ISSN 1729-2646
e-ISSN 2500-3909
том **25**, №**4**
2025

НАДЕЖНОСТЬ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

В НОМЕРЕ

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПУБЛИКАЦИЙ В ЖУРНАЛЕ «НАДЕЖНОСТЬ»

СТРУКТУРНАЯ НАДЕЖНОСТЬ

- 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 этапах жизненного цикла
- Методы испытаний, критерии принятия решений по результатам испытании, ускоренные испытания, методы оценки надежности систем по результатам испытаний

ФУНКЦИОНАЛЬНАЯ НАДЕЖНОСТЬ

- Объект, предмет и цели исследования, показатели функциональной надежности, терминология, принципы и методы расчета
- Методы оценки и прогнозирования надежности программного обеспечения и программно-аппаратных комплексов 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

- Показатели функциональной безопасности; функции безопасности, полнота безопасности
- 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

- Методы пассивной защиты от отказов, математические модели структурного резервирования, постепенной деградации избыточных систем, маскирования неисправностей, 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.

УПРАВЛЕНИЕ РИСКАМИ

- Общая теория рисков, методологические вопросы формализации рисков
- Классификация рисков объектов. Принципы и методы оценивания рисков. Методы определения допустимых уровней риска. Методология управления рисками разной природы
- Методы и модели определения интегральных рисков

СЕРТИФИКАЦИЯ И СТАНДАРТИЗАЦИЯ

- Аккредитация органов по сертификации и испытательных лабораторий - состояние проблемы 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
- Влияние закона «О техническом регулировании» на развитие теории и практики надежности и функциональной безопасности
- Состояние и перспективы стандартизации в области надежности, отказоустойчивости и живучести, функциональной безопасности и управления рисками

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ

- Методы проактивного управления надежностью и безопасностью
- Методы оценивания надежности и безопасности при неполных данных
- Нормирование показателей надежности и безопасности в больших системах
- Методы проектирования надежности и безопасности уникальных ответственных систем

ТЕХНИЧЕСКАЯ ЭФФЕКТИВНОСТЬ СИСТЕМ УПРАВЛЕНИЯ

- Показатели функциональной и технической эффективности
- Методы оценивания технической эффективности систем управления
- Технологии построения систем управления с повышенной эффективностью
- Нормативные требования к обеспечению технической эффективности систем управления

УПРАВЛЕНИЕ ТЕХНИЧЕСКИМИ АКТИВАМИ

- Проблемы управления техническими активами в больших системах
- Методология управления техническими активами
- Управление техническими и техногенными рисками в больших системах
- Управление ресурсами составных объектов систем
- Оценка деятельности структурных подразделений
- Корпоративная платформа управления техническими активами

ОБРАБОТКА БОЛЬШИХ ДАННЫХ. СИСТЕМЫ УПРАВЛЕНИЯ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

- Технологии подготовки больших данных и отбора признаков для машинного обучения
- Методы и алгоритмы машинного обучения, развитие и результаты применения технологии больших данных
- Прогнозирование динамики изменения состояний систем управления
- Применение методов искусственного интеллекта в задачах надежности и безопасности

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

- Методы защиты информации в автоматизированных системах управления
- Методы обеспечения безопасности информации в программных средствах
- Системы защиты информации
- Методы и технологии комплексного обеспечения функциональной и информационной безопасности в системах управления
- Технологии подтверждения соответствия требованиям безопасности информации

СИСТЕМНЫЙ АНАЛИЗ В ЗАДАЧАХ НАДЁЖНОСТИ И БЕЗОПАСНОСТИ

- Методология аналитических и системных исследований в задачах надёжности и безопасности
- Системные исследования управления и принятия решений. Стратегическое и оперативное управление.
- Сбор, обработка данных и прогнозирование. Статистика, теория вероятностей, комбинаторика, методы измерения и моделирования в системно-аналитических исследованиях
- Информационное обеспечение системного анализа, систем управления и принятия решений

ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ

- Назначение и структура современных ИТС Информационные и коммуникационные технологии и решения, востребованные при создании и эксплуатации ИТС
- Использование и развитие мирового опыта при создании российских ИТС.
- Роль и место систем безопасности в ИТС
- Нейронные системы и искусственный интеллект в ИТС
- Достоверные данные и система обнаружения
- Повышение безопасности с помощью видеоаналитики

ТЕРМИНОЛОГИЯ НАДЁЖНОСТИ, ОТКАЗОУСТОЙЧИВОСТИ, БЕЗОПАСНОСТИ, РИСКОВ И ЖИВУЧЕСТИ

- Методологические и методические вопросы исследования терминологии надёжности, отказоустойчивости, безопасности, рисков и живучести
- Современный понятийный аппарат в области надёжности, отказоустойчивости, безопасности, рисков и живучести
- Проблема согласования и стандартизации терминологии в области надёжности, отказоустойчивости, безопасности, рисков и живучести, принятой в России, с используемой в международной практике
- Вопросы стандартизации терминологии в области надёжности, отказоустойчивости, безопасности, рисков и живучести

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

Надежность
Префикс DOI: 10.21683
ISSN 1729-2646
e-ISSN 2500-3909

УЧРЕДИТЕЛЬ ЖУРНАЛА:
ООО «Журнал «Надежность»

Зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Регистрационное свидетельство ПИ № ФС77-46055 от 05 августа 2011 года.

Официальный печатный орган Российской академии надежности

Отпечатано в ООО «Отмара. нет». 107140, г. Москва, ул. Русаковская, д. 13, стр. 5, 2 этаж, пом. III/6-7

Издатель журнала
ООО «Журнал «Надежность»

Генеральный директор
Саламатин Д.А.

