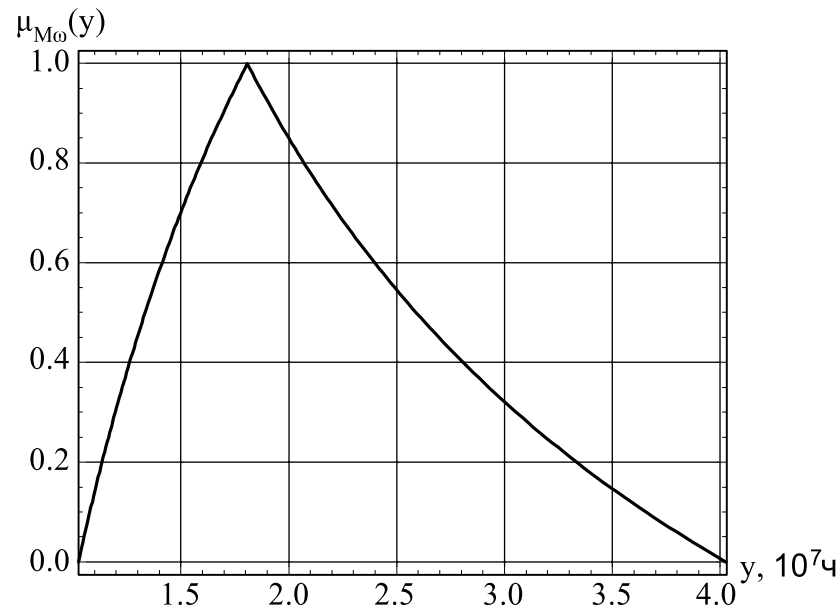


Fig. 1. Membership function of mean operating time to failure of a complex

At the same time, the value $M\omega$ calculated in the classical way makes $1.808 \times 10^7 h$ that coincides with a maximum of membership function, and the value $M[\omega]$ obtained as a result of defuzzification procedure makes $2.029 \times 10^7 h$ that reflects asymmetric property of obtained membership function. We also have estimated the contribution of each of fuzzy parameters to uncertainty of a result according to [8]. So, for the parameter λ_x , we have obtained 0.506858, for $\lambda_\gamma - 0.4 \times 10^{-7}$, for $\lambda_\xi - 0.491839$, and for $\lambda_\eta - 0.00130296$.

Conclusion

Thus, the given study has presented an approach to the estimation of mean operating time to failure of a complex "facility of protection – safety system" in view of uncertainty of initial data in the task. Considering the process of a complex's operation as a random fuzzy process of recovery, the ratios have been obtained that allow us to write down a membership function for mean operating time to failure of a complex. Knowing the membership function of a complex's parameters, mean operating time to failure of a complex has been estimated by applying defuzzification procedure.

References

1. Malashinin I.I., Pereguda A.I. Calculation and optimization of systems dependability of emergency protection of nuclear reactors. – M.: Energoatomizdat, 1985 – p. 112.

2. **Pereguda A.I., Timashov D.A.** Mathematical model of operation process of the automated technological complex “facility of protection – safety system” with recoverable components and the periodic control of a safety system // News of high schools. Nuclear power engineering. – 2007. – #3, edition 2. – pp. 101-109.
3. **Pitiev Yu., I.** Opportunity as an alternative of probability. Mathematical and empirical fundamentals, application. – M.: Fizmatgiz, 2007 – p. 464.
4. **Liu B.** Uncertainty Theory. – 2nd edition. – Berlin: Springer-Verlag, 2007. – 255 pp.
5. **Liu B.** Uncertainty Theory: An Introduction to Its Axiomatic Foundations. – Berlin: Springer-Verlag, 2004. – 411 pp.
6. **Kwakernaak H.** Fuzzy random variables – I. Definitions and theorems // Information Sciences. – 1978. – Vol. 15 – Pp. 1-29.
7. **Hanss M.** Applied Fuzzy Arithmetic: An Introduction with Engineering Applications. – Springer-Verlag, 2005. – 256 pp.
8. **Buckley J. J.** Fuzzy Probability and Statistics. – Springer-Verlag, 2006. – 270 p.
9. **Zhao R., Tang W., Yun H.** Random fuzzy renewal process // European Journal of Operational Research. – 2006. – Vol. 169. – Pp. 189-201.
10. **Shen Q., Zhao R., Tang W.** Random fuzzy alternating renewal processes // Soft Computing. – 2008. – Vol. 13, no. 2. – Pp. 139-147.
11. **Leonenko A.V.** Fuzzy modeling in Matlab and fuzzyTECH. – St. Petersburg: BHV – Petersburg, 2005, p. 736.
12. **Baihelt F., Franken P.** Dependability and maintenance service. The mathematical approach: Tr. from German – M.: Radio and communication, 1988. – p. 392.

Ермаков А.О., Новожилов Е.О.

ОЦЕНКА РИСКОВ, СВЯЗАННЫХ С ИЗЛОМАМИ И ДЕФЕКТАМИ БОКОВЫХ РАМ ТЕЛЕЖЕК ГРУЗОВЫХ ВАГОНОВ

В статье представлен метод оценки рисков, связанных с изломами и дефектами боковых рам тележек грузовых вагонов. Рассматривается построение матриц рисков по изготовителям боковых рам, включая оценку последствий и частот событий, связанных с изломами и выявленными дефектами боковых рам. Предлагаемый метод направлен на обеспечение поддержки принятия управленческих решений по дальнейшей эксплуатации грузовых вагонов на основе риск – менеджмента.

Ключевые слова: рама боковая; вагон грузовой; излом; дефект; риск; оценка риска; матрица рисков.

Введение

В последние годы на сети железных дорог России и других стран СНГ участились случаи излома боковых рам тележек грузовых вагонов. Каждый такой излом сопряжен со сходом одного или нескольких вагонов, локомотива и иногда приводит к тяжелым последствиям, связанным с человеческими жертвами.

Характерной особенностью сложившейся ситуации является то, что изломы боковых рам происходят на сроке эксплуатации от 1 до 4 лет при гарантийном сроке эксплуатации 5 лет, что свидетельствует об их недопустимо низкой надежности.

Следует отметить, что в 2001 году был введен ОСТ 32.183-2001 «Тележки двухосные грузовых вагонов колеи 1520 мм. Детали литые. Рама боковая и балка надрессорная. Технические условия». Его применение заводами-изготовителями началось в 2002 году. С середины 2005 года двухосные тележки грузовых вагонов выпускаются по ГОСТ 9246-2004 «Тележки двухосные грузовых вагонов магистральных железных дорог колеи 1520 мм. Технические условия».

Статистические данные показывают, что значительное увеличение количества изломов боковых рам приходится на период с 2006 г. по настоящее время (рис. 1).

В данных условиях является актуальным использование методов поддержки принятия решений по управлению надежностью и безопасностью функционирования грузовых вагонов на основе инструментов оценки рисков [1, 2]. Представление рисков в форме матриц рисков позволяет проводить оценку рисков и определять соответствующие мероприятия по их снижению, а также оценивать динамику рисков.

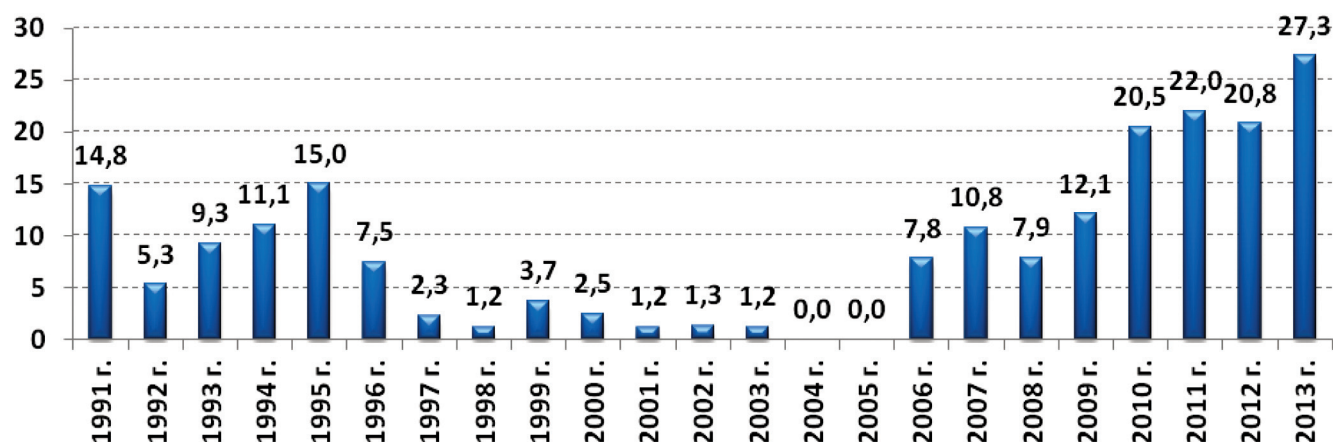


Рис. 1. Количество изломов боковых рам по годам учета на 1 млн вагонов в год

Классификация событий по тяжести последствий

Согласно классификации уровней тяжести последствий по ГОСТ Р 54505-2011 «Безопасность функциональная. Управление рисками на железнодорожном транспорте» и в соответствии с Приказом Минтранса РФ от 25 декабря 2006 г. № 163 «Об утверждении Положения о порядке служебного расследования и учета транспортных происшествий и иных, связанных с нарушением правил безопасности движения и эксплуатации железнодорожного транспорта, событий», транспортным происшествиям и событиям, возникающим по причине излома боковой рамы тележки грузового вагона целесообразно присвоить следующие уровни тяжести последствий:

- крушениям и авариям – «катастрофический»;
- сходам и событиям без схода – «критический».

Эксплуатация грузового вагона с тележками, имеющими дефектные боковые рамы, запрещается. В связи с этим, фактам обнаружения трещин и других литейных дефектов боковых рам при эксплуатации или проведении деповского ремонта присваиваются следующие уровни тяжести последствий:

- дефектам, выявленным в процессе эксплуатации при проведении технического обслуживания вагонов – «несущественный»;
- дефектам, выявленным в процессе проведения деповского ремонта – «незначительный».

Оценка частоты событий

Расчет частоты событий проводится отдельно для событий с различной тяжестью последствий: крушений и аварий; сходов и событий без сходов; выявленных трещин и других дефектов при техническом обслуживании; выявленных трещин и других дефектов при деповском ремонте.

Частота событий вычисляется отдельно для каждой партии рам. Партия рам включает все боковые рамы, выпущенные в определенном календарном году определенным изготовителем.

Частота событий определяется как отношение количества событий данного вида к объему рассматриваемой партии боковых рам, деленное на интервал наблюдения, который принимается равным сроку эксплуатации партии рам, от года ее выпуска до текущего момента:

$$F = \frac{n}{N \cdot T}, \quad (1)$$

где F – частота крушений и аварий (сходов и событий без сходов) вследствие излома рам или частота выявления трещин и других неустраняемых дефектов при техническом обслуживании (деповском ремонте), 1/год;

n – количество изломов боковых рам данной партии, приведших к крушению или аварии (сходу или событию без схода) за период наблюдения или количество трещин и других неустраняемых дефектов, выявленных в данной партии при техническом обслуживании (деповском ремонте) за период наблюдения;

N – объем партии (количество боковых рам в партии);

T – период наблюдения, лет.

Выбор шкалы тяжести последствий

Шкала тяжести последствий для построения матриц рисков, связанных с изломами и дефектами боковых рам, принимается в соответствии с типовой шкалой по ГОСТ Р 54505-2011 «Безопасность функциональная. Управление рисками на железнодорожном транспорте». Она является качественной и использует 4 интервала уровней: катастрофический, критический (для событий изломов рам) и несущественный, незначительный (для событий выявления трещин и других неустраняемых дефектов рам).

Выбор шкалы частот

Шкала частот для построения матриц рисков, связанных с изломами и дефектами боковых рам, принимается аналогичной типовой шкале по ГОСТ Р 54505. Поскольку значения частот для событий в настоящих Методических указаниях выражаются количественно, интервалы уровней представляются диапазонами количественных значений. Шаг шкалы – логарифмический. Количество интервалов в настоящих Методических указаниях принимается равным 7. Если рассчитанные по (1) значения частот событий находятся за пределами шкалы, то меньшие значения заменяются минимальным значением шкалы, а большие – максимальным ее значением.

Коэффициент кратности границ интервалов шкалы частот для оценки рисков, связанных с изломами и дефектами боковых рам, рекомендуется принимать равным 2 или 2,5.

Задание допустимых уровней рисков

Для событий, возникающих в результате изломов (крушения и аварии, сходы и события без сходов) в качестве показателя для установки допустимых уровней рисков устанавливается допустимый уровень по частоте изломов (опасных отказов) боковой рамы $f_{оп} = 1 \times 10^{-6}$ 1/год на 1 млн боковых рам [3]. Такая частота изломов допускается для обеспечения требуемых показателей безопасности движения и при этом не требуется каких-либо корректирующих действий. Таким образом, указанное значение соответствует границе между интервалом уровней риска «не принимаемый в расчет» (зеленая зона), и интервалом уровней риска «допустимый» (желтая зона) для событий с наихудшей (катастрофической) тяжестью последствий – крушения и аварии.

Для событий выявления трещин или других дефектов боковых рам при техническом обслуживании вагона в качестве показателя для установки допустимых уровней рисков устанавливается нормативная доля дефектных изделий в партии $S_n = 2 \times 10^{-4}$ [3]. Указанное значение

соответствует границе между интервалом уровней риска «не принимаемый в расчет» (зеленая зона), и интервалом уровней риска «допустимый» (желтая зона) для событий незначительной тяжести последствий – трещины и другие неустраняемые дефекты, выявляемые при техническом обслуживании.

Сглаживание временного ряда частот

Перед отображением на матрицах уровни частот событий, образующие временной ряд по годам выпуска партий, сглаживаются методом скользящего среднего. Это делается с целью ослабления влияния случайных выбросов на результат оценки рисков (например, один случайный излом в рамках данного года выпуска может привести к недопустимому риску).

Сглаживание реализуется следующим образом. Пусть задана исходная последовательность частот событий (точек временного ряда) $f(1), f(2), \dots, f(K)$. Для данного временного ряда, содержащего K точек, задается ширина W области усреднения – количество точек ряда, участвующих в формировании сглаженного значения рассматриваемой точки. Как правило, область усреднения симметрична относительно рассматриваемой точки и поэтому W – нечетное.

Для любого нечетного значения $W > 1$ можно задать целочисленные симметричные смещения границ области усреднения $i_{\min} = (1 - W)/2$; $i_{\max} = (W - 1)/2$, где центральной точке будет соответствовать $i = 0$. Для каждой i -й точки ($i = i_{\min}, i_{\min} + 1, \dots, -1, 0, 1, \dots, i_{\max} - 1, i_{\max}$) в области усреднения

задается соответствующий весовой коэффициент p_i , причем $\sum_{i=i_{\min}}^{i_{\max}} p_i = 1$.

Формула для вычисления скользящего среднего имеет вид

$$F(k) = \sum_{i=i_{\min}}^{i_{\max}} p_i \cdot f(k+i). \quad (2)$$

Таким образом, после выполнения сглаживания каждая точка $f(k)$ исходного ряда заменяется на усредненную точку $F(k)$, где $k = 1 \dots K$.

Для корректного сглаживания в областях начала и окончания ряда принимаются следующие условия:

- если $(k+i) < 1$, то в выражении (2) принимается $S(k+i) = S(1)$;
- если $(k+i) > K$, то в выражении (2) принимается $S(k+i) = S(K)$.

Для сглаживания однократных случайных выбросов временного ряда без существенного влияния на систематические составляющие рекомендуется использование следующих параметров: $W = 5$; $i_{\min} = -2$; $i_{\max} = 2$; $p_{-2} = 0,027$; $p_{-1} = 0,135$; $p_0 = 0,676$; $p_1 = 0,135$; $p_2 = 0,027$ (для временного ряда 5 и более точек) и $W = 3$; $i_{\min} = -1$; $i_{\max} = 1$; $p_{-1} = 0,15$; $p_0 = 0,7$; $p_1 = 0,15$ (для временного ряда 3 или 4 точки). При меньшем количестве точек в ряду сглаживание не проводится.

Таким образом, временной ряд рассчитанных частот по событиям каждого вида для заданного производителя усредняется с использованием формулы (2) и выбранных параметров усреднения. Затем сглаженные значения частот используются при построении матрицы рисков.

Задание категории рисков

Категории рисков для оценки уровней рисков, связанных с изломами и дефектами боковых рам, принимаются в соответствии с ГОСТ Р 54505. Риск оценивается по 4 интервальным категориям: недопустимый, нежелательный, допустимый и не принимаемый в расчет. Данные категории соответственно отображаются следующими цветами ячеек матрицы рисков: красный, оранжевый, желтый, зеленый.

Построение матриц рисков

С использованием рассмотренных выше данных по частотам и последствиям событий, по каждому изготовителю для всех партий, изготовленных за заданный интервал наблюдения, строятся матрицы рисков, связанных с изломами и дефектами боковых рам. Общий вид такой матрицы показан на рисунке 2.

Уровни частот в комбинации с уровнями тяжести последствий определяют категории рисков, связанных с изломами и с дефектами боковых рам.

Следует отметить, что в данной матрице рисков используются две различные шкалы уровней частот для двух рассматриваемых видов событий – изломов и дефектов боковых рам.

Уровень частоты, 1/год		Трещины и дефекты, выявленные при деповском ремонте	Трещины и дефекты, выявленные при техническом обслуживании	Сходы / случаи без схода	Крушения и аварии	
	5...10 изломов на 100 000 рам в год 2...5 дефектов на 1000 рам в год	$(5...10) \times 10^{-5}$ $(2...5) \times 10^{-3}$	Недопустимый риск	Недопустимый риск	Недопустимый риск	Недопустимый риск
	2...5 изломов на 100 000 рам в год 1...2 дефекта на 1000 рам в год	$(2...5) \times 10^{-5}$ $(1...2) \times 10^{-3}$	Нежелательный риск	Недопустимый риск	Недопустимый риск	Недопустимый риск
	1...2 излома на 100 000 рам в год 5...10 дефектов на 10 000 рам в год	$(1...2) \times 10^{-5}$ $(5...10) \times 10^{-4}$	Допустимый риск	Нежелательный риск	Недопустимый риск	Недопустимый риск
	5...10 изломов на 1 000 000 рам в год 2...5 дефектов на 10 000 рам в год	$(5...10) \times 10^{-6}$ $(2...5) \times 10^{-4}$	Не принимаемый в расчет риск	Допустимый риск	Нежелательный риск	Недопустимый риск
	2...5 изломов на 1 000 000 рам в год 1...2 дефекта на 10 000 рам в год	$(2...5) \times 10^{-6}$ $(1...2) \times 10^{-4}$	Не принимаемый в расчет риск	Не принимаемый в расчет риск	Допустимый риск	Нежелательный риск
	1...2 излома на 1 000 000 рам в год 5...10 дефектов на 100 000 рам в год	$(1...2) \times 10^{-6}$ $(5...10) \times 10^{-5}$	Не принимаемый в расчет риск	Не принимаемый в расчет риск	Не принимаемый в расчет риск	Допустимый риск
	5...10 изломов на 10 000 000 рам в год 2...5 дефектов на 100 000 рам в год	$(5...10) \times 10^{-7}$ $(2...5) \times 10^{-5}$	Не принимаемый в расчет риск	Не принимаемый в расчет риск	Не принимаемый в расчет риск	Не принимаемый в расчет риск
			Незначительный (вагон поврежден незначительно, необ- ходим текущий ремонт)	Несущественный (вагон поврежден, необходим средний или депокский ремонт)	Критический (вагон поврежден, необходим капитальный ремонт)	Катастрофический (вагон поврежден до степени исключения из инвентаря)
			Уровень тяжести последствий			

Рис. 2. Общий вид матрицы рисков, связанных с изломами и дефектами боковых рам заданного изготовителя за интервал наблюдения

В ячейках матрицы размещают точки, соответствующие уровню последствий и уровню частоты для заданного риска, связанного с рамами данного изготовителя по всем партиям, выпущенным за заданный интервал наблюдения.

Пример построения матрицы рисков

Рассмотрим построение матрицы рисков для партий изготовителя «Бежицкий сталелитейный завод», выпущенных за период наблюдения с 2002 по 2013 г. по состоянию на 1 апреля 2013 г.