Адрес: 109029, г. Москва, ул. Нижегородская, д. 27, стр. 1
ООО «Журнал «Надежность»
www.dependability.ru
телефон редакции 8 (495) 967-77-05,
e-mail: dependability@bk.ru

Подписано в печать 11.11.2025
Объем 88, Тираж 500 экз, Заказ № 19620
Формат 60x90/8, Бумага глянец

Журнал издается ежеквартально с 2001 года.
Стоимость* подписки на бумажную версию* (без стоимости доставки) на 2026 год:
– на год (4 выпуска) – 6 600 руб.;
– на полугодие (2 выпуска) – 3 300 руб.;
– цена одного номера – 1 650 руб.
* Указана стоимость с учетом НДС по ставке 10%
Статьи рецензируются.
Статьи опубликованы в авторской редакции.

ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ И ПРОЕКТНО-КОНСТРУКТОРСКИЙ ИНСТИТУТ ИНФОРМАТИЗАЦИИ, АВТОМАТИЗАЦИИ И СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ» (АО «НИИАС»)

Журнал разносторонне освещает проблемы надёжности, отказоустойчивости, безопасности, рисков, живучести, интеллектуального управления транспортом и активами.

Рубрики журнала

- Структурная надежность
- Функциональная надежность
- Функциональная безопасность систем
- Отказоустойчивость систем
- Управление рисками
- Сертификация и стандартизация
- Инновационные технологии в области надежности и безопасности
- Техническая эффективность систем управления
- Управление техническими активами
- Обработка больших данных. Системы управления и искусственный интеллект
- Методы и системы защиты информации
- Системный анализ в задачах надежности и безопасности
- Интеллектуальные транспортные системы
- Терминологические вопросы надёжности, отказоустойчивости, безопасности, рисков и живучести
- Сообщения

Рецензируемый научно-практический журнал «Надёжность» включен в перечень ведущих рецензируемых научных журналов, рекомендуемых Высшей аттестационной комиссией России для опубликования основных научных результатов диссертаций на соискание учёной степени кандидата и доктора наук по следующим специальностям и соответствующим им отраслям науки:

1.2. **Компьютерные науки и информатика** (1.2.1. Искусственный интеллект и машинное обучение (физико-математические науки), 1.2.2. Математическое моделирование, численные методы и комплексы программ (физико-математические, технические науки))

2.3. **Информационные технологии и телекоммуникации** (2.3.1. Системный анализ, управление и обработка информации, статистика (технические науки), 2.3.3. Автоматизация и управление технологическими процессами и производствами (технические науки), 2.3.4. Управление в организационных системах (технические науки), 2.3.5. Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (технические науки), 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки))

2.9. **Транспортные системы** (2.9.1. Транспортные и транспортно-технологические системы страны, ее регионов и городов, организация производства на транспорте (технические науки), 2.9.4. Управление процессами перевозок (технические науки), 2.9.8. Интеллектуальные транспортные системы (технические науки))

Журнал «Надежность» входит в категорию К2 перечня рецензируемых научных изданий ВАК, принятого в соответствии с рекомендацией Высшей аттестационной комиссии при Минобрнауки России от 21 декабря 2023 № 3-пл/1 «О категорировании перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук»

СОДЕРЖАНИЕ

УДК 528.088.3
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-3-16

Требования к точности и достоверности в вероятностных моделях

Accuracy and precision requirements in probability models[1]

Зиновий Круглый[1]*
Zinovi Krougly[1]*

[1] *Факультет Прикладной Математики, Западный Университет, Лондон, Онтарио, Канада*
[1] *Department of Applied Mathematics, Western University, London, Ontario, Canada N6A5B7*
* *e-mail: zkrougly@uwo.ca*

Зиновий Круглый

Резюме. *Численное преобразование Лапласа и его обратное преобразование – сложная задача в теории массового обслуживания и других вероятностных моделях. Для нахождения стабильных и вычислительно эффективных методов используется подход двойного преобразования. Для проверки и улучшения полученного инверсионного решения выполняются прямые преобразования Лапласа от численно инвертированных преобразований с последующим сравнением с исходной функцией. Наиболее перспективные методы были применены к вычислительным вероятностным моделям, когда не существует аналитических решений для обратного преобразования Лапласа. Вычислительная эффективность, обеспечиваемая в зависимости от заданного уровня точности, продемонстрирована для различных моделей M/G/1 систем массового обслуживания.*

Abstract. *Numerical Laplace transform and inverse Laplace transform is a challenging task in queueing theory and others probability models. A double transformation approach is used to find stable, accurate, and computationally efficient methods for performing the numerical Laplace and inverse Laplace transform. To validate and improve the inversion solution obtained, direct Laplace transforms are taken of the numerically inverted transforms to compare with the original function. Algorithms provide increasing accuracy as precision level increases. The most promising methods were applied to computational probability models, when there are no closed-form solutions of the Laplace transform inversion. The computational efficiency compared to precision levels is demonstrated for different service models in M/G/1 queuing systems.*

Ключевые слова: *численное прямое и обратное преобразование Лапласа, высокоточные вычисления, точность и достоверность в вероятностных моделях*
Keywords: *numerical Laplace transform, numerical Laplace transform inversion, high precision computation, applications in probability models*