Исходные данные для матриц рисков, связанных с изломами и дефектами рам Бежицкого сталелитейного завода (БСЗ) за интервал наблюдения с 2002 по 2013 г. представлены в столбцах 1-5 таблицы 1 [4, 5]. Для количества изломов интервал наблюдения равен сроку службы рамы, а для трещин и других неустраняемых дефектов, выявленных при техническом обслуживании вагона – 4,3 года, поскольку данные по дефектам известны только начиная с 2009 г. Данные по количеству трещин и дефектов, выявленных при деповском ремонте, не представлены.

Таблица 1. Данные по количеству изломов и дефектов по партиям Бежицкого сталелитейного завода, изготовленным с 2002 по 2013 г.

Год выпуска партии	Объем партии	Кол-во изломов (крушения и аварии)	Кол-во изломов (сходы и сл. без схода)	Кол-во дефектов	Ч-та изломов (крушения и аварии), 1/год	Ч-та изломов (сходы и сл. без схода), 1/год	Ч-та дефектов, 1/год
2002	23761	0	0	87	0	0	$8,52 \times 10^{-4}$
2003	34353	0	0	249	0	0	$1,69 \times 10^{-3}$
2004	47708	0	0	208	0	0	$1,01 \times 10^{-3}$
2005	36933	0	0	133	0	0	$8,37 \times 10^{-4}$
2006	46419	0	0	120	0	0	$6,01 \times 10^{-4}$
2007	41909	0	0	168	0	0	$9,32 \times 10^{-4}$
2008	38920	0	0	111	0	0	$6,63 \times 10^{-4}$
2009	21374	0	1	67	0	$1,09 \times 10^{-5}$	$7,29 \times 10^{-4}$
2010	40966	0	0	25	0	0	$1,85 \times 10^{-4}$
2011	44390	0	0	10	0	0	$9,79 \times 10^{-4}$
2012	48959	0	0	7	0	0	$1,10 \times 10^{-4}$
2013	13930	0	0	0	0	0	0

Выполним оценку частот событий по выражению (1):

- рассчитаем частоты катастрофических событий для партий 2002-2013 гг. изготовителя БСЗ, используя количество изломов, вызвавших крушения и аварии. Результаты вносим в столбец 6 таблицы 1;
- рассчитаем частоты критических событий для партий 2002-2013 гг. изготовителя БСЗ, используя количество изломов, вызвавших сходы и события без схода. Результаты вносим в столбец 7 таблицы 1.
- рассчитаем частоты незначительных событий для партий 2002-2013 гг. изготовителя БСЗ, используя количество дефектов, выявленных при техническом обслуживании. Результаты вносим в столбец 7 таблицы 1.

По формуле (2) выполним сглаживание временных рядов частот в столбцах 5, 6 и 7 таблицы 1. Результат представлен в таблице 2.

Полученные комбинации тяжести последствий и соответствующих им сглаженных значений частот из таблицы 2 наносим на шаблон матрицы рисков (рис. 2). В результате получаем матрицу рисков, связанных с изломами и дефектами для партий БСЗ 2002-2013 гг. (рис. 3).

Таблица 2. Исходные и усредненные данные частот событий

Год выпуска партии	Ч-та изломов (крушения и аварии), 1/год		Ч-та изломов (сходы и сл. без схода), 1/год		Ч-та дефектов, 1/год	
	(исходн.)	(усредн.)	(исходн.)	(усредн.)	(исходн.)	(усредн.)
2002	0	0	0	0	$8,52 \times 10^{-4}$	$9,68 \times 10^{-4}$
2003	0	0	0	0	$1,69 \times 10^{-3}$	$1,44 \times 10^{-3}$
2004	0	0	0	0	$1,01 \times 10^{-3}$	$1,07 \times 10^{-3}$
2005	0	0	0	0	$8,37 \times 10^{-4}$	$8,55 \times 10^{-4}$
2006	0	0	0	0	$6,01 \times 10^{-4}$	$6,91 \times 10^{-4}$
2007	0	0	0	$2,94 \times 10^{-7}$	$9,32 \times 10^{-4}$	$8,43 \times 10^{-4}$
2008	0	0	0	$1,47 \times 10^{-6}$	$6,63 \times 10^{-4}$	$6,94 \times 10^{-4}$
2009	0	0	$1,09 \times 10^{-5}$	$7,36 \times 10^{-6}$	$7,29 \times 10^{-4}$	$6,35 \times 10^{-4}$
2010	0	0	0	$1,47 \times 10^{-6}$	$1,85 \times 10^{-4}$	$2,58 \times 10^{-4}$
2011	0	0	0	$2,94 \times 10^{-7}$	$9,79 \times 10^{-4}$	$1,26 \times 10^{-4}$
2012	0	0	0	0	$1,10 \times 10^{-4}$	$9,26 \times 10^{-5}$
2013	0	0	0	0	0	$1,75 \times 10^{-5}$

Риски, связанные с **изломами** и **дефектами** рам выпуска Бежицкий сталелитейный завод
 партии с 2002 по 2013 год
 по состоянию на 1 квартал 2013 года

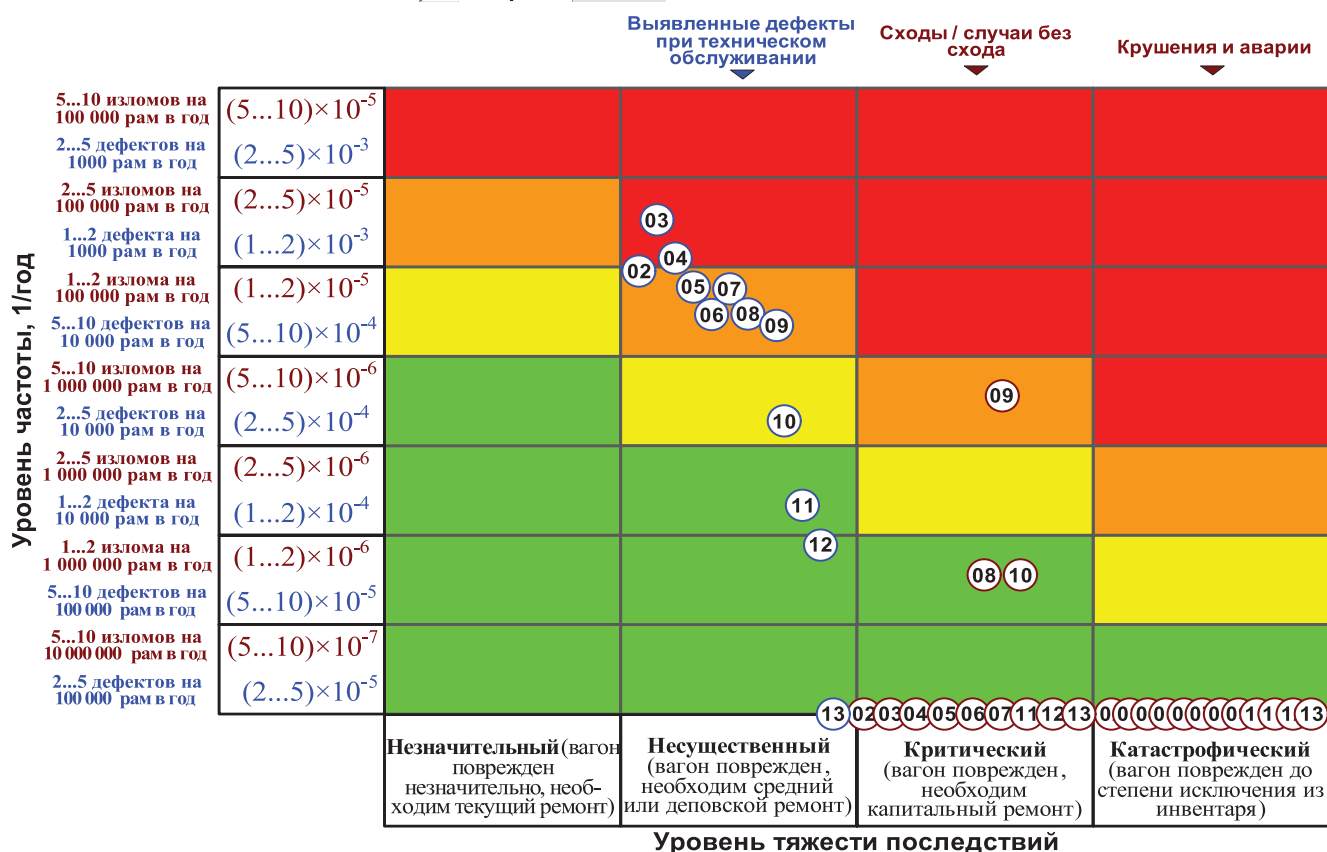


Рис. 3. Матрица рисков, связанных с изломами и дефектами рам выпуска БСЗ за 2002-2013 гг.

Аналогично строятся матрицы рисков для партий других изготовителей.

Мероприятия и принятие решений

Принятие решения о дальнейшей эксплуатации вагонов с партией рам, выпущенных конкретным изготовителем в заданный год, проводится на основе категории риска на матрице рисков.

Следует отметить, что недопустимые риски характеризуют продукцию изготовителя как потенциально опасную, не обеспечивающую безопасность и надежность перевозочного процесса. Такие риски должны исключаться.

При обработке риска необходимо обратить внимание на соблюдение требований на следующих основных этапах жизненного цикла боковой рамы тележки:

- проектирование;
- изготовление;
- ремонт;
- эксплуатация.

На этапе проектирования необходимо проанализировать соблюдение требований:

- к конструкции рамы;
- к конструкции тележки;
- к свойствам материала.

На этапе изготовления необходимо проанализировать соблюдение требований технологии, которая включает:

- структуру технологического процесса изготовления;
- оборудование, применяемое при изготовлении (например, применение ледниковых стержневых систем);
- свойства материала;
- методы выходного неразрушающего контроля.

При проведении ремонта необходимо проанализировать соблюдение требований технологии, которая включает:

- структуру технологического процесса ремонта;
- методы входного неразрушающего контроля;
- методы выходного неразрушающего контроля.

На этапе эксплуатации необходимо проанализировать соблюдение требований:

- контроля при техническом обслуживании тележек;
- соблюдение условий эксплуатации подвижного состава.

Рассмотренный метод оценки рисков, связанных с изломами и дефектами боковых рам тележек грузовых вагонов позволяет осуществить поддержку принятия решений по дальнейшей эксплуатации грузовых вагонов, использующих боковые рамы определенной партии. На основе оценки рисков может быть повышена эффективность рекламационной работы владельца инфраструктуры и собственника вагонов с изготовителями боковых рам.

Авторы выражают признательность д.т.н., профессору Шубинскому И.Б. за помощь, оказанную при подготовке данной статьи.

Список использованных источников

1. Методические рекомендации по практическому применению ГОСТ Р 54505-2011 «Безопасность функциональная. Управление рисками на железнодорожном транспорте». Утверждены ОАО «РЖД» 03.03.2012 г.
2. **Методические рекомендации по оценке рисков на железнодорожной инфраструктуре ОАО «РЖД». Утверждены ОАО «РЖД» 21.11.2011 г.**
3. Проект документа «Методика отнесения грузовых вагонов к категории со сниженным уровнем эксплуатационной безопасности по показателям надежности и функциональной безопасности литых деталей тележек (рам боковых и балок надрессорных). Часть 1. Рамы боковые».
4. Анализ технического состояния несущих литых деталей тележек грузовых вагонов за 2012 год. ПКБ ЦВ, 2013 г., 114 стр.
5. Данные отчетности, сформированные в соответствии с Оперативным приказом ОАО «РЖД» от 29 декабря 2009 г. № ЦВр-179.

Ermakov A.O., Novozhilov E.O.

ASSESSMENT OF RISKS RELATED TO FRACTURES AND DEFECTS OF SIDE FRAMES OF FREIGHT CAR BOGIES

The paper presents a method for assessing risks associated with fractures and defects of side frames of freight car bogies. The construction of a risk matrix as per manufacturers of side frames, including the assessment of the impact and the frequency of events related to the fractures and detected defects of side frames, is considered. The proposed method is aimed at providing support for making management decisions as to further operation of freight cars on the basis of risk management.

Keywords: side frame, freight car, fracture, defect, risk, risk assessment, matrix of risks.

Introduction

In recent years, there have been more cases of fracture of side frames of freight car bogies on the railway network of Russia and other CIS countries. Each of such fractures is associated with derailment of one or more cars, locomotive, and sometimes leads to severe consequences related to fatalities.

A characteristic feature of this situation is that fractures of bogie frames occur at the time of operation from 1 to 4 years with the warranty period of 5 years, which demonstrates their unacceptably low reliability.

It should be noted that in 2001 they introduced OST 32.183-2001 “Two-axle bogies of freight cars for 1520 mm gauge. Molded pieces. Side frame and bolster. Technical specifications.” Manufacturers began to introduce the standard in 2002. Since mid-2005, two-axle bogies of freight cars have been produced according to GOST 9246-2004 “Two-axle bogies of freight cars for mainline railways of 1520 mm gauge. Technical specifications.”

The statistics show that a significant increase in the number of bogie frame fractures falls on the period from 2006 up to the present (Fig. 1).

Under these circumstances, it is vital to use of methods for support of decision-making as to management of reliability and safety of freight cars on the basis of risk assessment tools [1, 2]. Presentation of risks in the form of a risk matrix allows us to assess risks and define appropriate mitigation measures, as well as to assess the dynamics of risks.

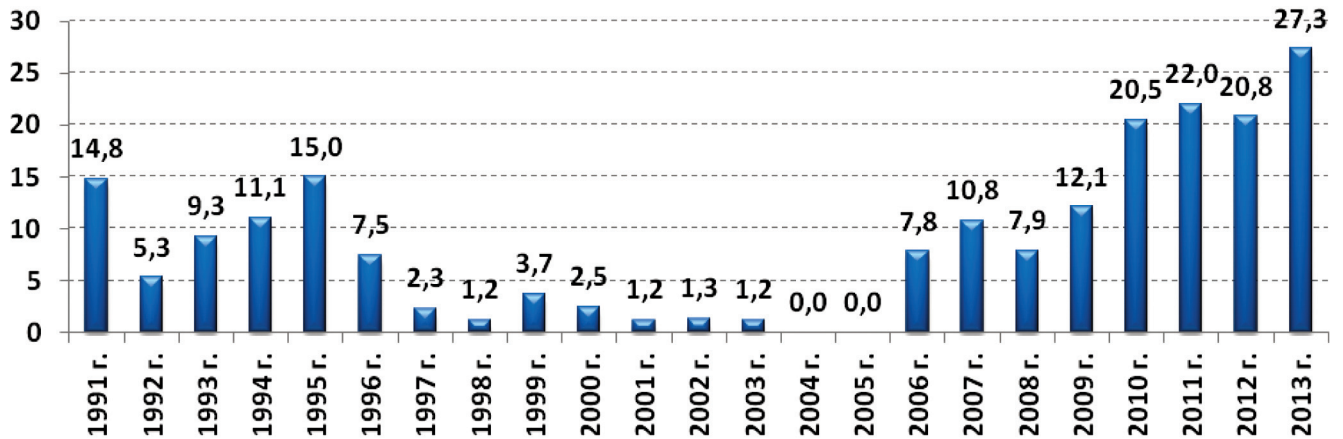


Fig. 1. Number of fractures of bogie frames as per accounted years per 1 mln cars a year

Classification of events as to severity of consequences

According to the classification of levels of consequence severity as to GOST R 54505-2011 “Functional safety. Risk management on railway transport” and in accordance with the Decree of the Ministry of Transport of the Russian Federation of December 25, 2006 #163 “On Approval of the Procedure of official investigation and accounting of transport accidents and other events related to violations of safety rules and operation of railway transport,” traffic accidents and events occurring due to fracture of a side frame of freight car bogie it is advisable to assign the following levels of severity:

- Crashes and accidents – “catastrophic”,
- Derailment and events without derailment – “critical”.

Operation of a freight wagon with bogies having defective side frames is prohibited. In this regard, facts of detecting cracks and other molding defects in side frames during operation or depot repair receive the following levels of consequence severity:

- Defects discovered during operation while maintaining wagons – “insignificant”,
- Defects identified during depot repair – “minor”.

Estimation of events frequency

Frequency of events is calculated separately for events with different severity of consequences: crashes accidents, derailments and events without derailment, cracks and other defects detected during maintenance, cracks and other defects detected during depot repair.

Event rate is calculated separately for each batch of frames. A batch of frames includes all side frames produced in a particular calendar year specified by the manufacturer.

Event rate is defined as the ratio of the number of events of this type to the volume of the considered batch of side frames divided by the interval of observation, which is taken equal to the operation period of the frames batch, from the year of its release up to the current moment:

$$F = \frac{n}{N \cdot T}, \quad (1)$$

where F is the frequency of crashes and accidents (derailments and events without derailment) caused by fractures of frames, or the frequency of cracks and other nonremovable defect detected during maintenance (depot repair), 1/year,

n is the number of fractures of side frames of the batch caused crashes or accidents (derailments and events without derailment) for the period of observation, or the number of 3a of cracks and other nonremovable defect detected during maintenance (depot repair) for the period of observation,

N is the volume of a batch (number of side frames in a batch),

T is the period of observation, years.

Selection of a consequence severity scale

To construct matrices of risks associated with fractures and defects of side frames, a consequence severity scale is adopted in accordance with the standard scale as to GOST R 54505-2011 “Functional safety. Risk management on railway transport.” It is a qualitative scale and uses 4 intervals of levels: catastrophic, critical (for events of frame fractures) and insignificant, minor (for events of detecting cracks and other nonremovable defects of frames).

Selection a frequency scale

To construct matrices of risks associated with fractures and defects of side frames, a frequency scale is adopted as similar to the standard scale according to GOST R 54505. Since the values of frequencies for events in these Guidelines are expressed quantitatively, intervals of levels are represented by ranges of quantitative values. A scale step is logarithmic. The number of intervals in these Guidelines is taken equal to 7. If the values of frequencies of events calculated according to (1) are outside the scale, the smaller values are replaced by the minimum value of the scale, and the larger ones by its maximum value.

To assess risks associated with fractures and defects of side frames, it is recommended to take a multiplicity factor of interval limits of the frequency scale as equal to 2 or 2.5.

Assignment of acceptable risk levels

For events that occur as a result of fractures (crashes and accidents, derailments and events without derailment), an acceptable level as to frequency of fractures (dangerous failure) of a side frame $f_{DF} = 1 \times 10^{-6}$ 1/year per 1 mln of side frames [3] is assigned as an indicator for setting acceptable levels of risks. Such frequency of fractures is accepted to provide the required safety performance of traffic, and in this case there is no need for any corrective activities. Thus, this value corresponds to the boundary between the interval of risk levels “negligible” (green zone), and the interval of risk levels of “acceptable” (yellow area) for events with the worst (catastrophic) consequence severity, i.e. crashes and accidents.

For events of detecting cracks or other defects of side frames during maintenance of a car, a standard share of defective items in the batch $S_g = 2 \times 10^{-4}$ [3] is assigned as an indicator for setting acceptable levels of risks. The specified value corresponds to the boundary between the interval of risk levels “negligible” (green zone), and the interval of risk levels “acceptable” (yellow area) for events of insignificant consequence severity, i.e. cracks and other nonremovable defects revealed by maintenance.

Smoothing of frequency time series

Before being displayed on matrices, frequency levels of events forming a time series as to years of release of batches are smoothed using a moving average. This is done to mitigate the impact of accidental overshoots on the result of risk assessment (e.g. one occasional fracture within a given year of release may lead to an unacceptable risk).

Smoothing is implemented as follows. Let there be an initial sequence of frequencies of events (time series points) $f(1), f(2), \dots, f(K)$. For the given time series containing K points, we set the width W of the averaging region, i.e. the number of series points involved in the formation of the smoothed value of the point under consideration. As a rule, the region of averaging is symmetric in relation to the point under consideration and, therefore, W is odd.

For any odd value of $W > 1$, we can set integer symmetrical shifts of the boundaries of an averaging region $i_{\min} = (1 - W)/2$; $i_{\max} = (W - 1)/2$, where a central point will be corresponded to by $i = 0$. For each the i -th point ($i = i_{\min}, i_{\min} + 1, \dots, -1, 0, 1, \dots, i_{\max} - 1, i_{\max}$), in the averaging region we set a corresponding weight coefficient p_i , and $\sum_{i=i_{\min}}^{i_{\max}} p_i = 1$.

The formula for calculation a moving average looks like

$$F(k) = \sum_{i=i_{\min}}^{i_{\max}} p_i \cdot f(k+i). \quad (2)$$

Therefore, after smoothing each point $f(k)$ of the initial series is replaced by an averaged point $F(k)$, where $k = 1 \dots K$.

For correct smoothing in the regions of series beginning and end, we assume that:

- if $(k+i) < 1$, then in expression (2) we accept $S(k+i) = S(1)$;
- if $(k+i) > K$, then in expression (2) we accept $S(k+i) = S(K)$.

To smooth single accidental overshoots of a time series without a significant impact on systematic constituents, it is recommended to use the following parameters: $W = 5$; $i_{\min} = -2$; $i_{\max} = 2$, $p_{-2} = 0,027$; $p_{-1} = 0,135$; $p_0 = 0,676$; $p_1 = 0,135$; $p_2 = 0,027$ (for the time series of 5 and more points) and $W = 3$; $i_{\min} = -1$; $i_{\max} = 1$; $p_{-1} = 0,15$; $p_0 = 0,7$; $p_1 = 0,15$ (for the time series of 3 or 4 points). In case of a smaller number of points in the series, smoothing is not done.

Therefore, the time series of calculated frequencies for each type of events for a given manufacturer is averaged using formula (2) and the selected parameters of averaging. Then smoothed values of frequencies are used in the construction of a risk matrix.

Assignment of a risk category

Risk categories to assess the levels of risks associated with fractures and defects of side frames are accepted in accordance with GOST R 54505. A risk is assessed by 4 interval categories: unacceptable, undesirable, acceptable, negligible. These categories are represented by the following colors of risk matrix cells: red, orange, yellow, green.

Construction of risk matrices

Using the above data on the frequencies and consequences of events for each manufacturer for all batches manufactured during the specified interval of observation, we construct matrices of risks associated with fractures and defects of side frames. The general view of such matrix is shown in Fig.2.

Frequency levels in combination with levels of consequence severity define categories of risks associated with fractures and defects of side frames.

It should be noted that this risk matrix uses two different frequency scales of frequency levels for two types of events under consideration, fracture and defects of side frames.

		Fractures and defects detected during depot repair	Fractures and defects detected during maintenance	Derailments/events without derailment	Crashes and accidents
		Unacceptable	Unacceptable	Unacceptable	Unacceptable
Level of frequency, 1/year	5...10 fractures per 100 000 frames a year 2...5 defects per 1000 frames a year	(5...10)×10 ⁻⁵ (2...5)×10 ⁻³	Unacceptable	Unacceptable	Unacceptable
	2...5 fractures per 100 000 frames a year 1...2 defects per 1000 frames a year	(2...5)×10 ⁻⁵ (1...2)×10 ⁻³	Unacceptable	Unacceptable	Unacceptable
	1...2 fractures per 100 000 frames a year 5...10 defects per 10 000 frames a year	(1...2)×10 ⁻⁵ (5...10)×10 ⁻⁴	Acceptable	Unacceptable	Unacceptable
	5...10 fractures per 1 000 000 frames a year 2...5 defects per 10 000 frames a year	(5...10)×10 ⁻⁶ (2...5)×10 ⁻⁴	Negligible	Acceptable	Unacceptable
	2...5 fractures per 1 000 000 frames a year 1...2 defects per 10 000 frames a year	(2...5)×10 ⁻⁶ (1...2)×10 ⁻⁴	Negligible	Negligible	Acceptable
	1...2 fractures per 1 000 000 a year 5...10 defects per 100 000 frames a year	(1...2)×10 ⁻⁶ (5...10)×10 ⁻⁵	Negligible	Negligible	Negligible
	5...10 fractures per 10 000 000 frames a year 2...5 defects per 100 000 frames a year	(5...10)×10 ⁻⁷ (2...5)×10 ⁻⁵	Negligible	Negligible	Negligible
		Insignificant (car damaged insignificantly, requiring current repair)	Minor (car damaged, requiring depot repair)	Critical (car damaged, requiring overhaul)	Catastrophic (car damaged severely requiring to be excluded from the inventory)
		Level of consequence severity			

Fig. 2. General view of a matrix of risks related to fractures and defects of side frames for a specified manufacturer for the interval of observation

The cells of the matrix contain points corresponding to a level of consequences and a level of frequencies for a specified risk related to frames of a specified manufacturer for all the batches produced for the given period of observation.

Example of construction of risk matrix

Let us consider the construction of a risk matrix for batches of the manufacturer Bezhitsky steelworks produced during the observation period from 2002 to 2013 as of April 1, 2013.

Initial data for matrices of risks associated with fractures and defects of frames by Bezhitsky steelworks (BSZ) for the observation interval from 2002 to 2013 are presented in columns 1-5 of Table 1 [4,5]. For the number of fractures the observation interval is equal to a frame lifetime, and for that of cracks and other nonremovable defects detected during maintenance of a wagon is equal to 4.3 years, since data on defects is known only since 2009. Data on the number of cracks and defects identified during depot repairs are not presented.

Let us assess frequencies of events using expression (1):

- Calculate frequencies of catastrophic events for the batches produced by BSZ in 2002-2013 using the number of fractures caused crashes and accidents. The results are put into column 6 of Table 1.

Table 1. Data on the number of fractures and defects for batches of Bezhitsky steelworks produced from 2002 to 2013

Year of batch release	Batch volume	Number of fractures (crashes and accidents)	Number of fractures (derailments and events without derailment)	Number of defects	Frequency of fractures (crashes and accidents), 1/year	Frequency of fractures (derailments and events without derailment), 1/year	Frequency of defects, 1/year
2002	23761	0	0	87	0	0	$8,52 \times 10^{-4}$
2003	34353	0	0	249	0	0	$1,69 \times 10^{-3}$
2004	47708	0	0	208	0	0	$1,01 \times 10^{-3}$
2005	36933	0	0	133	0	0	$8,37 \times 10^{-4}$
2006	46419	0	0	120	0	0	$6,01 \times 10^{-4}$
2007	41909	0	0	168	0	0	$9,32 \times 10^{-4}$
2008	38920	0	0	111	0	0	$6,63 \times 10^{-4}$
2009	21374	0	1	67	0	$1,09 \times 10^{-5}$	$7,29 \times 10^{-4}$
2010	40966	0	0	25	0	0	$1,85 \times 10^{-4}$
2011	44390	0	0	10	0	0	$9,79 \times 10^{-4}$
2012	48959	0	0	7	0	0	$1,10 \times 10^{-4}$
2013	13930	0	0	0	0	0	0

Table 2. Basic and averaged data about frequencies of events

Year of batch production	Frequency of fractures (crashes and accidents), 1/year		Frequency of fractures (derailments and events without derailment), 1/year		Frequency of defects, 1/year	
	(basic)	(averaged)	(basic)	(averaged)	(basic)	(averaged)
2002	0	0	0	0	$8,52 \times 10^{-4}$	$9,68 \times 10^{-4}$
2003	0	0	0	0	$1,69 \times 10^{-3}$	$1,44 \times 10^{-3}$
2004	0	0	0	0	$1,01 \times 10^{-3}$	$1,07 \times 10^{-3}$
2005	0	0	0	0	$8,37 \times 10^{-4}$	$8,55 \times 10^{-4}$
2006	0	0	0	0	$6,01 \times 10^{-4}$	$6,91 \times 10^{-4}$
2007	0	0	0	$2,94 \times 10^{-7}$	$9,32 \times 10^{-4}$	$8,43 \times 10^{-4}$
2008	0	0	0	$1,47 \times 10^{-6}$	$6,63 \times 10^{-4}$	$6,94 \times 10^{-4}$
2009	0	0	$1,09 \times 10^{-5}$	$7,36 \times 10^{-6}$	$7,29 \times 10^{-4}$	$6,35 \times 10^{-4}$
2010	0	0	0	$1,47 \times 10^{-6}$	$1,85 \times 10^{-4}$	$2,58 \times 10^{-4}$
2011	0	0	0	$2,94 \times 10^{-7}$	$9,79 \times 10^{-4}$	$1,26 \times 10^{-4}$
2012	0	0	0	0	$1,10 \times 10^{-4}$	$9,26 \times 10^{-5}$
2013	0	0	0	0	0	$1,75 \times 10^{-5}$

- Calculate frequencies of critical events for the batches produced by BSZ in 2002-2013 using the number of fractures caused derailments and events without derailment. The results are put into column 7 of Table 1.

- Calculate frequencies of insignificant events for the batches produced by BSZ in 2002-2013 using the number of fractures identified during maintenance. The results are put into column 7 of Table 1.

Using formula (2), let us smooth time series of frequencies in columns 5, 6 and 7 of Table 1. The result is presented in Table 2.

5) The obtained combinations of consequence severity and corresponding smoothed values of frequencies from Table 2 are put on the pattern of a risk matrix (Fig. 2). As a result, we get a matrix of risks associated with fractures and defects for the batches produced by BSZ in 2002-2013 (Fig. 3).

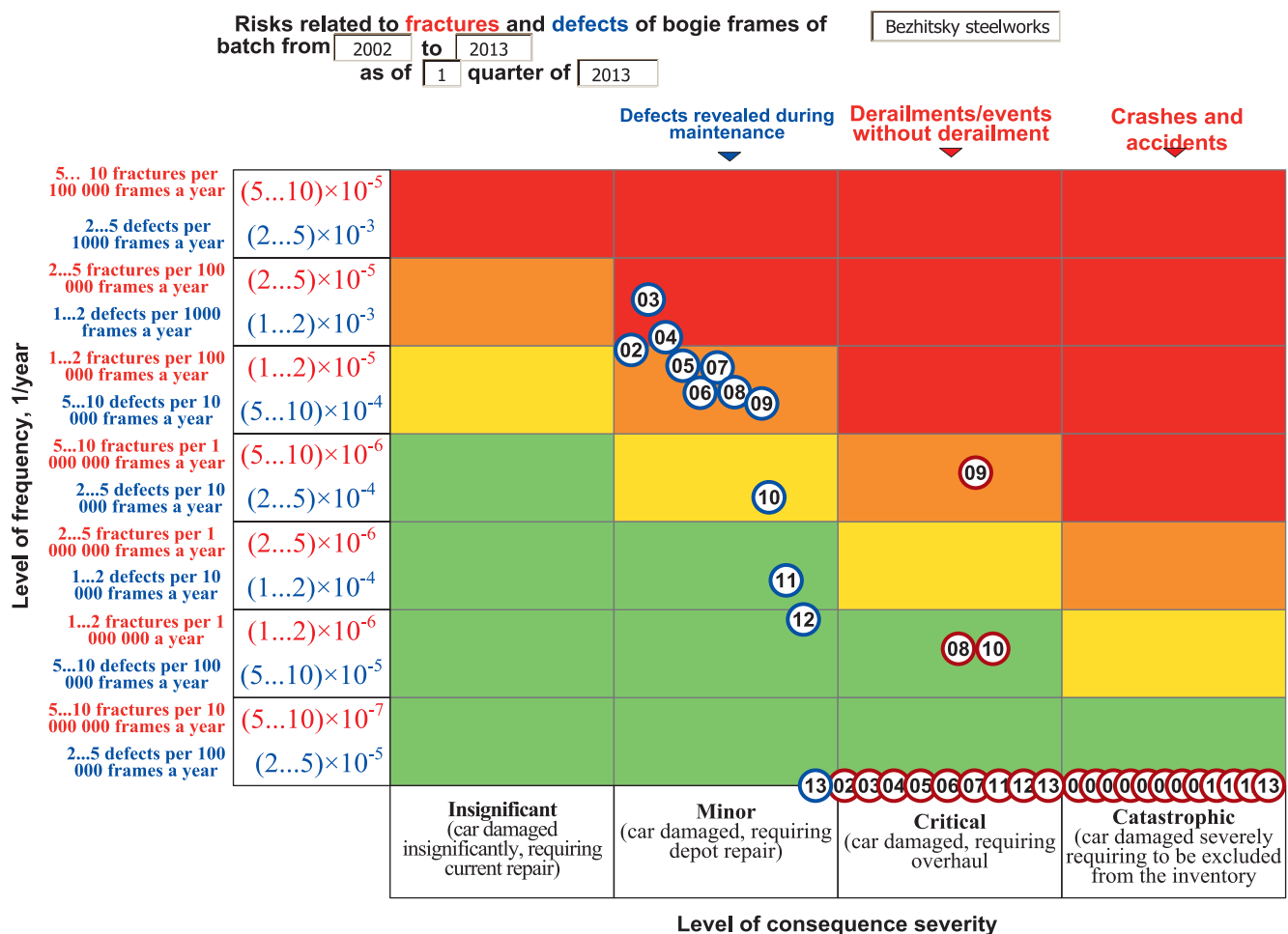


Fig. 3. Matrix of risks related to fractures and defects of frames produced by Bezhitsky steelworks in the period of 2002-2013

Matrices of risks for batches of other manufacturers are constructed in a similar way.

Activities and decision making

Deciding on further use of wagons with the batch of frames produced by a particular manufacturer in a given year is based on the risk category using a risk matrix.

It should be noted that unacceptable risks characterize products of a manufacturer as potentially dangerous, not ensuring the safety and reliability of transportation process. Such risks should be excluded.

When dealing with the risk, we should pay attention to compliance with requirements at the following key stages in the life cycle of a bogie frame:

- Designing,
- Production,
- Repair,
- Operation.

At the designing stage it is necessary to analyze compliance with requirements for:

- A frame design,
- A bogie design,
- Properties of the material.

At the production stage we should analyze compliance with requirements for technology, which comprises:

- Structure of the process of manufacture,
- The equipment used in manufacturing (e.g. the use of ice frameworks),
- Material properties,
- Methods of output nondestructive testing.

During repair, it is necessary to analyze compliance with requirements for technology, which includes:

- Structure of the technological process of repair,
- Methods of input nondestructive testing,
- Methods of output nondestructive testing.

During the operation stage, it is necessary to analyze compliance with requirements for:

- Control for maintenance of bogies,
- Compliance with conditions of rolling stock operation.

The considered method for assessing risks associated with fractures and defects of side frames of freight car bogies allows us to provide support for decision making as to further operation of freight cars that use side frames of a certain batch. On the basis of risk assessment, one can increase the efficiency of reclamation work of an infrastructure operator and car owner with manufacturers of side frames.

The authors express their gratitude to professor I.B. Shubinsky, PhD, for his assistance in preparing this paper.

References

1. Guidelines for application of GOST R 54505-2011 "Functional safety. Risk management on railway transport." Approved by JSC RZD as of 03.03.2012.
2. Guidelines for assessing risks on railway infrastructure of JSC RZD. Approved by JSC RZD as of 21.11.2011.
3. Draft "Guidelines for labeling freight cars as cars with a decreased level of operational safety as to reliability and functional safety parameters of molded pieces of bogies (side frames and bolsters). Part 1. Side frames».
4. Analysis of technical state of carrying molded pieces of freight car bogies for 2012. Design Bureau of Wagon Fleet (TSV), 2013, pp.114.
5. Statistics made in accordance with the Decree of JSC RZD dated December 29, 2009. #TSVr-179.

Абрамова Н.А., Макаренко Д.И., Телицына Т.А.

МОДЕЛЬ И МЕТОД ДЛЯ ОПРЕДЕЛЕНИЯ ПОДСИСТЕМ, НАИБОЛЕЕ ПОДВЕРЖЕННЫХ ДЕСТАБИЛИЗИРУЮЩИМ ВОЗДЕЙСТВИЯМ, В ИЕРАРХИИ СОСТАВНОГО ОБЪЕКТА ЗАЩИТЫ

Разработаны формальная модель и экспертно-формальный метод для определения зоны риска: типов объектов, наиболее подверженных влиянию намеренных антропогенных дестабилизирующих воздействий в иерархии составного объекта защиты при заданной стратегии защиты. Объяснительные возможности модели продемонстрированы при анализе стратегий защиты и последствий их несоблюдения на примере угрозы теракта.

Ключевые слова: безопасность, уязвимость, привлекательность, дестабилизирующее воздействие, объект защиты, угроза теракта.

Введение

Сегодня особенно актуальна задача анализа подверженности дестабилизирующим воздействиям (ДВ) для разных видов объектов защиты. Таким объектом может быть определенная территория (регион, страна), мегаполис со всеми своими инфраструктурными объектами или отдельный аэропорт с его подсистемами и т.д.

Однако такая задача является комплексной и сложной. Так, например, создание систем обеспечения комплексной безопасности мегаполисов может быть отнесено к категории сложнейших слабоструктурированных и слабоформализованных крупномасштабных проблем междисциплинарного характера. Сложность, практически по всем известным мерам, связана и с предметной областью – безопасностью жизнедеятельности мегаполисов, и с системами обеспечения безопасности с их многоуровневым характером, когда система включает ряд уровней: от технических средств контроля через распределенную информационную инфраструктуру, системы поддержки принятия решений до организационных систем и нормативно-правовых документов, регулирующих их деятельность и взаимодействие. При этом высокие требования надежности, устойчивости, живучести, безопасности предъявляются как к инфраструктурам мегаполиса, так и к их системам управления.

Целью анализа подверженности ДВ является определение наиболее слабых мест данного объекта (или территории) для проведения оперативных мероприятий в условиях повышенной угрозы

ДВ или уточнения стратегии защиты объектов и выбора приоритетных направлений инвестиций (ряд типовых задач такого рода рассмотрен в [1]).

Авторами разработаны формальная модель и экспертно-формальный метод для определения зоны риска: типов объектов, наиболее подверженных дестабилизирующим воздействиям в составе составного объекта при заданной стратегии защиты. Следует отметить, что в дальнейшем в статье в качестве ДВ рассматривается теракт, однако разработанные теоретические средства применимы и для других ДВ со схожей спецификой (т.е. намеренные антропогенные ДВ).

Разработанные модель и метод основаны на принципах критериального подхода и оптимизации, принятых в теории принятия решений, с их адаптацией к предметной области по составу критериев и к специфике терактов как намеренных антропогенных ДВ [1, 2].

Центральное место в этой адаптации занимает формализация понятия «подверженность объекта терактам» – его представление с использованием укрупненных критериев оценки, предложенных ранее в работе [3], позволяет проводить сравнительную оценку объектов. В разделе 1 приведены: формализация понятия «подверженность объекта терактам», формальная постановка задачи, модель ситуации, к которой относится решаемая задача, и метод решения.

Далее в разделе 2 на примерах показаны объяснительные возможности модели для некоторых практически значимых ситуаций (анализ стратегий защиты и некоторых последствий их несоблюдения, диагностика ошибочного прогнозирования зоны риска).

На основе анализа узких мест модели в разделе 3 определены подходы к ее дальнейшему развитию и постановке новых исследовательских задач.

1. Модель и метод для определения подсистем и узлов составного объекта защиты, наиболее подверженных влиянию терактов

1.1. Формализация понятия «подверженность объекта терактам»

Основная задача выявления подсистем и узлов, наиболее подверженных влиянию ДВ, может рассматриваться с разных точек зрения в зависимости от контекста, в котором предполагается использование результатов ее решения на практике.

В частности, при формализации понятия «подверженность терактам» свойство подверженности объекта терактам TL , как и другие аналогичные свойства, может рассматриваться, как

- собственное **свойство объекта**, $TL(o)$;
- направленное на объект **свойство среды**, из которой исходит более или менее постоянно действующий дестабилизирующий фактор террористической угрозы, возможно сопровождаемый сопутствующими и противодействующими факторами, $TL(E)^1$;
- свойство $TL(o, E)$, учитывающее **обе составляющие**.

В любом случае, даже если для прикладных целей требуется комплексное свойство, представляется целесообразным уметь оценивать его составляющие по отдельности. И это относится как к критериальному подходу, так и к подходу, основанному на рисках.

С формально-логических позиций можно говорить о «предметах», к которым относится исследуемое свойство P .

¹ Это свойство особенно понятно в случае внешнего терроризма и внешних сил, которые влияют на его интенсивность, когда среду естественно понимать как внешнюю среду. Однако и в случае внутреннего или смешанного терроризма целесообразно выделять факторы, относительно неподвластные терроризируемой стороне.

Для примера – в подходе, основанном на уязвимости [4], уязвимость рассматривается как собственное свойство объекта инфраструктуры или территории, $P(o)$. В подходе известной британской аналитической компании Maplecroft [5], анализирующей подверженность стран рискам терактов, рассматривается комплексный индекс, характеризующий свойство среды $P(E)$. Однако Maplecroft также проводит анализы комплексных рисков, учитывающих, помимо внешней угрозы терроризма, например, внутренние риски для бизнеса или прав человека, т.е. анализируется комплексное свойство $P(o, E)$.