Для цитирования: *Круглый З. Требования к точности и достоверности в вероятностных моделях // Надежность. 2025. №4. С. 3-16. https://doi.org/10.21683/1729-2646-2025-25-4-3-16*
For citation: *Krougly Z. Accuracy and precision requirements in probability models. Dependability 2025;4: 3-16. https://doi.org/10.21683/1729-2646-2025-25-4-3-16*

Поступила: *25.05.2024* / **После доработки:** *11.06.2025* / **К печати:** *28.09.2025*
Received on: *25.05.2024* / **Revised on:** *11.06.2025* / **For printing:** *28.09.2025*

Введение

Численное инвертирование преобразования Лапласа для получения различных показателей эффективности расчетов является важным приемом в теории массового обслуживания и смежных стохастических моделях [1], [6], [16]. Методы преобразования Лапласа могут упростить задачу решения систем дифференциальных уравнений [5] и могут быть рассмотрены с точки зрения типичных приложений [4], [8]. Инвертирование преобразования Лапласа широко используется в различных прикладных областях, включая анализ производительности в теории массового обслуживания и соответствующих вероятностных моделях [1], [6], [16]. Для численного инвертирования преобразований Лапласа разработано несколько алгоритмов, см., например, обзоры [4] и [13].

Алгоритм Гавера-Стефеста [18] является одним из наиболее эффективных методов для решения этой задачи. Сходимость данного алгоритма была исследована в работе [14]. К сожалению, несмотря на теоретические преимущества, в ряде практических приложений численная аппроксимация часто сталкивается с проблемами точности [1], [9], [11], [12], [13], [15]. Небольшие ошибки округления при вычислениях в стандартной двойной арифметике могут значительно искажать результаты, делая эти алгоритмы практически непригодными для применения.

[1] Ре-публикация статьи Zinovi Krougly. "Accuracy and Precision Requirements in Probability Models" Reliability: Theory & Applications, vol. 16, no. 1 (61), 2021, pp. 133-151. doi:10.24412/1932-2321-2021-161-133-151

Числа с двойной точностью, представленные в формате с плавающей запятой, обеспечивают точность вычислений до 15-17 значащих десятичных цифр (в среднем 16,3) в диапазоне от 10^{-308} до 10^{308}. При использовании расширенной точности можно добавить дополнительные значащие цифры и получать результаты, более точно сходящиеся к решению. Для численной реализации преобразования Лапласа и его инверсий мы использовали библиотеки численных классов C++ и MATLAB [10], [12], а также применили пакет ARPREC [3].

В работе [9] представлен подход двойного преобразования, включающий вычислительно эффективные методы для обратного преобразования Лапласа. Рассмотрены сложные численные примеры с периодическими и осциллирующими функциями. Было установлено, что количество членов разложения и выбранный уровень точности должны находиться в гармоничном балансе, чтобы получить корректные и стабильные результаты. В данной работе мы исследуем стабильность и точность инверсии преобразования Лапласа с использованием алгоритма Гавера-Стефеста [18]. Численные результаты были первоначально сопоставлены с известными аналитическими решениями. Затем наиболее интересные методы были применены к вероятностным моделям, для которых необходимо численное обратное преобразование Лапласа.

Для численного прямого преобразования Лапласа было реализовано составное правило Симпсона [9]. Численные примеры иллюстрируют вычислительную точность и стабильность прямого преобразования Лапласа и его инверсии благодаря увеличению уровня точности (N) и количества членов (L), включенных в разложение.

Остальная часть статьи организована следующим образом. Для обозначения преобразуемой функции мы используем строчные буквы $f(t)$, и заглавную букву $C(s)$ для обозначения ее преобразования Лапласа, например $\mathcal{L}\{f(t)\} = C(s)$. Если аналитическая форма инверсии $C(s)$ неизвестна, мы сравниваем исходное $C(s)$ и численное решение $\tilde{\tilde{C}}(s)$ после двойного преобразования. Результаты иллюстрируются графиками и оценками погрешностей.

В разделе 1 дается краткое описание основной теории и ее обозначений. В разделе 2 представлено численное вычисление прямого преобразования Лапласа с использованием составного правила Симпсона. В разделе 3 представлена методика численного двойного преобразования Лапласа. В разделах 4, 5 и 6 рассмотрены проблемные примеры и роль высокоточной арифметики при применении к вероятностным моделям. В разделах 7, 8, и 9 приведены численные преобразования Лапласа и их инверсии, в частности, для применения в моделях $M/D/1$ и $M/G/1$. Мы исследуем устойчивость и точность инверсии преобразования Лапласа, а также влияние числа членов разложения и уровня точности на численное приближение. Мы обсуждаем методику двойного преобразования для проверки результатов численной инверсии. В разделе 10 демонстрируется методика двойного преобразования и требования к точности для аппроксимации распределения времени ожидания в модели $M/D/1$.

1. Численные преобразования Лапласа и их инверсии

Пусть $f(t)$ – функция, определенная для $t \geq 0$. Тогда интеграл

$$\mathcal{L}\{f(t)\} = \int_0^\infty e^{-st} f(t)\, dt \qquad (1)$$

считается преобразованием Лапласа от $f(t)$ при условии, что интеграл сходится. Символ $\mathcal{L}$ – это оператор преобразования Лапласа, который действует на функцию $f(t)$ и порождает новую функцию $C(s) = \mathcal{L}\{f(t)\}$.

Если $C(s)$ представляет собой преобразование Лапласа функции $f(t)$, то есть $\mathcal{L}\{f(t)\} = C(s)$, то $f(t)$ является обратным преобразованием Лапласа для $C(s)$ и $f(t) = \mathcal{L}^{-1}\{C(s)\}$. Обратное преобразование Лапласа $\mathcal{L}^{-1}\{C(s)\}$ однозначно определено в том смысле, что если $C(s)=G(s)$ и $f(t)$ и $g(t)$ непрерывные функции, то $f(t)=g(t)$.