В данном разделе предлагается модель понятия TL , в которой подверженность терактам рассматривается как собственное свойство объекта инфраструктуры $TL(o)$, что соответствует условиям относительного постоянства «среды», и, в частности, постоянно действующему дестабилизирующему фактору терроризма. Эта модель ориентирована на решение основной задачи в контексте таких ситуаций, как оценка оперативной обстановки и принятие решений о направлении защитных мер в составном объекте, оценка качества стратегий его защиты и др.

1.2. Критерии подверженности терактам

В качестве общего критерия для оценки объекта o в составе составного объекта принимается критерий $TL(o)$, который с точки зрения интересов служб обеспечения безопасности интерпретируется как **критерий подверженности терактам** объекта o , а с точки зрения интересов террористов – как **критерий относительной привлекательности o для совершения теракта**. Критерий $TL(o)$ представляется как составной критерий, состоящий из пары укрупненных критериев, определенных в работе [3]:

$$TL(o) = (A(o), W(o)),$$

где $A(o)$ – привлекательность o для террористов,

$W(o)$ – уязвимость o .

Уязвимость $W(o)$ рассматривается как свойство, дополнительное к защищенности: уязвимость максимальна при минимальной защищенности и наоборот.

При этом предполагается, что $A(o)$ характеризует привлекательность o вне зависимости от его защищенности (как естественной, так и намеренной), а составной критерий $TL(o)$ рассматривается как **относительная привлекательность**, поскольку он учитывает оба аспекта, значимых для подверженности терактам.

Каждый из составляющих критериев $A(o)$ и $W(o)$, является переменной, которая принимает значения на конечной порядковой шкале.

Обычно для оценок используются грубые шкалы с небольшим числом значений, нередко – вербальных. Например, для оценки уязвимости-защищенности может быть принята четырехзначная шкала со значениями:

«максимальная уязвимость / минимальная защищенность» (уровень защищенности настолько мал, что не снижает привлекательности для террористов),

«уязвимость довольно высокая»,

«уязвимость довольно низкая»,

«минимальная уязвимость / максимальная защищенность» (уровень защищенности настолько велик, что относительная привлекательность для террористов практически отсутствует).

Предполагается, что интуитивные оценки относительной привлекательности для террористов обладают свойствами нестрогой монотонности:

$$A(o_1) > A(o_2) \ \& \ W(o_1) = W(o_2) \Rightarrow \neg (TL(o_1) < TL(o_2))$$

$$W(o_1) > W(o_2) \ \& \ A(o_1) = A(o_2) \Rightarrow \neg (TL(o_1) < T(o_2)).$$

Если в составном объекте защиты имеются объекты, неразличимые по критерию $TL(o)$, уместно говорить об однотипных объектах и о типе объектов. В дальнейшем будем считать, что обозначение o относится к типу объектов.

Связь оценок с состоянием объекта. Оценки объекта защиты по критерию $TL(o)$ характеризуют его текущее состояние. Существенное различие составляющих состоит в том, что свойство уязвимости (или, напротив, защищенности) для служб обеспечения безопасности является управляемым. Кроме того, изменение состояния уязвимости, вообще говоря, может меняться в зависимости от различных факторов, например, от качества оперативной работы служб охраны. Текущая оценка по критерию уязвимости $W(o)$ соответствует стратегии защиты объектов, одинаковой для всех объектов данного типа.

При решении задачи определения наиболее уязвимых типов объектов в данной модели предполагается, что текущее состояние уязвимости соответствует оценкам.

1.3. Структурная модель составного объекта защиты

Составной объект защиты в общем случае рассматривается как иерархия составляющих объектов, включая элементарные, т.е. неделимые при принятом структурировании объекты («узлы») и составные объекты («подсистемы»). В типологии T объектов, составляющих составной объект, к одному типу относятся объекты, не различаемые с точки зрения подверженности терактам.

Например, к одному типу в составе составного объекта защиты **мегаполис** могут относиться все **международные аэропорты** с одинаковой защищенностью / уязвимостью, а составляющими для них могут быть такие объекты, как «зеленая зона», залы прибытия и т.д. (в контексте теракта в Домодедово в 2011г. [6]).

Узел иерархии в типологии объектов T – это некоторый тип составных объектов O , состоящий из множества типов составляющих объектов (элементарных или составных) ближайшего нижнего уровня иерархии.

Узел иерархии сложного инфраструктурного объекта, например, аэропорт, может рассматриваться как самостоятельный объект защиты, если для него разрабатывается своя стратегия защиты.

В качестве простейшей структурной модели составного объекта при решении основной задачи рассматривается модель M_0 , состоящая из одного узла иерархии. Она привлекательна тем, что к этой модели естественным образом применима модель многокритериальной оптимизации – поиск наиболее привлекательных типов объектов в множестве типов объектов, образующем типологию T такого составного объекта O .

Под **стратегией** защиты S составного объекта O будем понимать совокупность более или менее общих эвристических правил, по которым определяется, какие именно типы объектов допустимы (или недопустимы) в типологии $T(O)$ защищаемого объекта O (примеры таких правил будут даны ниже.)

Метод решения основной задачи на сегодня разработан для модели M_0 .

1.4. Формальная постановка задачи

Пусть дан составной объект защиты O с одним уровнем иерархии, $O=\{o\}$, и для него определены:

- шкалы S_1, S_2 для оценки типов объектов в составе O по критериям привлекательности для террористов $A(o)$ и уязвимости $W(o)$ соответственно;
- типология объектов в составе объекта O , $T(O)$ с оценками на заданных шкалах;
- стратегия C защиты объекта O .

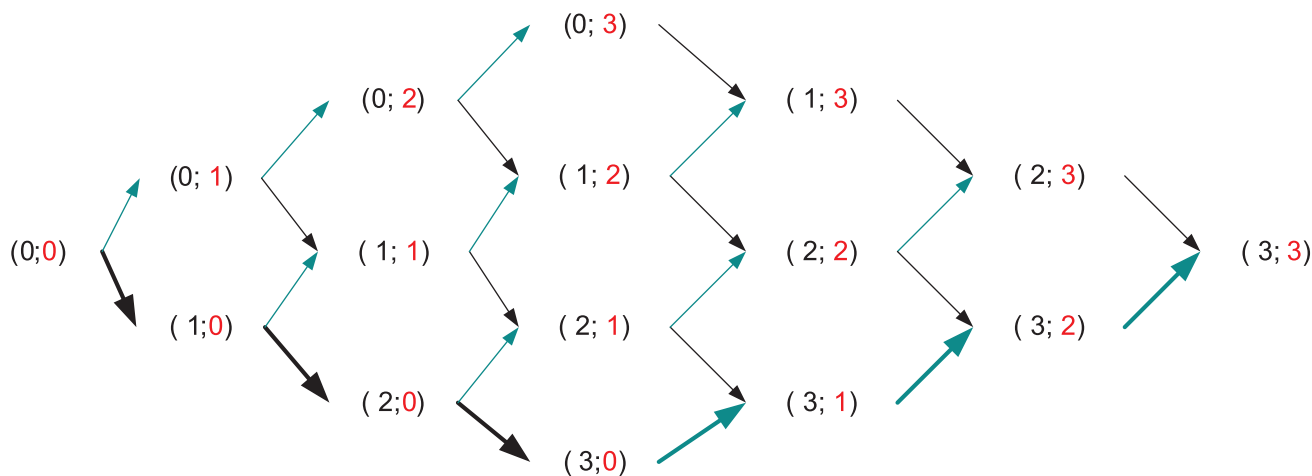
Требуется определить зону риска Z , т.е. тип объектов или, в более общем случае, множество типов объектов, относительно наиболее привлекательных для проведения теракта, иначе говоря, наиболее подверженных риску теракта.

Для простоты принимаем, что все значения на каждой из оценочных шкал S_1, S_2 используются при оценке объектов в структуре O .

1.5. Описание метода решения задачи

Для наглядности метод описывается на примере, в котором для каждого из критериев приняты одинаковые шкалы с балльными оценками (0,1,2,3). На рис. 1 полное множество $\bar{M}$ типов объектов, мыслимое для принятых шкал оценки по составному критерию $TL(o)$, представлено в виде так называемой диаграммы Хассе. Каждый тип объектов представлен парой значений:

Подверженность Терактам $TL(o)=(\text{Привлекательность } A(o), \text{ Уязвимость } W(o))$



Подверженность Терактам $TL(o)=(\text{Привлекательность } A(o), \text{ Уязвимость } W(o))$

Рис. 1. Полное множество типов объектов, мыслимое для принятых шкал оценки по составному критерию

Например, пара (1,3), означает тип объектов с оценками $A(o)=1$, $W(o)=3$. Стрелки показывают на увеличение оценки по одному из критериев при сохранении оценки по другому критерию.

Множество $\bar{M}$ частично упорядочено. Так

- ряд (последовательность) $R1=((3;0), (3;1), (3;2), (3;3))$ представляет все типы объектов, наиболее привлекательных по первому критерию, привлекательности, $A(o)$, которые упорядочены по возрастанию второго критерия, уязвимости, $W(o)$;
- ряд $R2=((0;0), (0;1), (0;2), (0;3))$, напротив, представляет все типы объектов, наименее привлекательных по критерию, $A(o)$, которые также упорядочены по возрастанию критерия, $W(o)$;

- ряд $R3=((0;0), (1;0), (2;0), (3;0))$ – все типы объектов, наименее привлекательных по второму критерию, уязвимости (т.е. оцениваемых как неуязвимые), которые упорядочены по возрастанию первого критерия, $A(o)$.

Этап 1. Определение типологии объектов в структуре составного объекта O в соответствии с принятой стратегией защиты C .

При выборе стратегий защиты обычно опираются на интуитивные эвристические правила здравого смысла, которые считаются рациональными и предполагается наличие (хотя и своей) рациональности у противоборствующей стороны.

С точки зрения выбора стратегий защиты очевидно, что относительно наиболее привлекательным для террористов по составному критерию $TL(o)$ был бы тип объектов с оценкой $(3,3)$, т.е. наиболее привлекательных и наиболее уязвимых, а также объекты, близкие по оценке к $(3,3)$.

Напротив, естественно предположить, что типы объектов ряда $R3$ имели бы нулевую привлекательность по критерию $A(o)$ независимо от их уязвимости.

Рассмотрим примеры эвристических правил, которые могут быть оценены как рациональные.

Общее правило 1, П1 («непривлекательные для террористов не защищаются»). Согласно этому правилу, объекты с оценкой в объекте O , защищаемом по правилу П1, из потенциального ряда типов объектов $R2=((0;\sim))$ где « $\sim$ » – любая уязвимость, в множестве $M_{П1}$ типов объектов, допускаемых этим правилом, могут присутствовать только объекты типа $(0;3)$, т.е. незащищенные. Разумеется, это правило подразумевает, что по умолчанию речь идет только о защите от террористов и естественные свойства защищенности объектов для простоты не учитываются.

В некоторой стратегии C' тип объектов $(1;0)$, интуитивно близкий по привлекательности к $R2$, также мог бы быть исключен дополнительным **частным правилом** П1'.

Общее правило 2, П2 («более привлекательные не могут быть более уязвимыми»). Согласно этому правилу, если хотя бы один тип объектов защищается, это должен быть тип $(3;3)$. Дополнительным частным правилом П2' путем защиты (т.е. снижения уязвимости) могут быть

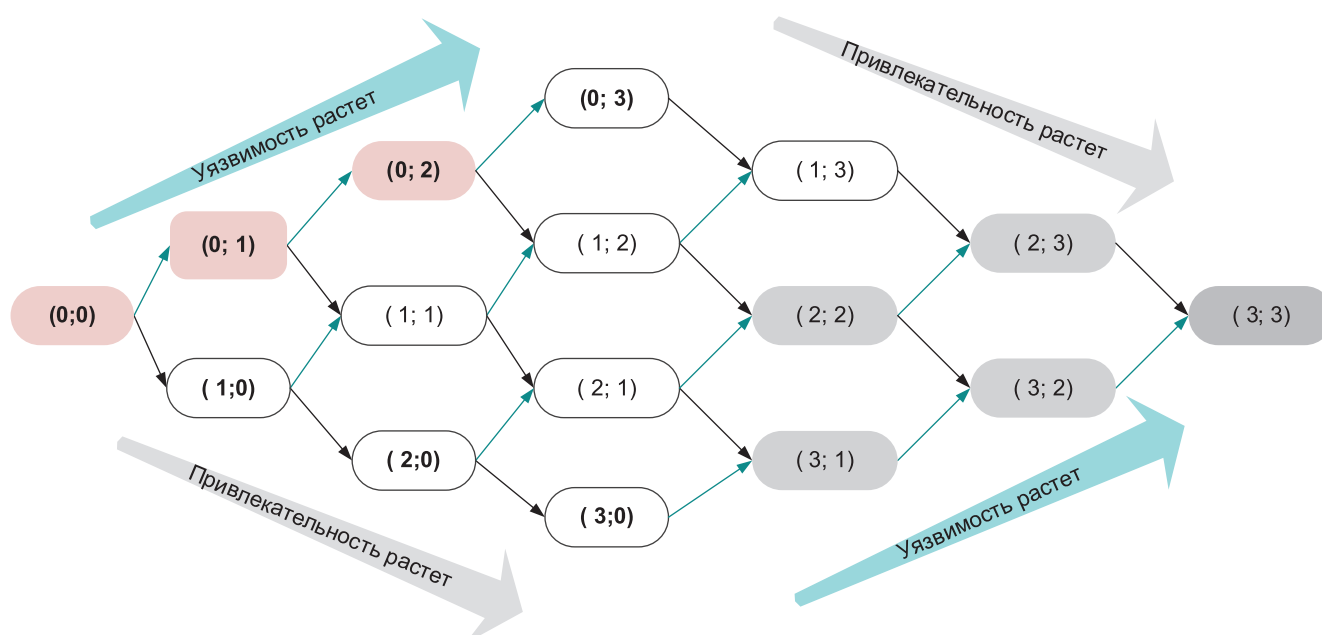


Рис. 2. Множество типов объектов при защите по стратегии C

исключены, например, типы объектов (2;3), (3;2), (2;2), (3;1), более близкие к (3;3) по сравнению с остальными.

На рис. 2 в полном множестве типов объектов затемнены типы объектов, которых не должно быть в составном объекте O при принятой стратегии защиты $C=\{П1, П2, П2'\}$.

В общем случае в соответствии с общими правилами стратегии защиты П1, П2 при построении множества типов объектов M_C , которые оцениваются как более или менее подверженные угрозе, с одной стороны, из полного множества $\bar{M}$ исключается множество $M_{\notin}$ типов объектов, которых вообще не может быть в типологии $O \setminus$ в O по правилу П1 (в примере это множество $M_{\notin} = \{(3;3), (2;3), (3;2), (2;2), (3;1)\}$), а с другой – зона M_H , относительно непривлекательная из-за низкой привлекательности даже при отсутствии защиты (в примере, $M_H = \{(0;0), (0;1), (0;2)\}$). В отличие от объектов из $M_{\notin}$, объекты из M_H могут присутствовать в типологии O , но не рассматриваются как объекты защиты.

Результат применения стратегии защиты получен в виде множества M_C ,

$$M_C = \bar{M} \setminus (M_{\notin} \cup M_H)$$

Этап 2. Определение множества Парето в $\bar{M}$. Грубая оценка наибольшей подверженности терактам.

На рис. 3 показано разбиение множества $\bar{M}$ рассматриваемого примера на 2 класса: множество Парето $M_H = \{(1;3), (2;1), (3;0)\}$ и множество всех остальных типов объектов $M_D = \{(1;0), (2;0), (1;1), (1;2), (0;3)\}$.

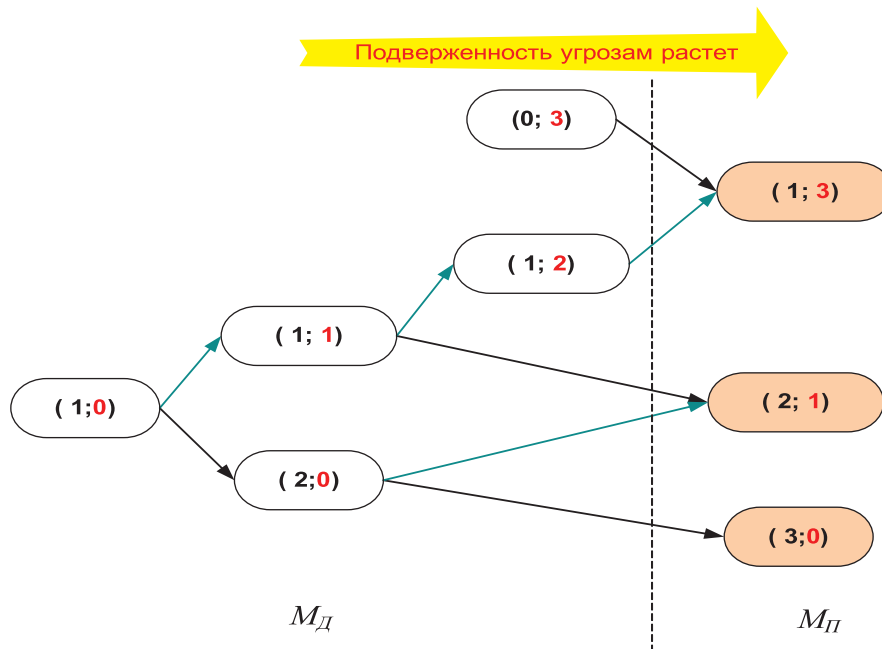


Рис. 3. Типы объектов, наиболее подверженные терактам по Парето

В отличие от типов объектов множества Парето, все объекты множества M_D являются **доминируемыми** в $\bar{M}$. Графически свойство доминирования типа объектов o типом o' выражается в том, что от типа o идет путь к типу o' . Так, для доминируемого типа (1;0) доминирующими по критерию уязвимости являются более уязвимые (1;1), (1;2), (1;3) при их равной привлекательности, причем

$(1;3) \in M_{II}$, т.е. не доминируется никакими другими объектами; объекты типа $(1;0)$ доминируются по критерию привлекательности объектами типа $(2;0)$, $(3;0)$ при равной уязвимости причем $(3;0) \in M_{II}$. Для того же типа $(1;0)$ тип $(2;1)$ является доминирующим как по критерию $Y(o)$, так и по $D(o)$, $(2;1) \in M_{II}$.

Доминируемость некоторого типа o по какому-то или по всем частным критериям означает, что он менее подвержен терактам, чем доминирующие типы (при рациональном выборе на основе частных критериев). Напротив, принадлежность типа объектов o множеству M_{II} означает, что доминирующих типов объектов для него нет, и на основе отдельных критериев в составе $TL(o) = (A(o), W(o))$ такие типы несравнимы, и все они могут рассматриваться как наиболее подверженные терактам по критерию Парето.

Такое решение представляется естественным при стремлении получить по возможности большие значения по каждому из составляющих критериев в составе $TL(o)$.

Обычно говорят, что множество Парето, содержит в себе подмножество всех элементов, каждый из которых «не хуже» всех остальных.

Этап 3. Определение экспертных предпочтений в множестве Парето.

Несмотря на интуитивную естественность определения множества всех типов объектов, наиболее подверженных терактам, как множества Парето (для выбранного множества составных критериев, в данном случае, PT_{II}), нетрудно понять, что при этом, по умолчанию, предполагается равносильность составных критериев и какого-либо агрегирования оценок по этим критериям не происходит.

В связи с этим необходимо дальнейшее уточнение множества зоны риска, Z в пределах множеств Парето

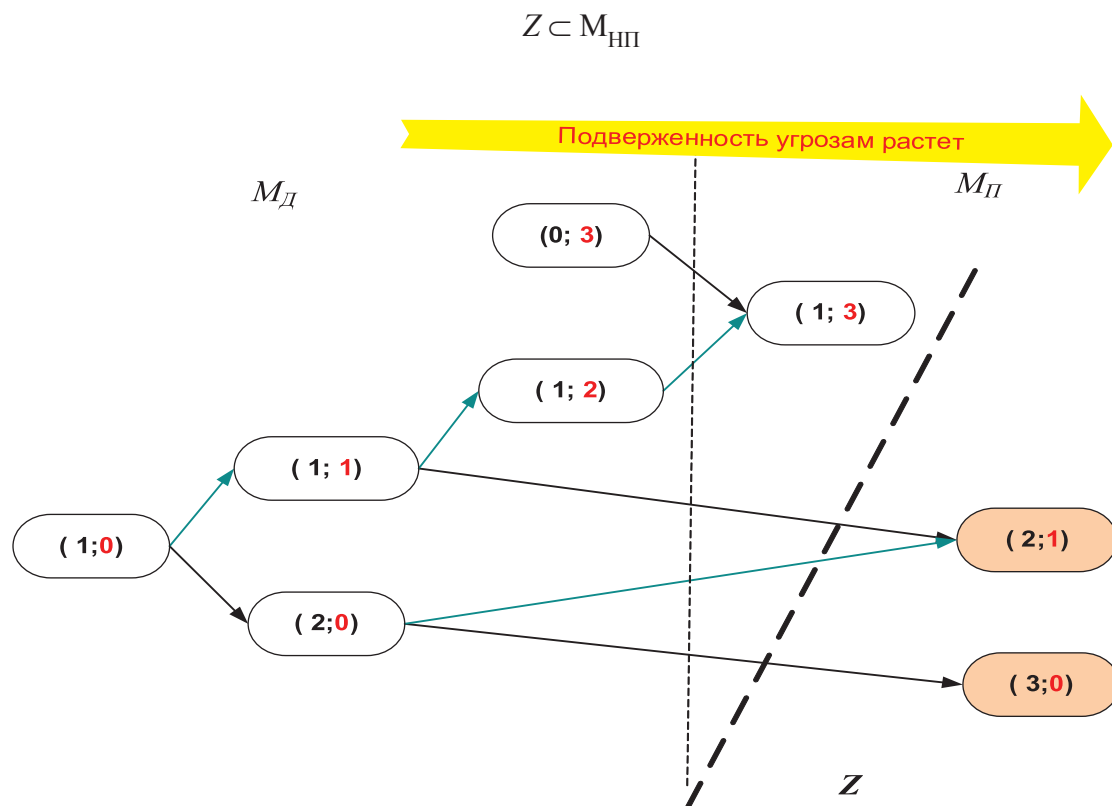


Рис. 4. Предпочтения внутри множества Парето

Окончательный выбор необходимо осуществлять экспертам с учетом не только относительного соотношения значимости (весов) критериев $A(o)$ и $W(o)$ вообще, но прежде всего – исходя из анализа конкретного множества Парето. При этом из множества Парето экспертами выделяется зона риска Z . Пример завершения решения поставленной задачи показан на Рис. 4.

2. Объяснительные возможности модели и метода для практически значимых ситуаций

Объяснительные возможности рассмотренной формализованной модели $M1$ ситуации, в которой определяется зона риска Z в составном объекте O , продемонстрируем на прежнем примере рис. 1 для двух типов практически значимых ситуаций.

Оперативное (в конкретной ситуации) ухудшение защищенности некоторого объекта относительно нормативной защищенности (т.е. повышение уязвимости). На рис. 5 стрелками 1 и 2 показаны два вида ухудшения. Перевод объекта из типа $(1;1)$ в более уязвимый тип $(1;2)$ и даже в $(1;3)$ не опасен, т.к. из-за низкой привлекательности объекта он не может стать объектом теракта (имеется резерв доминирующих объектов, которые не находятся в зоне риска.)

Напротив повышение уязвимости объекта типа $(2;0)$ (переход из типа $(2;0)$ в $(2;1)$) переводит его в зону риска Z .

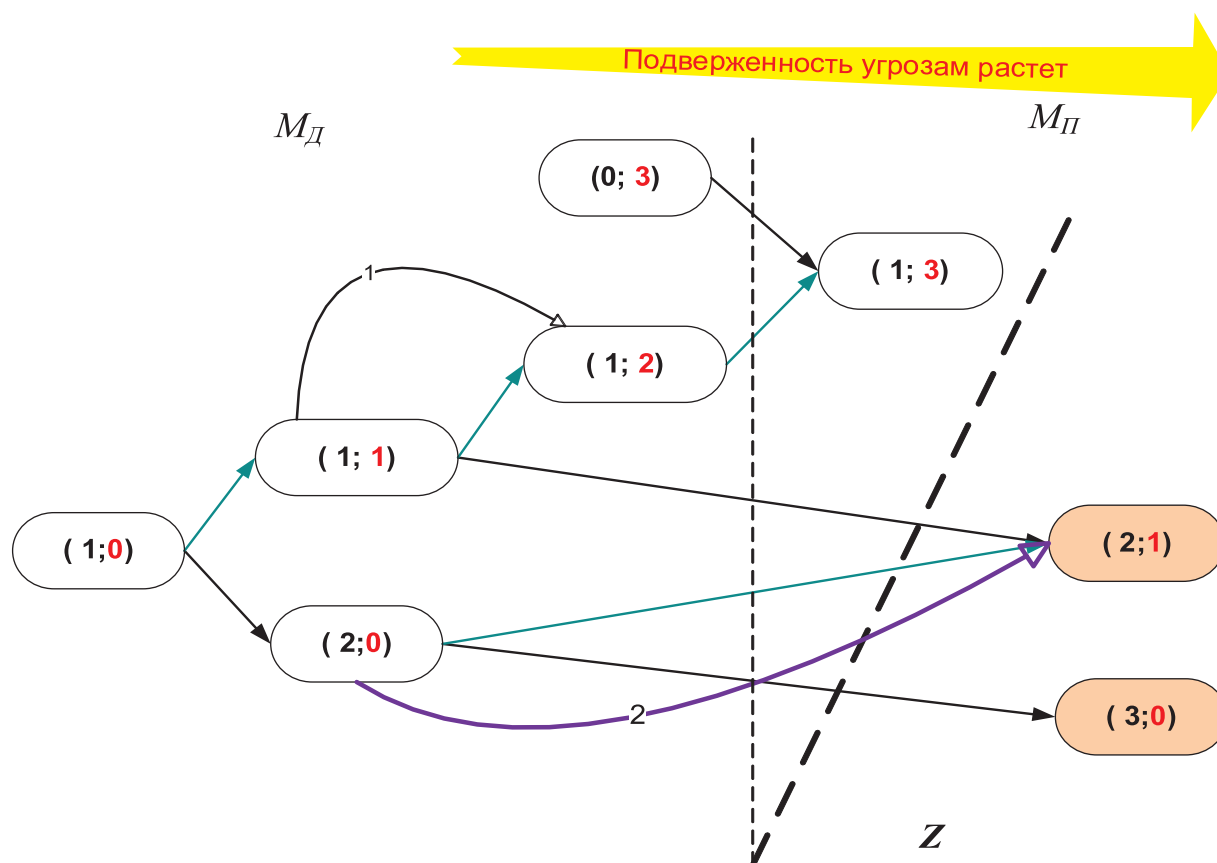


Рис. 5. Оперативные нарушения

Свежий пример ситуации – это повышение уязвимости зала прибытия в Домодедово из-за снижения качества охраны входов в аэропорт транспортной милицией.

Для принятия решений об ответственности за психологически объяснимое снижение качества охраны относительно неважного объекта – входа в аэропорт, существенно учитывать, что понимание структуры защищенности объектов (типа рис. 4), как и связь охраны входа и предпочтительности (относительной привлекательности) зала прибытия в качестве места теракта для террористов не входят в компетенцию милиции.

Меры по обеспечению и контролю над обеспечением требуемого качества реализации стратегии защиты, как и сама стратегия защиты должны лежать на службах обеспечения безопасности составного объекта – аэропорта, по логике управления, в силу их информированности. Не исключено, что на качество охраны могло повлиять простое информирование охраны о том, что меры наказания при охране конкретных узлов определяются в соответствии с (обозначенным) уровнем риска из-за снижения качества охраны.

Оценка эффекта от изменения стратегии защиты. Стратегию «повысить уровень защиты», о необходимости которой в разных странах нередко начинают говорить в ситуациях после терактов, естественно применять, в первую очередь, к зоне риска (или, по крайней мере, к множеству Парето), поскольку в противном случае состав типов объектов, наиболее подверженных угрозам, не изменится.

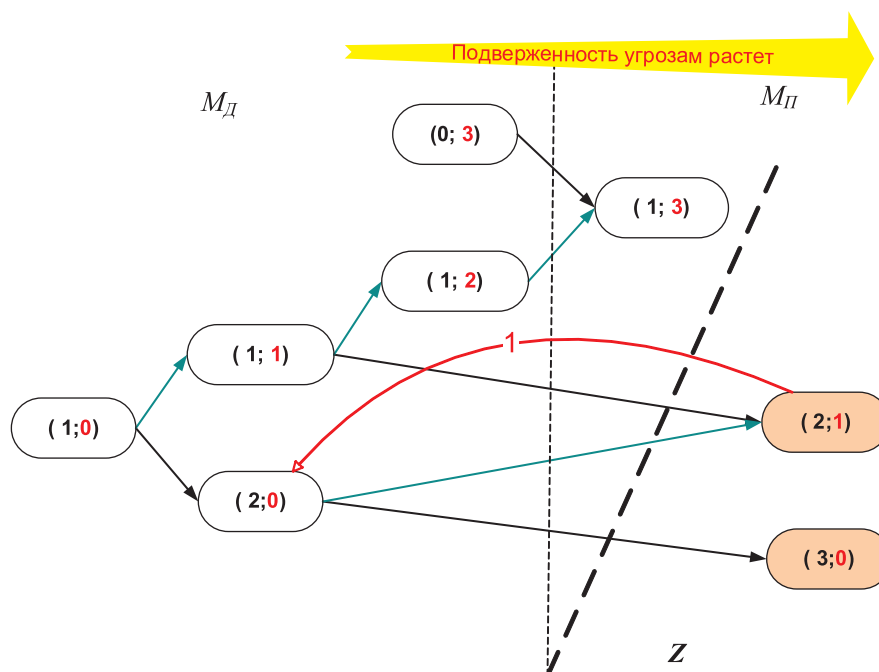


Рис. 6. Улучшение защищенности

На рис. 6 стрелкой 1 показан эффект повышения уровня защиты для объектов типа $(2; 1)$ из зоны риска Z , т.е. их перевод в менее уязвимый тип $(2; 0)$.

В результате число объектов в зоне риска уменьшилось. Однако в условиях, когда в зоне риска остаются только максимально защищенные типы объектов (в данном примере, $(3; 0)$) дальнейшие усилия по повышению защищенности составного объекта O не изменят множества M объектов, наиболее подверженных угрозам.

Диагностика ошибочно спрогнозированной зоны риска. Прогнозирование зоны риска во множестве объектов с разной степенью защищенности и привлекательности представленным методом или каким-то иным основано на целом ряде человеческих допущений. Такие допущения относятся

к числу рисков для достоверности, обусловленных человеческим фактором [7]. Обнаружение ошибочности прогноза, а в нашем случае – факта террористической атаки на объект, не входящий в зону риска, требует последующей диагностики и коррекции модели, принятой для прогноза. Причины ошибочности прогноза могут быть самыми разными, включая и нарушения стратегии защиты. Особую роль среди этих причин составляют ошибки модели привлекательности для террористов, которая закладывается в типологию объектов защиты через оценки типов объектов по критерию $A(o)$ (в теоретических терминах это ошибочность гипотезы общего знания.) По крайней мере, один тип ошибок такого рода состоит в том, что, с точки зрения террориста, объекты фактически относятся не к тому типу привлекательности, как это представляется защищающей стороне.

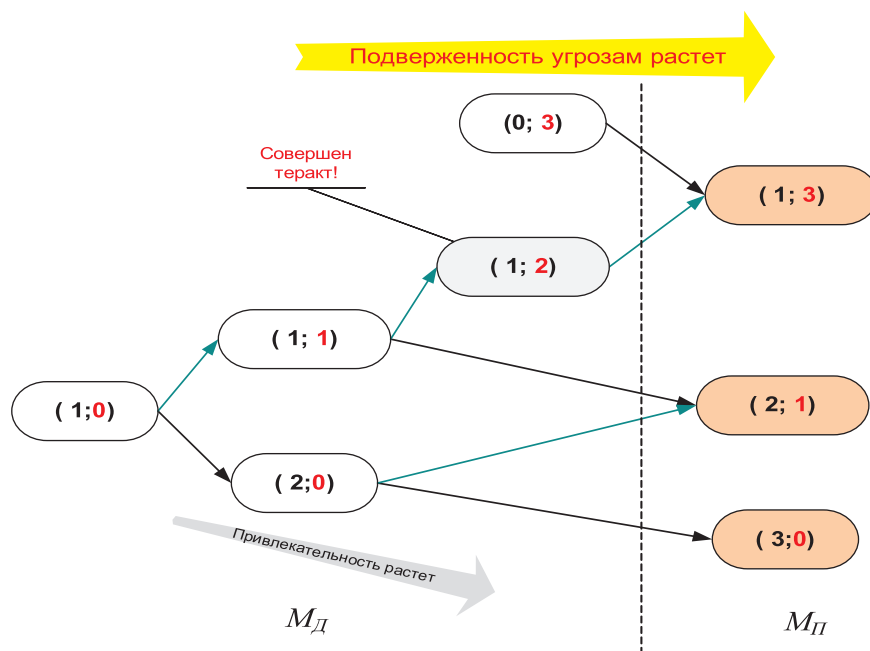


Рис. 7. Ошибка модели привлекательности

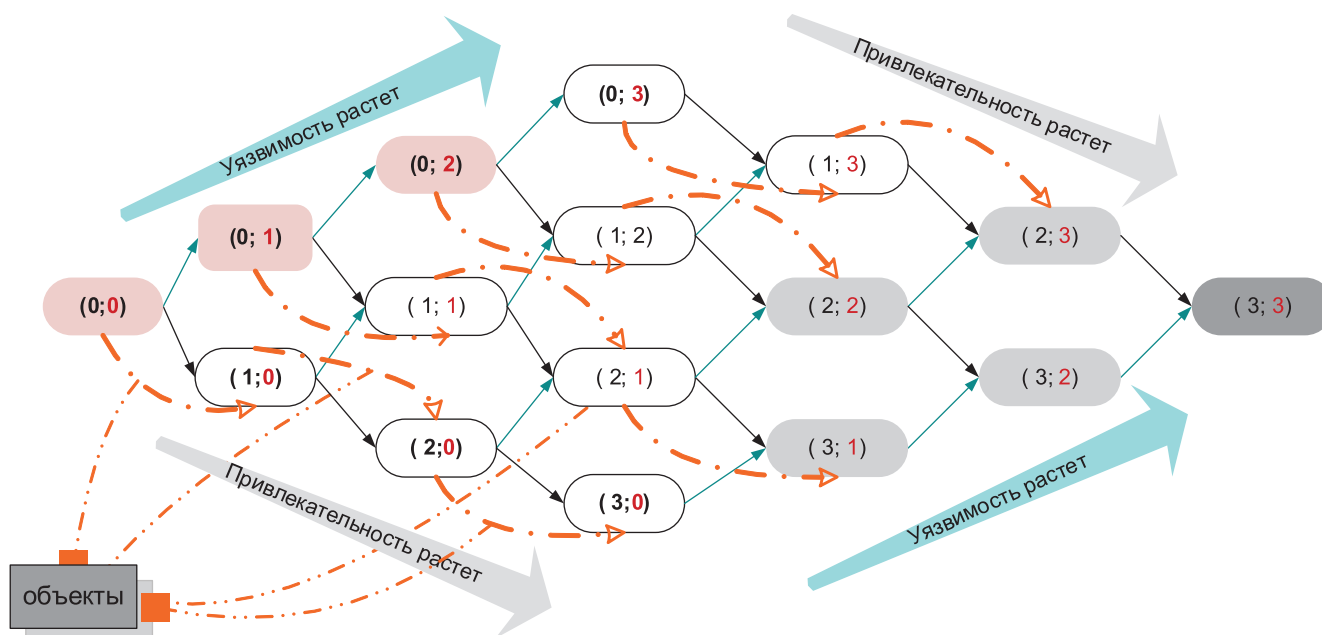


Рис. 8. Сдвиг модели привлекательности

Возможность диагностирования таких ошибок, т.е. формирования гипотез о причинах ошибок, показана для нашего примера на рис. 7 и 8. На рис. 7 выделен тип объектов, (1;2), к которому был отнесен объект теракта; этот объект не входит в зону риска согласно принятой модели привлекательности для террористов. Одной из причин того, что террористы не следовали этой модели, оставаясь в рамках гипотез о рациональности, могло быть то, что защищенность объекта O в целом высока, а давление (интенсивность) дестабилизирующего фактора терроризма также высоко. Результатом может быть сдвиг модели привлекательности, не учтенный при прогнозировании зоны риска (рис. 8).

3. Анализ узких мест и ограничений модели ситуации, лежащей в основе метода. Дальнейшее развитие

В соответствии с принципом развития и сквозного применения методов верификации с целью защиты от рисков для достоверности методов, закладываемых в системы обеспечения безопасности, предложенный метод оценивания объектов, наиболее подверженных терактам, и модель ситуаций оценивания, в которых он может применяться, должны быть подвергнуты анализу. Цель такого анализа – выявление узких мест, ограничений, рисков из-за человеческого фактора.

Для демонстрации содержания и возможностей такого анализа приведем один его фрагмент. В его основе лежит ограничение предложенной модели, состоящее в том, что предлагаемые критерии привлекательности $A(o)$ и уязвимости $W(o)$ для оценки отдельных типов объектов в составе объекта защиты являются очень обобщенными. Для получения оценок по этим критериям нужен переход от оценок по частным критериям к комплексным оценкам по критериям $A(o)$ и $W(o)$, причем эти критерии могут оказаться взаимозависимыми.

Учет зависимости $A(o)$ и $W(o)$ от общих факторов. Далеко неочевидным является вопрос о том, как учитывать разные частные критерии и факторы в составе основных критериев: привлекательности $A(o)$ и уязвимости-защищенности $W(o)$ при оценке объектов по этим двум критериям.

Прежде всего, речь идет о таких показателях, как критичность (важность) объекта, которые могут быть отнесены и к $A(o)$, и к $W(o)$. Ведь более критичный объект, с одной стороны, более привлекателен для террористов, а с другой – обычно он бывает более защищенным в соответствии с типичными стратегиями защиты.

В случае фактора критичности $C(o)$ он, безусловно, является одним из основных при оценке привлекательности $A(o)$. Однако в модели оценка производится для текущего состояния дел при фиксированной стратегии защиты $C(O)$, так что зависимость $C(O)$ от критичности уже учтена в стратегии и ее включение в $W(o)$ больше не требуется.

Если же требуется рассматривать и сопоставлять разные стратегии защиты, оценивать чувствительность к модификациям стратегии (или различным знаниям о ней у противоборствующих сторон) нужно рассматривать разные модели ситуации. Такие действия по модификации стратегии рекомендуется обеспечивать программной поддержкой (мультипликацией в духе рис. 6, 7) для наглядности.

Во всех случаях требуется индивидуальный анализ для каждого критерия или фактора, чтобы исключить дублирование учета одного и того же фактора через $A(o)$ и $W(o)$: в предложенной модели критерии $A(o)$ и $W(o)$ рассматриваются как независимые (для этой цели могут быть полезны когнитивные карты, описывающие взаимодействие различных факторов и их влияние на выбранные обобщенные критерии. Пример такой карты представлен в работе [3].

Дальнейшее развитие по этому направлению состоит в переходе к рефлексивным моделям, учитывающим оценки сторонами чужих знаний. Предполагается, что дальнейшее развитие модели и методов ее анализа должно допускать не только учет разных знаний противоборствующих сторон, но и «рефлексивные игры»: мимикрию в случае терактов, создание ловушек для террористов и т.п.

При анализе влияния внешней угрозы терактов на систему обеспечения безопасности с применением предложенного метода (или, возможно, других методов того же рода) акцент делается на текущее состояние уязвимости / защищенности сложного объекта и его текущую оценку террористами. Однако в действительности для достоверности «коротких» прогнозов важно учитывать и долгосрочную динамику взаимодействия внешнего дестабилизирующего фактора терроризма и сопутствующих ему факторов с внутренними стратегическими решениями по такому взаимодействию.

Заключение

Предложенная модель с методом для определения зоны риска в ситуации, когда подверженность отдельных объектов в составе составного объекта защиты обусловлена двумя критериями: привлекательностью отдельных типов объектов и их уязвимостью при принятой стратегии защиты составного объекта, при всей ее простоте, показала свою работоспособность для разных практических ситуаций.

Вместе с тем, ввиду ограничений, связанных с этой моделью, требуется, с одной стороны дальнейшее развитие модели и метода, а с другой – развитие подхода, направленного на анализ долгосрочной динамики взаимодействия систем обеспечения безопасности с постоянно действующим дестабилизирующим фактором терроризма.