Преобразование Лапласа может быть инвертировано алгебраически или численно. Условное обозначение $\tilde{f}(t)$ используется для численной аррроксимации $f(t)$ (численная инверсия преобразования Лапласа $C(s)$), $\tilde{C}(s)$ используется для численного преобразования Лапласа $f(t)$.

Если t случайная величина с функцией плотности распределения вероятности $f(t)$ и кумулятивной функцией распределения $F(t)$, то это дает

$$C(0) = \int_0^\infty e^{-st} dF(t) = \int_0^\infty e^{-st} f(t)\, dt = 1 \qquad (2)$$

2. Численное вычисление прямого преобразования Лапласа

Для проверки и улучшения решения инверсии, полученного с помощью алгоритма Гавера-Стефеста, используется численное прямое преобразование Лапласа для этой инверсии, которое сравнивается с исходным преобразованием Лапласа. Чтобы обеспечить высокую точность аппроксимации, численное прямое преобразование Лапласа реализуется [9] с помощью составного правила Симпсона [2]. Для обеспечения высокой точности мы использовали расчет по составному правилу Симпсона с большим количеством подинтервалов.

Преобразование Лапласа функции $f(t)$ определяется выражением (1) на интервале $[0,\infty]$. Проблему с бесконечным верхним пределом интегрирования можно устранить, применив подстановку $t=-\ln(u)$, $dt=u^{-1}du$, которая заменяет бесконечные пределы на конечные.

Когда $t = 0$, $u = 1$ и когда $t\to\infty$, $u\to 0$, тогда

$$\int_0^\infty e^{-st} f(t)\, dt = \int_0^1 e^{\ln(u^s)} f(-\ln(u)) u^{-1} du = \int_0^1 u^{s-1} f(-\ln(u))\, du. \qquad (3)$$

Поведение преобразуемой функции должно быть рассмотрено в новых пределах, а экспоненциальная функция внутри интеграла требует особого изучения с точки зрения высокой точности.

2.1. Вычисление прямого преобразования Лапласа с помощью составного правила Симпсона

Для интегрирования по интервалу $[a,b]$ выбирается четное n таким образом, чтобы функция была достаточно гладкой на каждом подинтервале $[x_j, x_{j+1}]$, где $x_j=a+jh$ для всех $j\in\{0,1,2,\ldots,n\}$ с $h=(b-a)/n$. В частности, $x_0=a$ и $x_n=b$. Тогда составное правило Симпсона имеет вид [2]:

$$\int_a^b f(x)dx \approx \frac{h}{3}\left[f(x_0)+2\sum_{j=1}^{n/2-1} f(x_{2j})+4\sum_{j=1}^{n/2} f(x_{2j-1})+f(x_n)\right] \quad (4)$$

Применяя это к преобразованному интегралу из уравнения (3), получаем $u_j=jh$ для всех $j\in\{0,1,2,\ldots,n\}$ с $h=1/n$. Следовательно,

$$C(s)\approx\frac{1}{3n}\left[\begin{array}{l} 0^{s-1}f\left(-ln(0)\right)+2\sum_{j=1}^{n/2-1}u_{2j}^{s-1}f\left(-ln\left(u_{2j}\right)\right)+ \\ 4\sum_{j=1}^{n/2}u_{2j-1}^{s-1}f\left(-ln\left(u_{2j-1}\right)\right)+1^{s-1}f\left(-ln(1)\right)\end{array}\right]. \quad (5)$$

Основная формула правила Симпсона делит интервал интегрирования $[a,b]$ на две части. Чтобы применить составное правило Симпсона, интервал $[a,b]$ должен быть разбит на четное число подинтервалов $n=2m$. Тогда

$$h=\frac{b-a}{n}=\frac{b-a}{2m}.$$

3. Численный метод двойного преобразования Лапласа

Мы определяем следующую технику двойного преобразования для инверсии преобразования Лапласа [9]:

$$\tilde{\tilde{C}}(s)=\mathcal{L}\left\{\mathcal{L}^{-1}\left\{C(s)\right\}\right\} \quad (6)$$

Это определение будет использоваться для оценки точности инверсии преобразования Лапласа, когда его аналитическое решение неизвестно.

После применения преобразования Лапласа задача переходит в область Лапласа и представляется как функция от s, а не от t.

Хотя вычисления в области Лапласа могут быть проще, оставлять решение в этой области, как правило, нецелесообразно. Для преобразования результата обратно во временную область применяются обратные преобразования Лапласа.

Когда аналитический ответ неизвестен, трудно оценить точность численного преобразования. Более того, трудно оценить, улучшает ли изменение метода или ухудшает точность инверсии. Используются следующие шаги:

1. Начинаем с доменной функции Лапласа $C(s)$;

2. Вычисляется численная инверсия с использованием заданного набора параметров. В этом случае мы будем контролировать уровень точности и количество членов аппроксимации. Установив уровень точности N_1, мы получим

$$\hat{f}_{N_1}(t)=\mathcal{L}_{N_1}^{-1}\left\{C(s)\right\}; \quad (7)$$

3. Используется численное преобразование Лапласа для $\hat{f}_{N_1}(t)$, в результате чего

$$\mathcal{L}\left\{\hat{f}_{N_1}(t)\right\}=\tilde{\tilde{C}}_{N_1}(s); \quad (8)$$

4. Сравниваются функции $C(s)$ и $\tilde{\tilde{C}}_{N_1}(s)$ и определяется функция ошибки:

$$\varepsilon_{N_1}(s)=\left|C(s)-\tilde{\tilde{C}}_{N_1}(s)\right|; \quad (9)$$

5. Повторяется процесс с другим уровнем точности N_2;

6. Сравниваются $\varepsilon_{N_1}(s)$ и $\varepsilon_{N_2}(s)$. Уровень точности, обеспечивающий меньшие погрешности, является более высоким, а разница между функциями погрешности может дать количественную оценку улучшения точности результата при увеличении уровня точности и добавлении дополнительных значащих цифр.