Литература

1. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426). – Hyattsville, MD: U.S. Federal Emergency Management Agency, 2003. – 420 p.
2. Национальная и глобальная безопасность. Терроризм в мегаполисе: оценка угроз и защищенности под общей редакцией / Под ред. В.З. Дворкина. – М.: Издательство «Права человека», 2002. – 113 с.
3. **Макаренко Д.И.** Систематизация критериев и значимых факторов для оценки подверженности сложных систем дестабилизирующим воздействиям / Надежность, 2013, №4 – в печати.
4. **D. Sarewitz, R. Pielke, M. Keykhah** Vulnerability and Risk: Some Thoughts From A Political and Policy Perspective, Risk Analysis, Vol. 23, No. 4. (2003), 805-810.
5. Review of Maplecroft's "Terrorism Risk Index 2011", Режим доступа: <http://foreignpolicyblogs.com/2010/12/04/review-of-maplecrofts-%E2%80%9Cterrorism-risk-index-2011%E2%80%9D/> (дата обращения: 08.08.2013)
6. Террористический акт в аэропорту Домодедово. Википедия. [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/Террористический_акт_в_аэропорту_Домодедово (дата обращения: 01.08.2013)
7. **Абрамова Н.А.** О проблеме рисков из-за человеческого фактора в экспертных методах и информационных технологиях // Проблемы управления – 2007, №2, С.11-17.

Abramova N.A., Makarenko D.I., Telitsyna T.A.

MODEL AND METHOD FOR DEFINITION OF SUBSYSTEMS MOST EXPOSED TO DISTURBANCES AS PART OF A COMPLEX FACILITY OF PROTECTION

A descriptive model and an expert-formal method have been developed for definition of a risk area – types of facilities most exposed to anthropogenic disturbances, as part of a complex object of protection, for the specified strategy of protection. The explanatory capacities of the model have been demonstrated through the analysis of protection strategies and consequences of their violations exemplified by a threat of terrorist attack.

Keywords: security, vulnerability, attractiveness, disturbances, facility of protection, threat of terrorist attack.

Introduction

Nowadays, a vital task is an analysis of susceptibility of various types of protected objects to disturbances (DB). Such an object can be a specific territory (region, country), a big city with all its infrastructure facilities or a separate airport with its subsystems etc.

However, such task is a complex and complicated one. For instance, development of integrated security systems for a big city can be categorized as advanced poorly structured and formalized interdisciplinary problems. The complexity of the task, according to practically all known criteria, is also related to the subject matter, i.e. the safety of normal life of big cities and to security systems with their multilevel nature when a system incorporates a number of levels ranging from technical facilities of control over a distributed information infrastructure, decision-making system to management systems and regulatory documents governing their application and interaction. At the same time, strict requirements of reliability, resilience, durability and safety are made both for infrastructures of big cities and their control and management systems.

The aim of the analysis of DB susceptibility is to define the weakest spots of the facility (or the territory) to do protection activities under the conditions of DB increased threats or to correct the strategy of facilities protection and choose priority directions of investment (a number of typical problems of the kind has been studied in [1]).

The authors of the paper have developed a descriptive model and an expert-formal method to define a risk zone – types of facilities most exposed to anthropogenic disturbances, as part of a complex object of protection, for the specified strategy of protection. It should be noted that further in the paper we con-

sider DB as a terrorist attack, however the theoretical tools developed are also applicable to other DBs of similar types (i.e. intentional anthropogenic DBs).

The model and method developed are based on the principles of a criterion approach and optimization accepted in the theory of decision making but adapted to the subject matter as to the type of criteria and the specifics of terrorist attacks as intentional anthropogenic DBs [1, 2].

The central place in this adaptation is taken by formalization of the term “susceptibility of an object to terrorist attacks” – its presentation using rough criteria of assessment (offered earlier in [3]) allows us to make a comparative evaluation of facilities. In Section 1 you can find the formalization of the term “susceptibility of an object to terrorist attacks”, formalized problem statement, a situation model where the task under consideration belongs to and the method of solution.

Further in Section 2, you can find the exemplified explanatory capabilities of the model for some situations of practical value (analysis of protection strategies and some consequences of their violations, diagnostics of mistaken prediction of a risk zone).

Based on the analysis of narrow places of the model, Section 3 defines the approaches to its further development and statement of new research problems.

1. Model and method for defining subsystems and nodes of a complex object of protection most exposed to terrorist attacks

1.1. Formalization of the term “susceptibility of an object to terrorist attacks”

The main task in defining subsystems and nodes most exposed to DB can be treated from various points of view depending on the context wherein the results of its solution are intended to be used in practice.

In particular, when formalizing the term “susceptibility of an object to terrorist attacks”, the property of a facility’s susceptibility to terrorist attacks TL , as well as other similar properties, can be considered as

- own **property of an object**, $TL(o)$;
- object-oriented **property of the environment** from where a more or less permanently operating disturbing factor of a terrorist attack possibly accompanied by collateral and counteracting factors arise, $TL(E)$ ¹;
- property $TL(o,E)$ considering **both constituents**.

In any case, even if for applied objectives, a complex property is required, it seems reasonable to know how to evaluate its constituents separately. And this applies to a criterion approach as well as an approach based on risks.

In formal and logic terms, we can speak about “things” where the investigated property P belongs to.

For example, in the approach based on vulnerability [4], the vulnerability is considered as an infrastructure facility’s or territory’s own property, $P(o)$. The approach used by a well-know British analytical company Maplecroft [5] who analyzes the susceptibility of countries to risks of terrorist attacks studies a complex index characterizing the property of environment, $P(E)$. However, Maplecroft also does analyses of complex risks taking into account, besides outer threats of terrorism, for example, inner risks for business or human rights, i.e. analyzing a complex property $P(o,E)$.

¹ This property is particularly clear in case of outer terrorism and outer forces that influence its intensity when it is natural to consider the environment as outer environment. However, in case of inner or mixed terrorism as well, it is reasonable to single out factors that are relatively out of control for the terrorized party.

This section offers a model of the term TL , wherein susceptibility to terrorist attacks is treated as an infrastructure object's own property, $TL(o)$, which corresponds to the conditions of a relative stability of the "environment" and in particular to a permanently operating disturbing factor of terrorism. This model is focused on solving the main task within the context of such situations as assessment of an operational situation and decision making about directions of protection measures within a compound object, evaluation of the quality of its protection strategies etc.

1.2. Criteria of susceptibility to terrorist attacks

As a common criterion for assessment of an object o as part of a compound object, we accept the criterion $TL(o)$ that in terms of the interests of security services is interpreted as **a criterion of susceptibility to terrorist attacks** for an object o , and in terms of the interests of terrorists as a criterion of relative attractiveness of an object o **for making a terrorist attack**. The criterion $TL(o)$ is understood as a compound criterion comprising a couple of rough criteria defined in [3]:

$$TL(o) = (A(o), V(o)),$$

where $A(o)$ is the attractiveness of o for terrorists,
 $V(o)$ is the vulnerability of o .

The vulnerability $V(o)$ is considered as a property additional to protection – the vulnerability is maximum in case of minimum protection, and vice versa.

It is assumed that $A(o)$ characterizes the attractiveness independently of its protection (both natural and intentional), while a compound criterion $TL(o)$ is considered as **relative attractiveness**, since it takes into account both criteria, important for susceptibility to terrorist attacks.

Each of the constituting criteria, $A(o)$ and $V(o)$, is a variable which takes on values on a finite order scale.

Generally, rough scales are used for assessment, with a small range of values, very often verbal ones. For example, for assessment of vulnerability-protection, one may accept a four-valued scale:

«maximum vulnerability / minimum protection» (the level of protection is so low that it doesn't decrease the attractiveness for terrorists),

«vulnerability is quite high»,

«vulnerability is quite low»,

«minimum vulnerability / maximum protection» (the level of protection is so high that there is practically no relative attractiveness for terrorists).

It is assumed that intuitive estimations of relative attractiveness for terrorists have the properties of inexact monotony:

$$A(o_1) > A(o_2) \ \& \ V(o_1) = V(o_2) \Rightarrow \neg (TL(o_1) < TL(o_2))$$

$$V(o_1) > V(o_2) \ \& \ A(o_1) = A(o_2) \Rightarrow \neg (TL(o_1) < T(o_2)).$$

If in its composition, a compound object has facilities indiscriminative as to the criterion $TL(o)$, it is appropriate to speak about homogenous facilities and a type of objects. Further on let us consider the notation o as referring to the type of objects.

Relation of estimations to the state of an object. Estimations of an object of protection as to the criterion $TL(o)$ characterizes its current state. An important difference of constituents consists in the fact that the property of vulnerability (or, on the contrary, protection) is controllable for security services. Also, generally speaking, the state of vulnerability can change due to various factors such as the quality of operational activities of security services. The current estimation as to the criterion of vulnerability $V(o)$ corresponds to the strategy of facilities protection, similar for all the objects of the type.

For solving tasks related to definition of most vulnerable objects in this model, it is assumed that the current state of vulnerability corresponds to estimations.

1.3. Structural model of a compound object of protection

Generally, a compound object of protection is considered as a hierarchy of constituting facilities, including elementary ones, i.e. indivisible ones for the accepted structuring (“nodes”) and composite facilities (“subsystems”). In the **T** typology of objects comprising a compound object, the facilities indiscriminate in terms of susceptibility to terrorist attack belong to the same type.

For example, of the same type within a **big city** compound object of protection can be all **international airports** with similar protection / vulnerability, and their constituents can be such facilities as “**green zone**”, **arrival areas** etc. (as exemplified by the terrorist attack at the Domodedovo airport in 2011 [6]).

A **hierarchy node** in the **T** typology of objects is some type of compound objects O comprising a set of types of constituting facilities (elementary or composite ones) belonging to the nearest lower level of the hierarchy.

A hierarchy node of a complex infrastructure object like an airport can be considered as a separate facility of protection if an individual strategy of protection is developed for it.

When solving the main task, as the simplest structural model of a compound object, we study the model M_0 comprising one node of hierarchy. It is attractive in that we can apply to it a model of multicriteria optimization – search of the most attractive types of objects in a set of object types forming the **T** typology of such compound object O .

By the **S strategy** of protection of a compound object O we’ll understand a set of more or less heuristic rules to define which types of objects are acceptable (or unacceptable) in the $T(O)$ typology of a protected object O . (Examples of such rules will be given below.)

The method for solving the main task is developed by now for the model M_0 .

1.4. Formal statement of the problem

Let there be a compound object O with one level of hierarchy, $O=\{o\}$, and for it there is defined what follows:

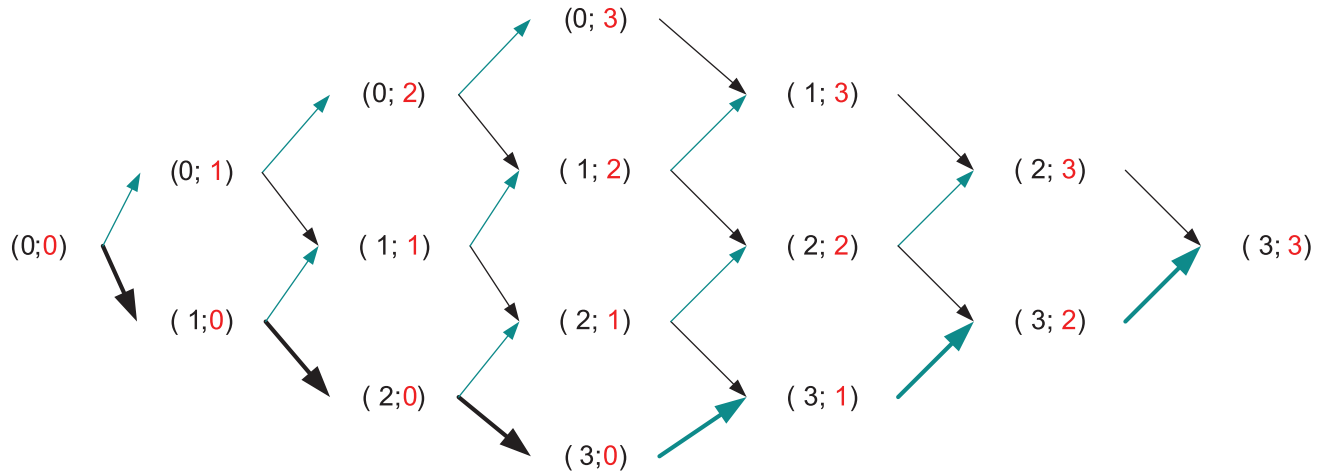
- scales S_1, S_2 for assessment of object types as part O as to criteria of attractiveness for terrorists, $A(o)$, and vulnerability, $V(o)$, respectively;
 - typology of objects as part of the object O , $T(O)$ with evaluations on the set scales;
 - S strategy of protection of the object O .

It is necessary to define the **risk zone** Z , i.e. the type of objects or, more generally, a set of object types, relatively most attractive for making a terrorist attack, in other words, most exposed to the risk of a terrorist attack.

For the sake of simplification, assume that all the values on each of estimation scales S_1, S_2 are used for assessment of objects as part of O .

1.5. Description of the problem solution method

To make it clear, the method is exemplified by a case where identical scales with scores (0,1,2,3) are accepted for each criterion. In Fig. 1 a full set $\bar{M}$ of object types imaginable for accepted scales of estimation as to a complex criterion $TL(o)$ is presented as a so called Hasse diagram. Each type of facilities is presented by a pair of values:



Susceptibility to terrorist attacks $TL(o) = (A(o), V(o))$

Fig. 1. Full set of types of objects possible for the adopted scales of assessment as to the compounded criterion

For example, pair (1,3) means the type of objects with scores $A(o)=1$, $V(o)=3$. The arrows show the increase of a score as to one of the criteria with the score remaining the same as to the other criterion.

The set $\bar{M}$ is partially normalized. Thus,

- range (sequence) $R1=((3;0), (3;1), (3;2), (3;3))$ presents all the types of objects most attractive as to the first criterion, attractiveness, $A(o)$, which are ordered as per increase of the second criterion, vulnerability, $V(o)$;
- range $R2=((0;0), (0;1), (0;2), (0;3))$, on the contrary, presents all the types of objects least attractive as to the criterion $A(o)$, which are also ordered as per increase of the criterion $V(o)$;
- range $R3=((0;0), (1;0), (2;0), (3;0))$, presents all the types of objects least attractive as to the second criterion, vulnerability (i.e. assessed as invulnerable), which are ordered as per increase of the first criterion $A(o)$.

Stage 1. Definition of the typology of objects as part of a compound object O according to the adopted strategy of protection S

When choosing a strategy of protection, one generally relies on intuitive heuristic rules of thumb that are thought rational, and one assumes that the counteracting party is rational (though in its own way).

In terms of selection of a protection strategy, it is obvious that terrorists would find as relatively most attractive as to the complex criterion $TL(o)$ the type of objects with a score (3,3), i.e. most attractive and most vulnerable ones, as well as objects near as per score to (3,3).

On the contrary, it is natural to suppose that the types of objects of range $R3$ would have a zero attractiveness as to the criterion $A(o)$, independently of their vulnerability.

Let us consider examples of heuristic rules that can be assessed as rational.

General rule 1, $R1$ ("objects not attractive for terrorists are not protected"). According to this rule, objects with score within O protected as to the rule $R1$ from the potential range of objects $R2=((0;\sim))$ where « $\sim$ » is any vulnerability, in the set M_{R1} of object types accepted by this rule can be only objects of

the type (0;3), i.e. unprotected. (Of course, this rule implies that by default we speak only about protection against terrorists, and natural properties of object protection are not taken into account for the sake of convenience).

In some strategy S' the type of objects (1;0) intuitively close to R2 in terms of attractiveness can also be excluded by an additional **specific rule** $R1'$.

General rule 2, R2 (“**more attractive objects cannot be more vulnerable**”). According to this rule, if even one of the type of object is protected, this should be the type (3;3). An additional specific rule $R2'$ by means of protection (i.e. reduction of vulnerability) can exclude for example the types of objects (2;3), (3,2), (2;2), (3;1) closer to (3;3) compared to others.

In Fig. 2 you can see in the full set of object types those darkened objects that should not be within a compound object O for the adopted strategy of protection $S=\{R1, R2, R2'\}$.

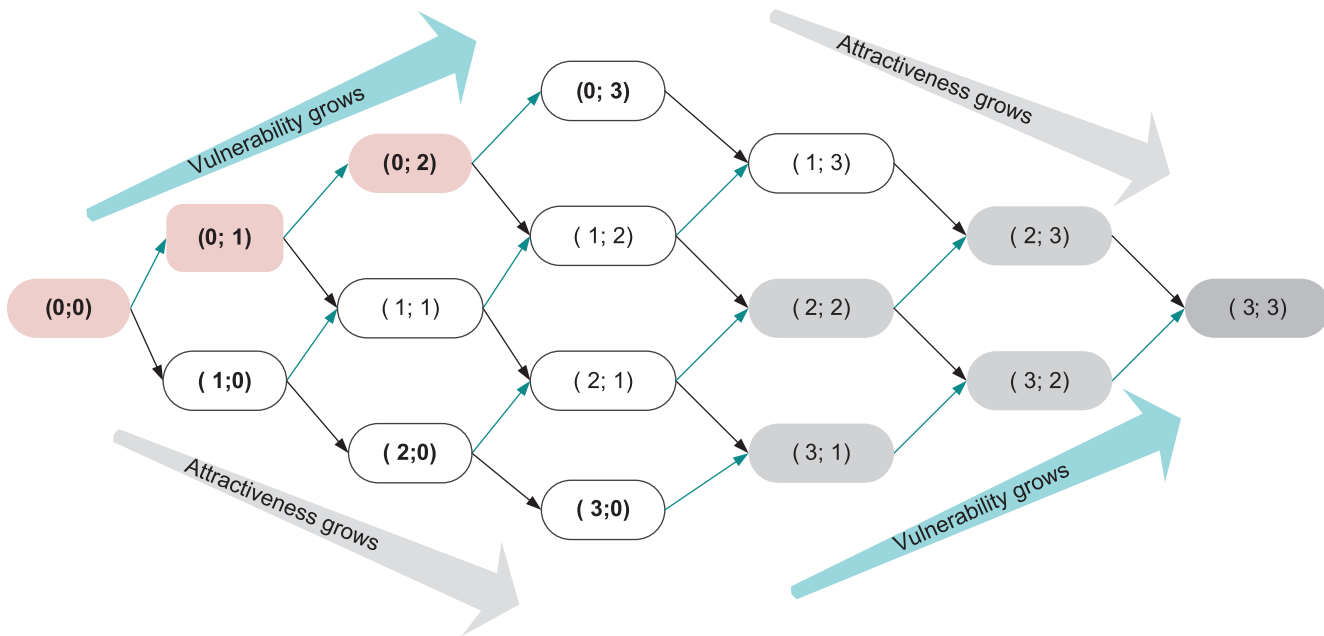


Fig. 2. Set of types of objects when protected using S strategy

Generally, according to the general rules of protection R1, R2, when constructing a set of object types M_S which are evaluated as more or less susceptible to a threat, we exclude from the full set $\bar{M}$ the set $M_{\bar{\epsilon}}$ of object types that in principle cannot be in the typology $O \setminus$ in O as to the rule R1 (in the example this is the set $M_{\bar{\epsilon}} = \{(3;3), (2;3), (3,2), (2;2), (3;1)\}$), on the one hand, and the zone M_u , on the other hand, relatively unattractive due to low attractiveness even in case of protection unavailability (in the example, $M_u = \{(0;0), (0;1), (0;2)\}$). In comparison to objects from $M_{\bar{\epsilon}}$, objects from M_u can be present in the typology O , but they are not considered as objects of protection.

The results of application of a protection strategy is received as the set M_S ,

$$M_S = \bar{M} \setminus (M_{\bar{\epsilon}} \cup M_u)$$

Stage 2. Definition of Pareto set in $\bar{M}$. Rough estimation of the highest susceptibility to terrorist attacks

Fig. 3 shows the division of the set $\bar{M}$ of the example under consideration into 2 classes: Pareto set $M_A = \{(1;3), (2;1), (3;0)\}$ and a set of all other types of objects $M_O = \{(1;0), (2;0), (1;1), (1;2), (0;3)\}$.