Для проверки и улучшения решения инверсии, полученного с помощью алгоритма Гавера-Стефеста, используется численное прямое преобразование Лапласа, которое сравнивается с исходным преобразованием. Численное прямое преобразование Лапласа реализуется в работе [9] с использованием составного правила Симпсона. [2]. Для обеспечения высокой точности мы использовали вычисления с увеличенным количеством подинтервалов.

4. Тестирование алгоритмов численной инверсии с произвольной точностью

В данной демонстрации применяются обратные преобразования Лапласа тестовых функций (табл. 1) для различных уровней численной точности. Дано $C(s)$, требуется найти $f(t)$, чтобы выполнялись следующие условия:

$$C(s)=\int_0^\infty e^{-st}f(t)dt. \quad (10)$$

Пример 1. Найти $\tilde{f}_{01}=\mathcal{L}^{-1}\left\{C_{01}(s)\right\}$, где

$$C_{01}(s)=1/(1+s/\beta)^\alpha \quad (\beta>0 \text{ и } \alpha>0). \quad (11)$$

Соответственно

$$f_{01}(t)=\beta^\alpha\Gamma(\alpha)t^{\alpha-1}e^{-t\beta}, \quad (12)$$

где $\Gamma(\alpha)$ – Гамма-функция.

Благодаря расширенной точности вычислений мы достигли более высокой точности численного инвертирования функции $C_{01}(s)=1/(1+s/\beta)^\alpha$. Точная инверсия имеет вид $f_{01}(t)=\beta^\alpha\Gamma(\alpha)t^{\alpha-1}e^{-t\beta}$.

Табл. 1. Преобразования Лапласа и обратные преобразования для тестовых функций, используемых в численных расчетах

№	$C(s)$	$f(t)$	Тип функции	Алгоритм преобразования
1.	$\frac{1}{(1+s/\beta)^{\alpha}}$	$\frac{\beta^{\alpha}}{\Gamma(\alpha)}t^{\alpha-1}e^{-t\beta}$	Гамма распределение	$\mathcal{L}^{-1}\{C(s)\}, \mathcal{L}\{\mathcal{L}^{-1}\{C(s)\}\}$
2.	$\frac{1}{\Gamma(\alpha)}\int_0^s t^{\alpha-1}e^{-t}dt$	Аналитическое решение неизвестно	Неполная Гамма-функция	$\mathcal{L}^{-1}\{C(s)\}, \mathcal{L}\{\mathcal{L}^{-1}\{C(s)\}\}$
3.	$\exp\left(-as^{\alpha}\right)$	$\delta(t-a)$, если $a=1$	Сдвинутая дельта функция Дирака	$\mathcal{L}^{-1}\{C(s)\}, \mathcal{L}\{\mathcal{L}^{-1}\{C(s)\}\}$
4.	$\sum_{i=1}^{2}\frac{p_i\mu_i}{\mu_i+s}$	$\sum_{i=1}^{2}p_i\mu_i e^{-\mu_i t}$	Гиперэкспоненциальное распределение	$\mathcal{L}^{-1}\{C(s)\}, \mathcal{L}\{\mathcal{L}^{-1}\{C(s)\}\}$
5.	$\frac{(1-\rho)s}{s-\lambda\left[1-B^{*}(s)\right]}$	Аналитическое решение неизвестно	$W_q(t)$ в $M/G/1$ модели	$\mathcal{L}^{-1}\{C(s)\}, \mathcal{L}\{\mathcal{L}^{-1}\{C(s)\}\}$

Результаты, представленные на рис. 1, соответствуют параметрам $\beta = 1$ и $\alpha = 20$, и иллюстрируют недостаточную точность приближения для уровня двойной точности ($N = 16$). Численная инверсия также оценивалась с учетом расширенной точности и числа членов разложения, $(N,L) = (32, 32)$.

На рис. 2 представлены два скриншота для той же функции, что и на рис. 1. Мы наблюдаем значительное улучшение результата при увеличении точности до 256 знаков, с ошибкой порядка 10^{-73}.

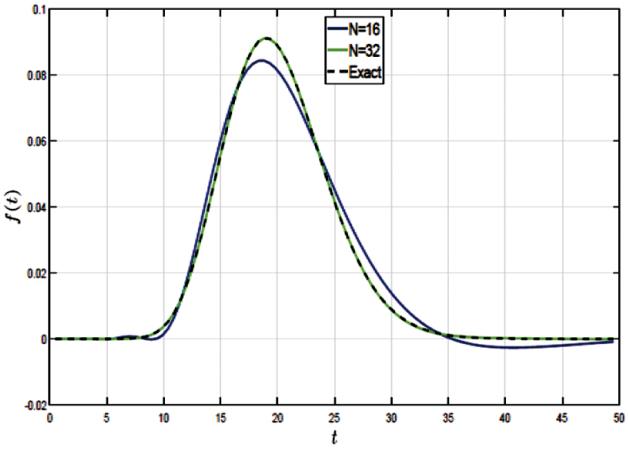


Рис. 1. Обратное преобразование Лапласа функции $C_{01}(s)=1/(1+s/\beta)^{\alpha}$ оценивается с двойной и повышенной точностью. Точное и численное решение с уровнем точности $N = 32$ визуально неразличимы

Существует множество примеров, когда не существует аналитического решения для обратного преобразования Лапласа. Для таких задач мы сравниваем численное решение $\tilde{C}(s)$ после применения техники двойного преобразования (6) с исходным преобразованием Лапласа $C(s)$.

Сначала мы проиллюстрируем метод двойного преобразования на рис. 3 для Гамма распределения с $\alpha = 1$ (экспоненциальное распределение) и $\alpha = 2{,}5$. Оба преобразования Лапласа и инвертирование работают очень

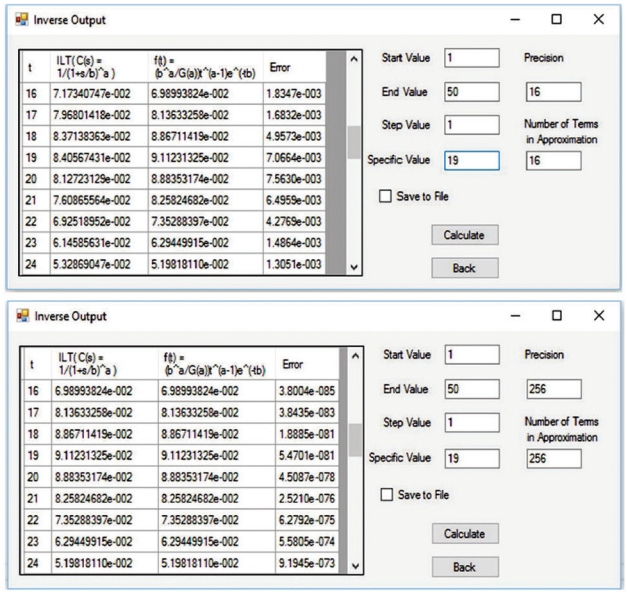


Рис. 2. Два скриншота для обратного преобразования Лапласа функции $C_{01}(s)=1/(1+s/\beta)^{\alpha}$ с двойной и повышенной точностью

хорошо. Ошибки E следующие: $2{,}5\times10^{-5}$ и $7{,}45\times10^{-4}$, соответствуют графикам в левой и правой частях.

5. Численное обратное преобразование Лапласа неполной Гамма функции

Следующий пример значительно отличается от предыдущего, поскольку мы не можем выразить обратное преобразование Лапласа аналитически. Нижняя неполная Гамма функция P и верхняя неполная Гамма функция Q определяются как

$$P(\alpha,x)=\frac{1}{\Gamma(\alpha)}\int_0^x t^{\alpha-1}e^{-t}dt, \qquad (13)$$

$$Q(\alpha,x)=\frac{1}{\Gamma(\alpha)}\int_x^{\infty} t^{\alpha-1}e^{-t}dt. \qquad (14)$$

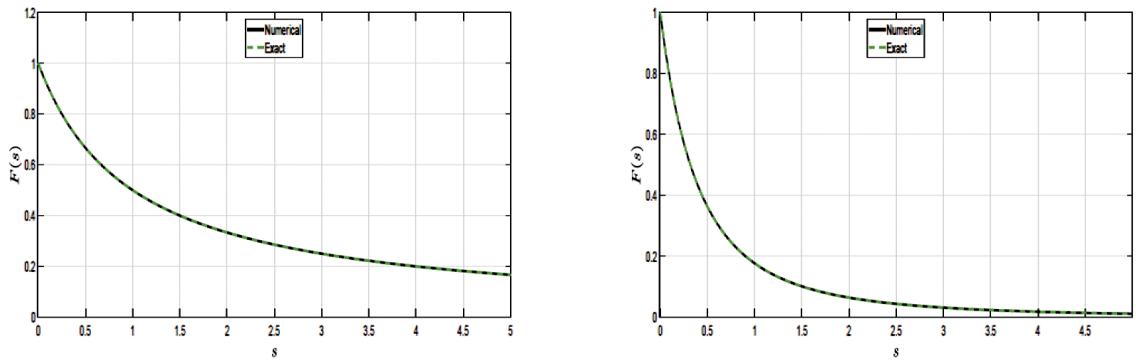


Рис. 3. Исходное преобразование Лапласа $C_{01}(s)=1/(1+s/\beta)^{\alpha}$; вычисляется его численная аппроксимация $\tilde{\tilde{C}}_{01}(s)=\mathcal{L}\{\mathcal{L}^{-1}\{1/(1+s/\beta)^{\alpha}\}\}$, оцененная для $\beta = 1{,}0$ при значениях $\alpha = 1{,}0$ (левый график) и $\alpha = 2{,}5$ (правый график). Исходное и численное решение визуально неразличимы