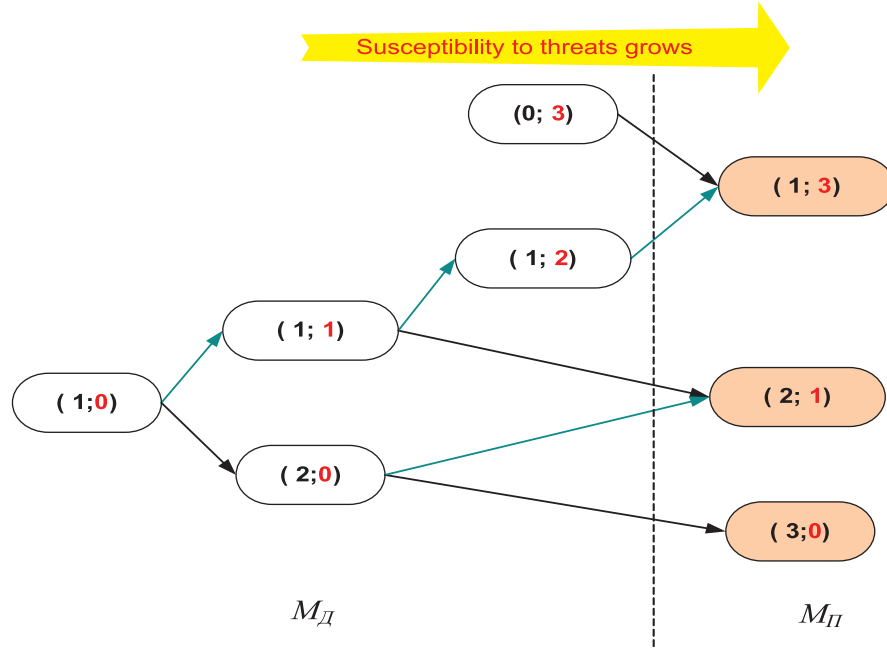


Fig. 3. Types of objects most exposed to terrorist attacks as per Pareto

Compared to a Pareto set of object types, all the objects of the set M_O are **dominated** in $\bar{M}$. Graphically the property of domination of the object type o by the type o' is expressed in that the route from the type o goes to the type o' . Thus, for the dominated type $(1;0)$, dominating types as per the criterion of vulnerability are more vulnerable types $(1;1)$, $(1;2)$, $(1;3)$ with their equal attractiveness, and $(1;3) \in M_H$, i.e. it is not dominated by any other objects; the objects of type $(1;0)$ are dominated as per the criterion of attractiveness by the objects of type $(2;0)$, $(3;0)$, with their equal vulnerability, and $(3;0) \in M_H$. For the same type $(1;0)$, the type $(2;1)$ is a dominating one both as per the criterion $V(o)$ and $O(o)$, $(2;1) \in M_H$.

The fact that some type o is dominated as per some or all specific criteria means that it is less susceptible to terrorist attacks than dominating types (in case of real selection based on specific criteria). On the contrary, the fact that the type of objects o belongs to the set M_A means that there are no dominating types for it, and on the basis of separate criteria as part of $TL(o) = (A(o), V(o))$ such types are incomparable, and all of them can be considered as most susceptible to terrorist attacks as per Pareto criterion.

Such solution seems to be natural when we attempt to get higher values if possible as per each of constituting criteria as part of $TL(o)$.

Generally they say that a Pareto set includes a subset of all elements where each of them is “not worse” than others.

Stage 3. Definition of expert preferences in a Pareto set

Despite the intuitive naturalness of defining a set of all objects types most susceptible to terrorist attacks as a Pareto set (for a selected set of constituting criteria, in this case PT_A), it is understandable that in this case by default we imply equivalence of constituting criteria, and there is no aggregation of estimations as per these criteria.

In reference with it, it is necessary to further specify a set of risk zone Z within the limits of Pareto sets,

$$Z \subset M_{UP}$$

The final selection should be done by experts taking into account not only a relative correlation of importance (weights) of criteria $A(o)$ and $V(o)$ in general, but in the first place considering the analysis of a specific Pareto set. In this case experts single out a risk zone Z from a Pareto set. The example of complete solution of the problem is shown in Fig. 4.

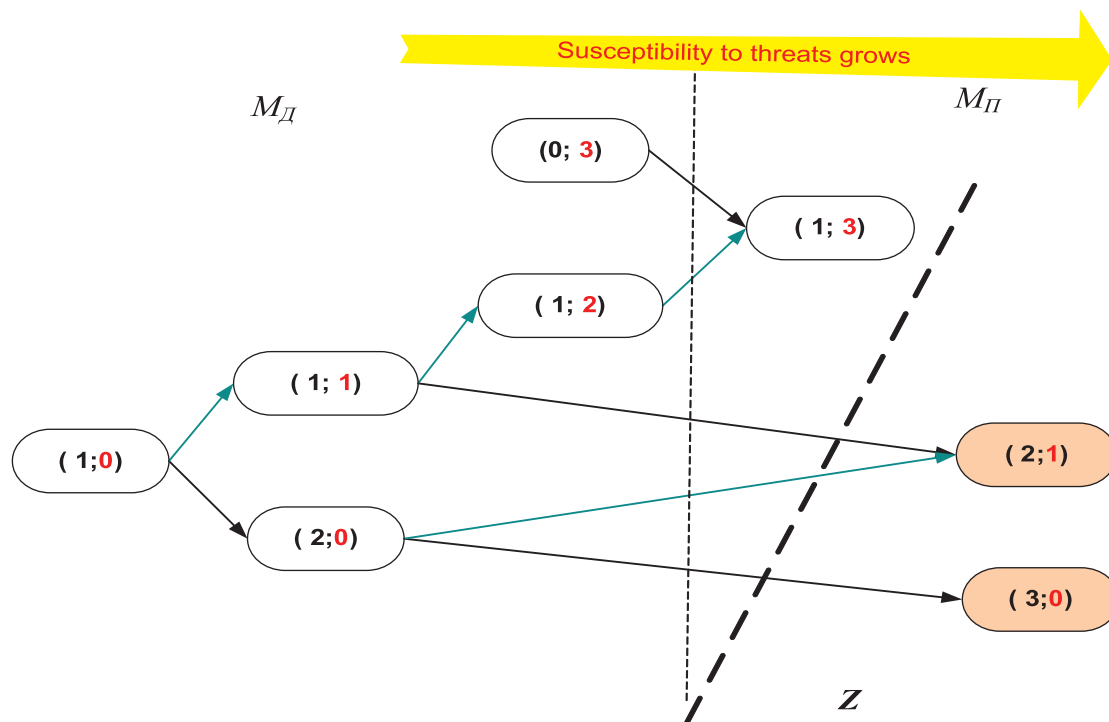


Fig. 4 Preferences within the Pareto set

2. Descriptive capabilities of the model and the method for situations of practical value

The descriptive capabilities of the investigated formalized model $M1$ of a situation where a risk zone Z is defined as part of a compound object O will be exemplified using the previous example in Fig. 1 for two types of situations of practical value.

Operational (in a specific situation) deterioration of protection of some facility in relation to standard protection (i.e. increase of vulnerability). Arrows 1 and 2 in Fig. 5 show two types of deterioration. Transit of an object from the type $(1;1)$ into the more vulnerable type $(1;2)$ and event in $(1;3)$ is not dangerous, as due to low attractiveness it will not be an object of a terrorist attack. (There is some reserve of dominating facilities that are out of a risk zone.)

On the contrary, increase of vulnerability of an object of type $(2;0)$ (transit from type $(2;0)$ into $(2;1)$) moves it into a risk zone Z .

A fresh example of the situation is increase of vulnerability of the arrival terminal in Domodedovo due to the decrease of protection quality by the transport police securing the airport entries.

To make decisions about responsibility for psychologically explainable reduction of quality in protection of a relatively unimportant facility, e.g. an airport entry, it is necessary to take into account that it is beyond the competence of the police to understand the structure of protection of facilities (such as Fig. 4) as well as the correlation between entry protection and preferences (relative attractiveness) of an arrival terminal as a place of a terrorist attack for terrorists.

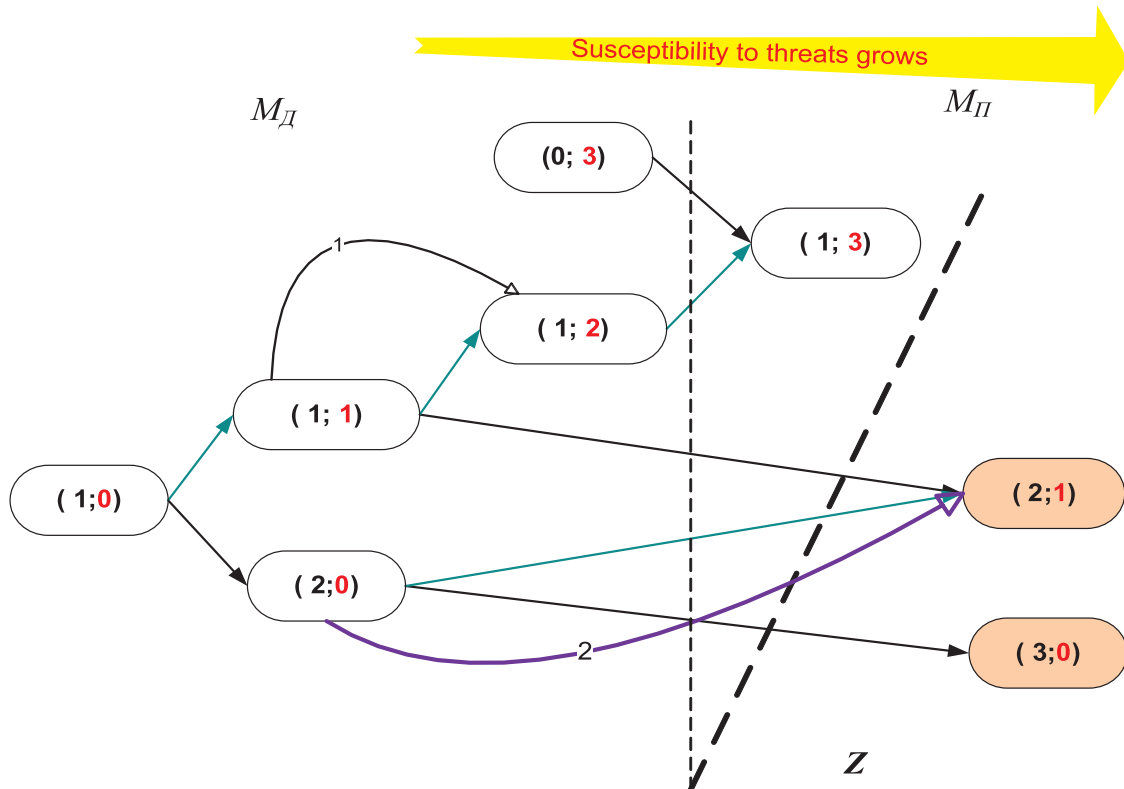


Fig. 5. Operational violations

Measures of ensuring and supervision over ensuring a required quality of protection strategy implementation as well as a strategy of protection itself should be in charge of security services protecting a compound object, an airport, due to their awareness as to the logics of management. It should not be ruled out that the quality of security could be influenced by simply briefing the guards that penalties for poor quality of protection of specific nodes were defined according to a (specified) level of risk.

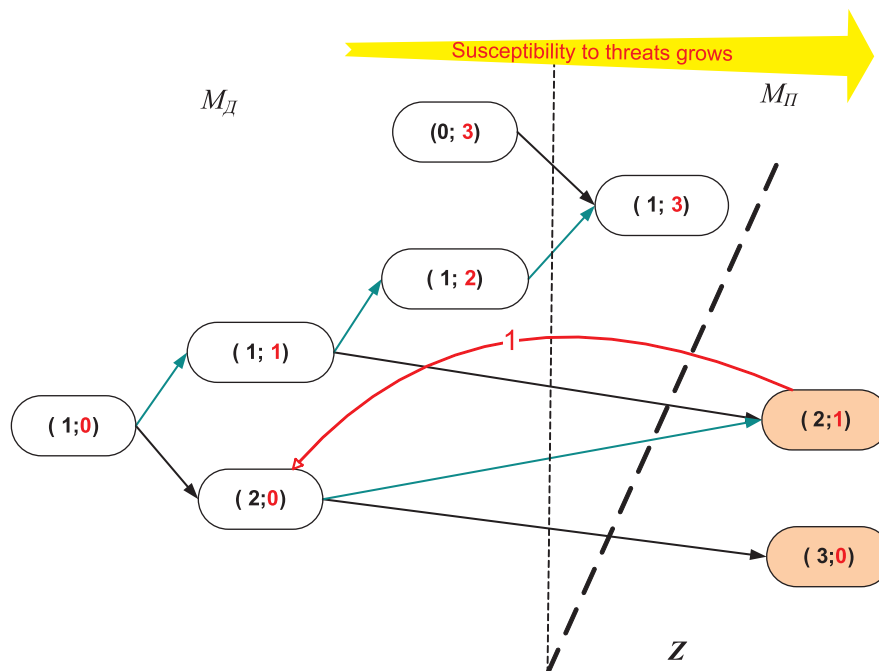


Fig. 6. Improvement of protection

Estimation of effect from a protection strategy change. The strategy “increase of protection level” that they start to promote in many countries after terrorist attacks should be naturally applied in the first place to a risk zone (or at least to a Pareto set), since otherwise a set of object types most exposed to terrorist attacks will not change.

Arrow 1 in Fig. 6 shows the effect from increase of a protection level for the objects of type (2;1) from the risk zone Z , i.e. their transit into a less vulnerable type (2;0).

As a result, the number of objects in a risk zone has decreased; however, in cases when a risk zone still contains only the objects with maximum protection (in this example (3;0)), further efforts in increasing protection of a compound object O will not change the set M of objects most exposed to threats.

Diagnostics of a mistakenly predicted risk zone. Prediction of a risk zone in a set of objects with varying degrees of protection and attractiveness by using the presented method or otherwise is based on a number of human assumptions. Such assumptions are among the risks for reliability caused by human factor [7]. Detection of erroneous prediction and in our case a fact of a terrorist attack at an object not being in a risk zone requires further diagnosis and correction of the model adopted for prediction. Reasons of forecast inaccuracy can be very different including violations of the protection strategy. Special role among these reasons is taken by mistakes of the model of attractiveness for terrorists, which is laid in the typology of objects to be protected through the evaluation of object types as per $A(o)$. (In theoretical terms, this is a false hypothesis of general knowledge.) At least one type of such errors consists in that from the viewpoint of terrorists, objects do not in fact belong to the type of attractiveness, as it is viewed by the protecting side.

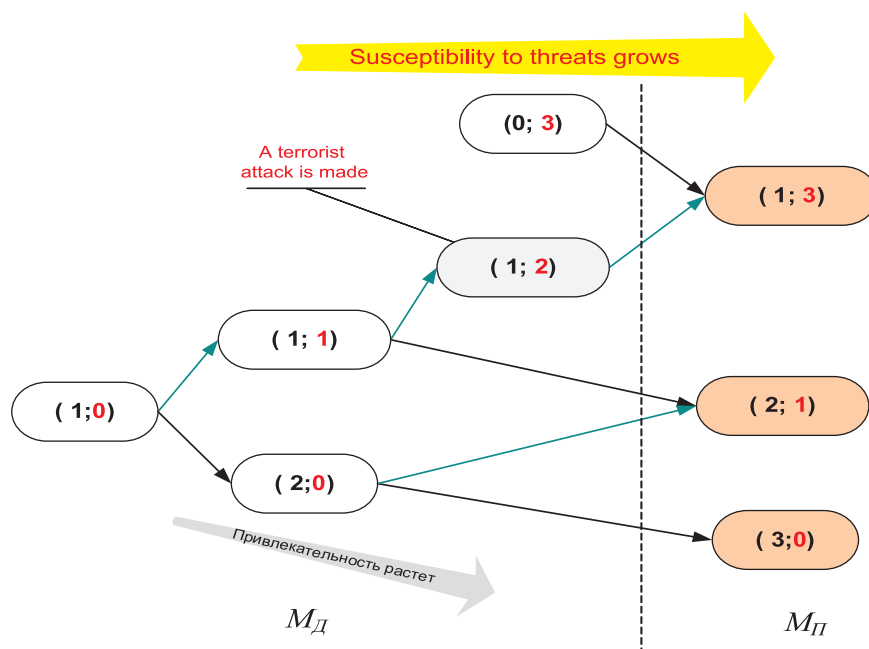


Fig. 7. Errors of the attractiveness model

The possibility of diagnosing such errors, i.e. forming hypotheses about the causes of errors, is shown for our example in Fig. 7 and Fig. 8. In Fig. 7 we have marked the object type (1;2), to which the object of a terrorist attack was attributed; this object does not belong to a risk zone, according to the accepted model of attractiveness for terrorists. One of the reasons that the terrorists did not follow this model, remaining within the framework of rationality hypotheses, could be that the protection of the object O is in general high and the pressure (intensity) of the destabilizing factor of terrorism is also high. The result may be a shift of the attractiveness model, not considered in predicting a risk zone (Fig. 8).

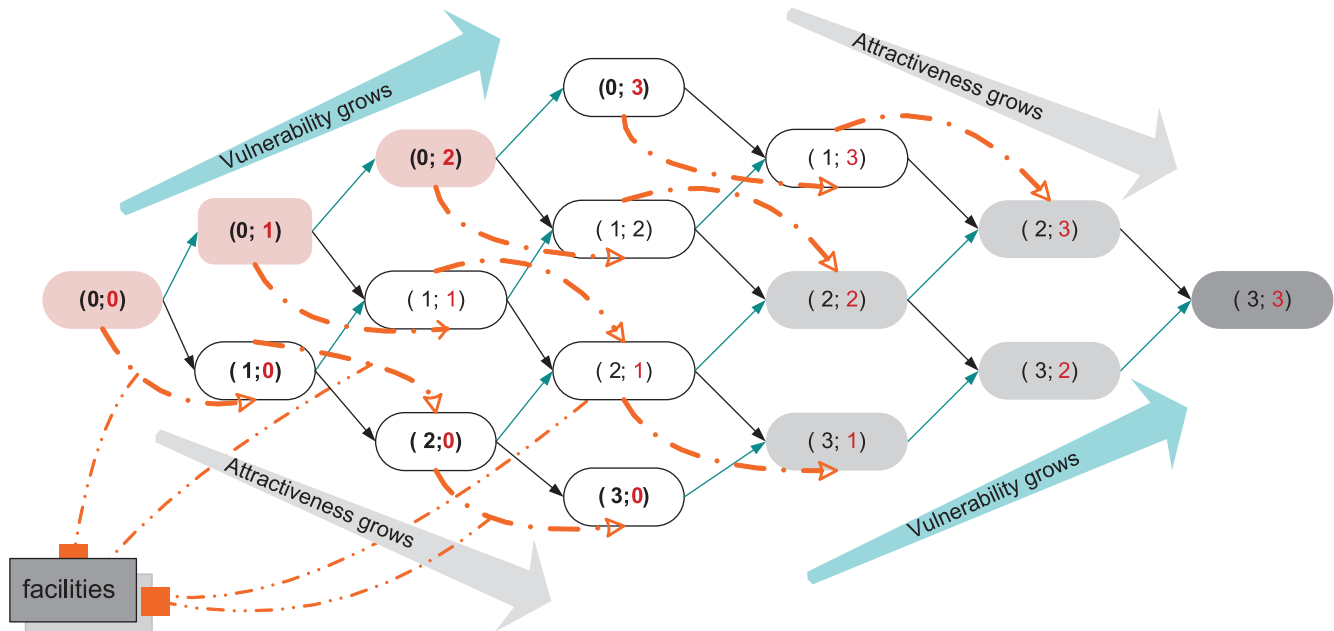


Fig. 8. Shift of the attractiveness model

3. Analysis of bottlenecks and limitations of a situation model forming the basis of the method. Further development

In accordance with the principle of development and cross-cutting application of verification methods to protect against risks to ensure the reliability of methods put in the basis of security systems, the proposed method of estimating objects most prone to terrorist attacks and a model of evaluation situations in which it can be applied should undergo analysis. The purpose of this analysis is to identify bottlenecks, constraints, risks due to a human factor.

To demonstrate the content and features of this analysis, let us present a fragment of such an analysis. It is based on the restriction of the proposed model consisting in the fact that the proposed criteria of attractiveness, $A(o)$, and vulnerability, $V(o)$ to assess certain types of objects as part of an object of protection are very generalized. To obtain estimates for these criteria, it is necessary to move from estimates as to specific criteria to integrated estimates as to criteria $A(o)$ and $V(o)$, and in this case these criteria may be interdependent.

Accounting of the dependence of $A(o)$ and $V(o)$ on general factors. It is not obvious how to take into account various specific criteria and factors in the composition of the main criteria: attractiveness, $A(o)$, and vulnerability-protection, $V(o)$, when assessing objects as to these two criteria.

First of all, we deal with such indices as criticality (importance) of an object, which can be attributed to $A(o)$ as well as to $V(o)$. Since a more critical object, on the one hand, is more attractive for terrorists, and on the other hand, it is usually more protected in accordance with typical security strategies of protection.

In the case of a criticality factor, $C(o)$, it is certainly among the main factors for evaluation of attractiveness, $A(o)$. However, in the model an estimation is made for the current state of affairs for a fixed protection strategy, $C(o)$, so the dependence of $C(o)$ on criticality is already included in the strategy, and its inclusion in the $V(o)$ is no longer required.

If it is necessary to review and compare different protection strategies, evaluate sensitivity to modifications of the strategy (or different knowledge of counteracting parties about it), it is required to consider

different models of the situation. It is recommended to do such activities related to modification of strategies using some software support (animation like in Fig. 6, Fig. 7) for clarity.

In all cases, an individual analysis is required for each criterion (or factor) to avoid duplication of accounting of the same factor via $A(o)$ and $V(o)$: in the proposed model the criteria $A(o)$ and $V(o)$ are treated as independent. (For this purpose, cognitive maps describing the interaction of various factors and their impact on selected generalized criteria may be useful. The example of such card is presented in [3].)

Further development in this direction consists in moving to reflexive models taking into account the estimations of the parties of others' knowledge. It is assumed that the further development of models and methods of its analysis should allow for not only taking into account the different knowledge of the opposing sides, but also the "reflexive games": mimicry in the case of terrorist attacks, creating traps for terrorists, etc.

When analyzing the influence of an external threat of a terrorist attack on a security system using the proposed method (or possibly other methods of the same kind), the focus is on the current state of vulnerability / security of a complex object and its current assessment by terrorists. However, in reality, for reliability of short-term predictions, it is also important to take into account the long-term dynamics of the interaction of an external destabilizing factor of terrorism and its attendant factors with internal strategic decisions on such interaction.

Conclusion

The offered model with the method of defining a risk zone in the situation when susceptibility of separate facilities of a complex object of protection is conditioned by two criteria, i.e. the attractiveness of separate facilities and their vulnerability (for the specified strategy of protection of a complex object), though simple, has shown its real value for various practical situations.

However, due to limitations related to the model, it is required that there will be the further development of the model and the method, from the one hand, and the development of the approach centered on the analysis of long-term dynamics of interaction of security systems with continuous disturbances made by the terrorism factor.

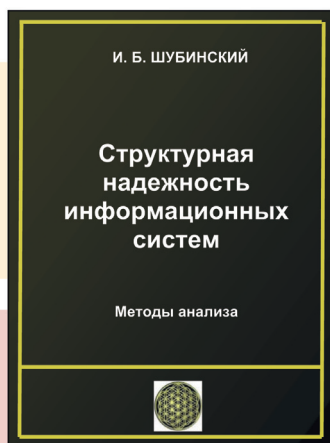
References

1. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426). – Hyattsville, MD: U.S. Federal Emergency Management Agency, 2003. – 420 p.
2. National and Global Security. Terrorism in a big city: assessment of threats and protection/Ed. Dvorkin V.Z. M.: Human Rights Publishing House, 2002. – 113 p.
3. **Makarenko D.I.** Systematization of criteria and critical factors for assessment of complex systems exposure to disturbances / Dependability, 2013, #4.
4. **D. Sarewitz, R. Pielke, M. Keykhah** Vulnerability and Risk: Some Thoughts From A Political and Policy Perspective, Risk Analysis, Vol. 23, No. 4. (2003), 805-810.
5. Review of Maplecroft's "Terrorism Risk Index 2011", Link: <http://foreignpolicyblogs.com/2010/12/04/review-of-maplecrofts-%E2%80%9Cterrorism-risk-index-2011%E2%80%9D/> (request data: 08.08.2013)
6. Terrorist attack at the Domodedovo airport. Wikipedia [Web resource] Link: <https://ru.wikipedia.org/wiki/> (request data: 01.08.2013)
7. **Abramova N.A.** About human factor risks in expert methods and information technology // Management issues– 2007, #2, p.11-17.

НАДЁЖНОСТЬ

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

Структурная надежность информационных систем

Методы анализа



Шубинский Игорь Борисович

СТРУКТУРНАЯ НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
Методы анализа

Редактор: Патрикеева Евгения Владимировна
Компьютерная верстка: Куртиш Борис Сергеевич
Корректор: Комарова Екатерина Евгеньевна

Подписано в печать 12.07.2012. Формат издания 70х100/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 17,55.
Тираж 700 экз. Заказ № 1452.

ООО «Журнал «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.

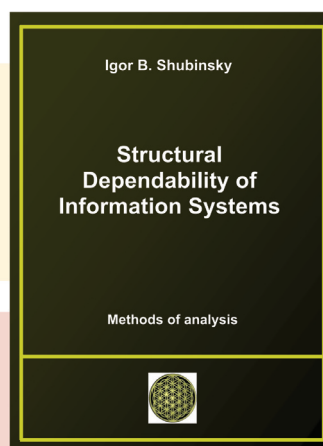
The book is intended primarily for professionals involved in practical work on the development, production, operation and modification of information systems. It is designed for scientists in the field of structural dependability of various discrete systems, academic staff and graduates (students) specializing 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

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



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

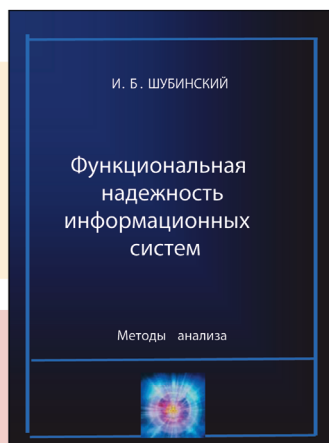
Editor: Patrikeeva Evgenia
Make-up: Kurtish Boris S.
Proofreading: Komarova Catherine E.

Copy deadline 12.07.2012. Format of the edition 70х100/16.
Offset printing. Offset paper. Conv. Sheet I. 24,05.
Circulation of 700 copies. Order number 1452.

НАДЁЖНОСТЬ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

ПРЕДСТАВЛЯЕТ



Приобрести издание можно через редакцию ООО «Журнал «Надёжность»»

8 (495) 967-77-05, доб.186
8-916-105-81-31
(Патрикеева Евгения)

E.Patrikeeva@gismps.ru,
www.dependability.pro

И. Б. ШУБИНСКИЙ

**Функциональная
надёжность
информационных
систем**

Методы анализа

Шубинский Игорь Борисович
ФУНКЦИОНАЛЬНАЯ НАДЁЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
Методы анализа

Редактор: Патрикеева Евгения Владимировна
Компьютерная верстка: Куртиш Борис Сергеевич
Корректор: Комарова Екатерина Евгеньевна

Подписано в печать 12.07.2012. Формат издания 70х100/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 24,05.
Тираж 700 экз. Заказ № 1453.

ООО «Журнал «Надёжность»»,
109029, г. Москва,
ул. Нижегородская, д.27, стр.1, офис 209
Тел./факс: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

И.Б.Шубинский «Функциональная надёжность информационных систем» 2012г.

В книге впервые представлена теория функциональной надёжности информационных систем как составная часть общей теории надёжности. Она включает понятия и определения; основные угрозы нарушения функциональной надёжности информационных систем; систему показателей; методы оценки функциональной надёжности цифровых устройств; методы и модели оценки функциональной надёжности программного обеспечения. В отдельной главе рассмотрена функциональная надёжность критически важных информационных систем, в том числе понятие критически важной системы, особенности оценки сбойных ошибок, оценки функциональной надёжности операторов, оценки опасных отказов и рисков, требования к функциональной надёжности и к архитектуре программного обеспечения критически важных информационных систем.

В конце каждой главы содержатся контрольные вопросы по наиболее сложному и значимому материалу главы.

Книга рассчитана, в первую очередь, на специалистов, занимающихся практической работой по разработке, производству, эксплуатации и модификации информационных технологий и информационных систем. Она предназначена научным работникам в области надёжности программно – аппаратных средств информационных систем, преподавательскому составу, аспирантам и студентам, специализирующимся в области информационных технологий, а также в области автоматизированных систем управления.

Приобрести издание можно через редакцию журнала «Надёжность» по тел. 8 (495) 967-77-05, доб.186; 8-916-105-81-31 (Патрикеева Евгения), e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

Igor B. Shubinsky FUNCTIONAL DEPENDABILITY OF INFORMATION SYSTEMS 2012

For the first time, this book presents the theory of functional dependability of information systems as a component of the general dependability theory. The book comprises basic concepts and definitions, major threats for the functional dependability of information systems, system parameters, methods for estimating the functional dependability of digital devices, and methods and models of estimating software functional dependability. A separated chapter considers the functional reliability of critical information systems, including the concept of a critical system, features of faults, estimation of functional reliability of operators, estimation of hazardous failures and risks, the requirements of functional dependability and the software architecture of critical information systems. A checklist of the most complex and significant subjects is provided at the end of each chapter.

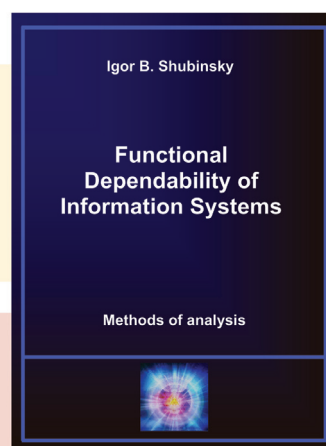
The book is primarily intended for experts who are engaged in practical development, manufacture, operation and updating of information technologies and information systems. It is intended for researchers in the field of software-hardware of information systems, academic staff, post-graduate students and students specializing in the field of information technologies as well as those working in the field of automated control systems.

Publication can be purchased through the editorial board of Journal Dependability Ltd.
by phone 8 (495) 967-77-05, ext.186; 8-916-105-81-31 (Patrikeeva Evgenia)
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

НАДЁЖНОСТЬ

DEPENDABILITY SCIENTIFIC AND TECHNICAL JOURNAL

REPRESENTS



Publication can be purchased through the editorial board of Journal Dependability Ltd.

8 (495) 967-77-05, ext.186;
8-916-105-81-31
(Patrikeeva Evgenia)

E.Patrikeeva@gismps.ru,
www.dependability.pro

Igor B. Shubinsky

**Functional
Dependability of
Information Systems**

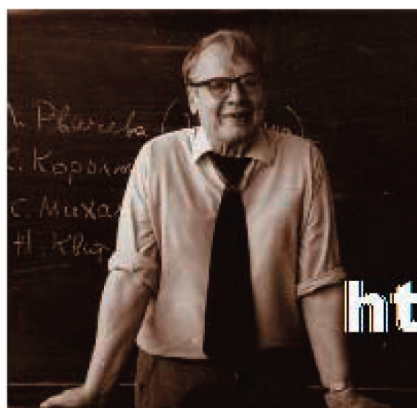
Methods of analysis

Igor B. Shubinsky
STRUCTURAL DEPENDABILITY OF INFORMATION SYSTEMS
Methods of analysis

Editor: Patrikeeva Evgenia
Make-up: Kurtish Boris S.
Proofreading: Komarova Catherine E.

Copy deadline 12.07.2012. Format of the edition 70х100/16.
Offset printing. Offset paper. Conv. Sheet I. 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



Дорогие коллеги!

В 2005 году была основана неформальная Ассоциация специалистов по надежности, прикладной вероятности и статистике (I.G.O.R.), которая имеет свой сайт в Интернете GNEDENKO FORUM. Сайт назван в честь выдающегося математика Бориса Владимировича Гнеденко (1912-1995). Целью Форума является улучшение профессиональных и персональных контактов специалистов по математической статистике, теории вероятностей и их важных ветвей, как Теория надежности и контроля качества, Теория массового обслуживания, Теории управления запасами и т.п.

Начиная с января 2006 года Форум издает ежеквартальный Международный электронный журнал

«Надежность: Теория и приложения» ("Reliability: Theory & Applications").

Журнал зарегистрирован в Библиотеке Конгресса США (ISSN 1932-2321). Все права сохраняются за авторами, так что статьи затем могут быть свободно опубликованы в любых других изданиях или представлены на конференции.



**Вступайте в Форум
Гнеденко!**

Добро

пожаловать!

В наших рядах уже более

500 специалистов

из **44** стран мира.

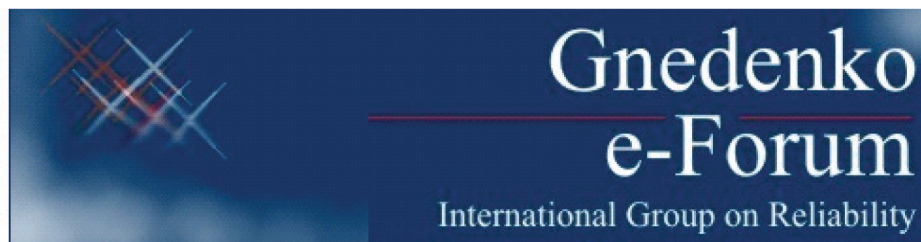
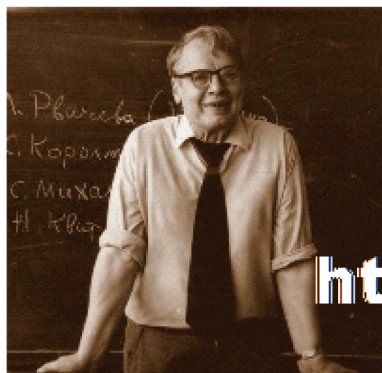
Для вступления в
Форум присылайте
фото и краткое резюме
по адресу:

Проф. Игорь Ушаков,
igusha22@gmail.com

или

к.т.н. Александр Бочков,
a.bochkov@gmail.com

Membership is free.



<http://Gnedenko-Forum.org/>

Dear colleagues!

In 2005 the informal Association of Experts in Reliability, Applied Probability and Statistics (I.G.O.R.) was established with its own Internet website GNEDENKO FORUM. The site has been named after the outstanding mathematician Boris Vladimirovich Gnedenko (1912-1995). The Forum's purpose is an improvement of personal and professional contacts between experts in the mathematical statistics, probability theory and their important branches, such as reliability theory and quality control, the theory of mass service, storekeeping theory, etc.

Since January 2006, the Forum has published a quarterly international electronic magazine

"Reliability: Theory and Applications".

The magazine is registered with the Library of Congress in the USA (ISSN 1932-2321). All rights reserved for authors so that articles can be freely published in any other publications or presented at conferences.



Join Gnedenko Forum!

Welcome!

**More than 500 experts
from 44 countries
worldwide have already
joined us!**

To join the Forum, send a
photo and a short CV to the
following address:

Prof. Igor Ushakov,
igusha22@gmail.com

or

Alexander Bochkov, PhD
a.bochkov@gmail.com

Membership is free.

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 приставным 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; строки 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 , $\odot$ — 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.: 8-916-105-8131
e-mail: E.Patrikeeva@gismps.ru

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: lab51.ipu@gmail.com

Ададуров Александр Сергеевич

кандидат технических наук, доцент, директор Санкт-Петербургского филиала ОАО «НИИАС»
тел.: +7 (812) 380-53-03
e-mail: a.adadurov@niias-spb.ru

Ададуров Сергей Евгеньевич

доктор технических наук, профессор, советник генерального директора ОАО «Росжелдорпроект»
тел.: +7 (495) 663-00-60
e-mail: czi_mpc@mail.ru

Антонов Александр Владимирович

доктор технических наук, профессор, декан факультета «Кибернетики» Обнинского института атомной энергетики (ИАТЭ НИЯУ МИФИ)
e-mail: antonov@iate.obninsk.ru

Власов Виктор Александрович

доктор технических наук, профессор, профессор кафедры «Автоматика» Национальный исследовательский ядерный университет «МИФИ»
e-mail: vlasov1941@yandex.ru

Власова Светлана Викторовна

старший инженер ОАО «ВНИИАЭС»
e-mail: kaf46@mail.ru

Ермаков Александр Олегович

руководитель Центра управления рисками ОАО «НИИАС»
тел.: +7 (495) 967-77-02
e-mail: alex267@rambler.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: lab51.ipu@gmail.com

Мальцев Георгий Николаевич

доктор технических наук, профессор ВКА им. Можайского
тел.: +7 (812) 385-12-67
e-mail: georgy_maltsev@mail.ru

Никитаев Валентин Григорьевич

доктор технических наук, профессор, Национальный исследовательский ядерный университет «МИФИ», заведующий кафедрой «Компьютерные медицинские системы»
e-mail: VGNikitayev@mephi.ru

Новожилов Евгений Олегович

кандидат технических наук, главный специалист Центра управления рисками ОАО «НИИАС»
тел.: +7 (495) 967-77-02
e-mail: novozhilov@newmail.ru

Перегида 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

Проничев Александр Николаевич

кандидат технических наук, Национальный исследовательский ядерный университет «МИФИ», доцент кафедры «Компьютерные медицинские системы»;
e-mail: ANPronichev@mephi.ru

Телицына Татьяна Андреевна

младший научный сотрудник лаборатории №51, Институт проблем управления им. В.А.Трапезникова РАН (ИПУ РАН)
тел.: +7 (495) 334-78-00
e-mail: lab51.ipu@gmail.com

Ткачев Олег Алексеевич

Доцент кафедры «Прикладная информатика» Института математики и информатики Московского педагогического университета, кандидат технических наук, доцент
тел.: +7 (916) 063-98-00
e-mail: tkachev_oleg55@mail.ru

Федотова Галина Алексеевна

Кандидат технических наук, старший научный сотрудник Институт систем энергетики им. Л.А. Мелентьева СО РАН
тел.: +7 (3952) 42-34-86
e-mail: fedotova@isem.sei.irk.ru

Чумаков Илья Александрович

аспирант кафедры АСУ

Обнинский институт атомной энергетики –
филиал Национального исследовательско-
го ядерного университета «МИФИ»
e-mail: aidforwork@gmail.com

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

Adadurov Alexander Sergeevich

PhD Engineering, Director of St. Petersburg
Branch of JSC NIIAS
Tel.: (812) 380-53-03
E-mail: a.adadurov@niias-spb.ru

Adadurov Sergey Evgenyevich

Doctor of Technical Sciences, Professor,
Adviser of Director General of JSC
Roszheldorproject
Tel.: +7 (495) 663-00-60
E-mail: czi_mpc@mail.ru

Antonov Alexander Vladimirovich

Doctor of Technical Sciences, Professor, Dean
of Faculty of Cybernetics,
Obninsk Institute of Atomic Energy, National
Research Nuclear University MIFI
E-mail: antonov@iate.obninsk.ru

Vlasov Victor Alexandrovich

Doctor of Technical Sciences, Professor,
Professor of Chair of Automation,
National Research Nuclear University MIFI
E-mail: vlasov1941@yandex.ru

Vlasova Svetlana Victorovna

Senior engineer of JSC VNIIAES
E-mail: kaf46@mail.ru

Ermakov Alexander Olegovich

Head of Risk Management Center JSC NIIAS
Tel.: +7 (495) 967-77-02
E-mail: alex267@rambler.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

Maltsev Georgy Nikolayevich

Doctor of Technical Sciences, Professor
Mozhaysky Military Space Academy

Tel.: +7 (812) 385-12-67

E-mail: georgy_maltsev@mail.ru

Nikitaev Valentin Grigoryevich

Doctor of Technical Sciences, professor,
National Research Nuclear University MIFI,
Head of Chair of Computer Medicine Systems
E-mail: VGNikitayev@mephi.ru

Novozhilov Evgeniy Olegovich

PhD Engineering, Senior Specialist of Risk
Management Center JSC NIIAS
Tel.: +7 (495) 967-77-02
E-mail: novozhilov@newmail.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.obninsk.ru

Pronichev Alexander Nikolayevich

PhD Engineering, National Research Nuclear
University MIFI,
Assistant professor of Chair of Computer
Medicine Systems
E-mail: ANPronichev@mephi.ru

Telitsyna Tatyana Andreevna

Junior 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

Tkachev Oleg Alekseevich

PhD Engineering, Assistant professor of Chair
of Applied Informatics,
Institute of Mathematics and Informatics,
Moscow Pedagogical University
Tel.: +7 (916) 063-98-00
E-mail: tkachev_oleg55@mail.ru

Fedotova Galina Alekseevna

PhD Engineering, senior researcher of
Melentiev Energy Systems Institute,
Siberian Branch of the Russian Academy of
Sciences
Tel.: +7 (3952) 42-34-86
E-mail: fedotova@isem.sei.irk.ru

Chumakov Ilya Alexandrovich

Postgraduate student of Chair of Automated
Control Systems,
Obninsk Institute of Atomic Energy, National
Research Nuclear University MIFI
E-mail: aidforwork@gmail.com

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/MЭК 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.