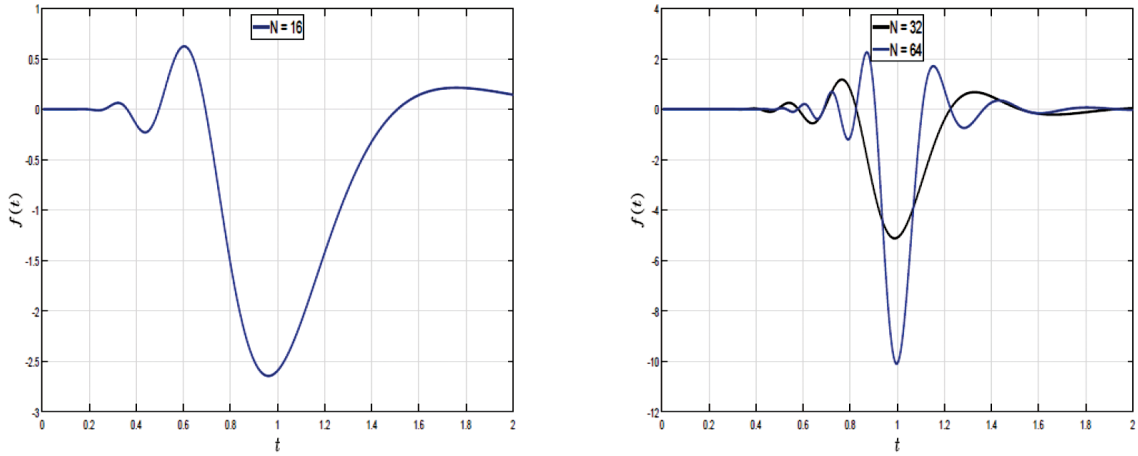


Рис. 4. Обратное преобразование Лапласа функции $C_{02}(s)=\frac{1}{\Gamma(\alpha)}\int_0^s t^{\alpha-1}e^{-t}dt$ с двойной точностью (левый график) и с точностью 32 и 64 знаков (правый график); важно отметить, что на графиках использованы разные масштабы

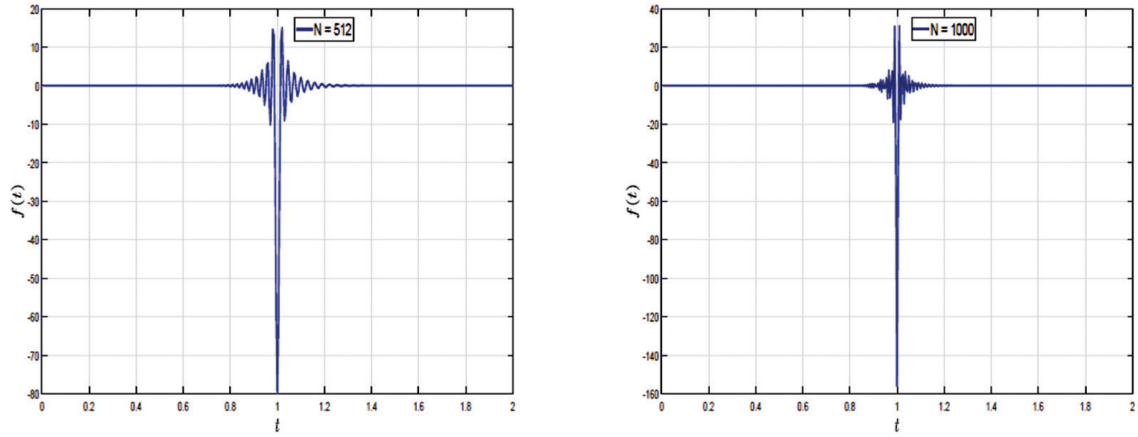


Рис. 5. Обратное преобразование Лапласа функции $C_{02}(s)=\frac{1}{\Gamma(\alpha)}\int_0^s t^{\alpha-1}e^{-t}dt$ на уровне точности 512 (левый график) и 1000 (правый график). Следует отметить, что на двух графиках используются разные масштабы

Мы использовали нормализованное определение неполной Гамма функции, где $P(\alpha,x)+Q(\alpha,x)=1$.

Пример 2. Определим $\tilde{f}_{02}(t)=\mathcal{L}^{-1}\{C_{02}(s)\}$ и $\tilde{C}_{02}(s)=\mathcal{L}\{\mathcal{L}^{-1}\{C_{02}(s)\}\}$, где

$$C_{02}(s)=P(\alpha,s)=\frac{1}{\Gamma(\alpha)}\int_0^s t^{\alpha-1}e^{-t}dt. \qquad (15)$$

Мы получили аппроксимацию (рис. 4) для инвертирования функции (15) с параметром $\alpha = 1{,}0$.

Точное решение обратного преобразования Лапласа имеет вид $-\delta(t-1)$, где $\delta(t)$ дельта функция Дирака (16).

Улучшения можно достичь при увеличении числа знаков N, начиная с двойной точности (рис. 4, левый график) и до точности 32 и 64 знаков (рис. 4, правый график).

Количество членов в аппроксимации соответствует уровню точности, $L=N$. Для более точной оценки используются уровни точности 500 и 1000, как показано на рис. 5.

Оригинал $C_{02}(s)$ сравнивается с численным решением $\tilde{\tilde{C}}_{02}(s)=\mathcal{L}\left\{\mathcal{L}^{-1}\left\{C_{02}(s)\right\}\right\}$, полученным после двойного преобразования. Таким образом, $\tilde{f}_{02}(t)$ вычисляется как численная инверсия $C_{02}(s)$. Затем преобразование Лапласа $\tilde{\tilde{C}}_{02}(s)$ от $\tilde{f}_{02}(t)$ сравнивается с исходной функцией $C_{02}(s)$. Исходное преобразование Лапласа $C_{02}(s)$ (Exact) и численная аппроксимация (Numerical) этого двойного преобразования показаны на рис. 6. Использованы следующие параметры: α = 0,5; 1; 3 и 5.

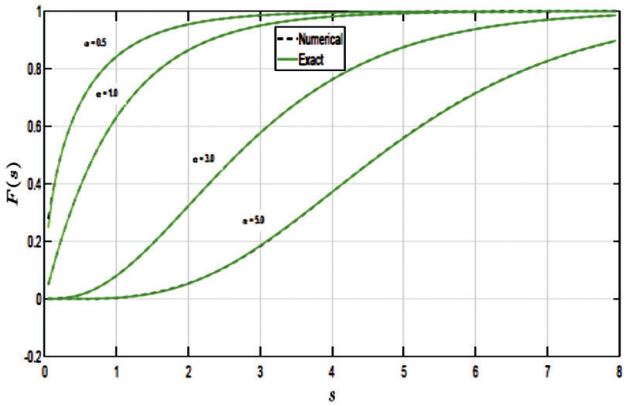


Рис. 6. Неполная Гамма функция $C_{02}(s)=\dfrac{1}{\Gamma(\alpha)}\int_0^s t^{\alpha-1}e^{-t}dt$; вычисляется ее численная аппроксимация $\tilde{\tilde{C}}_{02}(s)=\mathcal{L}\left\{\mathcal{L}^{-1}\left\{\dfrac{1}{\Gamma(\alpha)}\int_0^s t^{\alpha-1}e^{-t}dt\right\}\right\}$ для значений α = 0,5; 1; 3 и 5.

6. Аппроксимация дельта функции Дирака

Дельта функцию Дирака [5] можно условно представить как функцию на вещественной прямой, которая равна нулю везде, кроме начала координат, где она бесконечна,

$$\delta(t)=\begin{cases}+\infty, & t=0;\\ 0, & t\neq 0\end{cases} \tag{16}$$

и которая также ограничена, чтобы удовлетворять тождеству

$$\int_{-\infty}^{\infty}\delta(t)\,dt=1. \tag{17}$$

Это всего лишь эвристическая характеристика. Дельта Дирака не является функцией в традиционном смысле, поскольку ни одна функция, определенная на вещественных числах, не обладает такими свойствами. Эта функция может быть строго определена либо как распределение, либо как мера.

Отметим, что дельта функция Дирака может быть определена как предел (в смысле распределений) последовательности нуль-центрированных нормальных распределений

$$\delta_a(t)=\frac{1}{a\sqrt{\pi}}e^{-\frac{t^2}{a^2}},\qquad a\to 0. \tag{18}$$

Преобразование Лапласа дельта функции определяется как [5]

$$\int_0^{\infty}e^{-st}\delta(t-a)\,dt=e^{-as}, \tag{19}$$

что согласуется с определением преобразования Лапласа для $\delta(t-a)$ как e^{-as}.

Пример 3. Найти $\tilde{f}_{03}(t)=\mathcal{L}^{-1}\left\{C_{03}(s)\right\}$ и $\tilde{C}_{03}(s)=\mathcal{L}\left\{\mathcal{L}^{-1}\left\{C_{03}(s)\right\}\right\}$, где

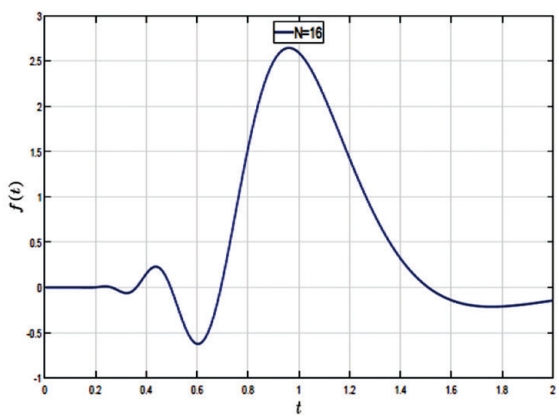
$$C_{03}(s)=\exp\left(-as^{\alpha}\right)\quad a>0 \text{ и } \alpha\in(0,1). \tag{20}$$

Выражение обратного преобразования Лапласа в терминах стандартных математических функций неизвестно. Мы можем работать с обратным преобразованием Лапласа и методом двойного преобразования, включая дельта функцию Дирака и ее сдвинутую форму.

Итак, если a=1, то $f(t)=\delta(t-a)$, где $\delta(t)$ дельта функция Дирака.

Пакет Математика дает численное значение обратного преобразования Лапласа для a=0,5 и α=0,5:

$$\mathcal{L}^{-1}\left\{\exp\left(-as^{\alpha}\right)\right\}=\frac{0.14104739588693907\exp(-0.0625/t)}{t^{3/2}}. \tag{21}$$



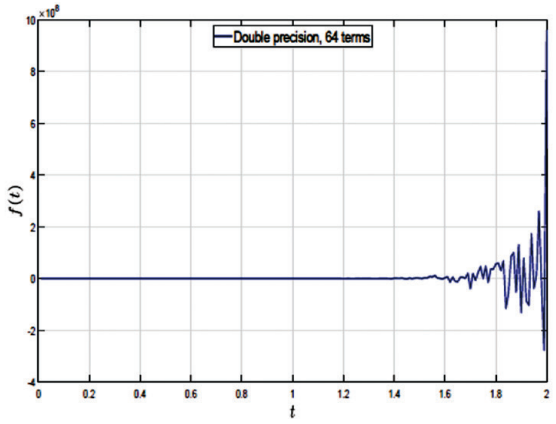


Рис. 7. Аппроксимация дельта функции Дирака с параметром a = 1, вычисленная с двойной точностью. Уровень точности N знаков и количество членов разложения L (16, 16) для левого графика и (16, 64) для правого графика.

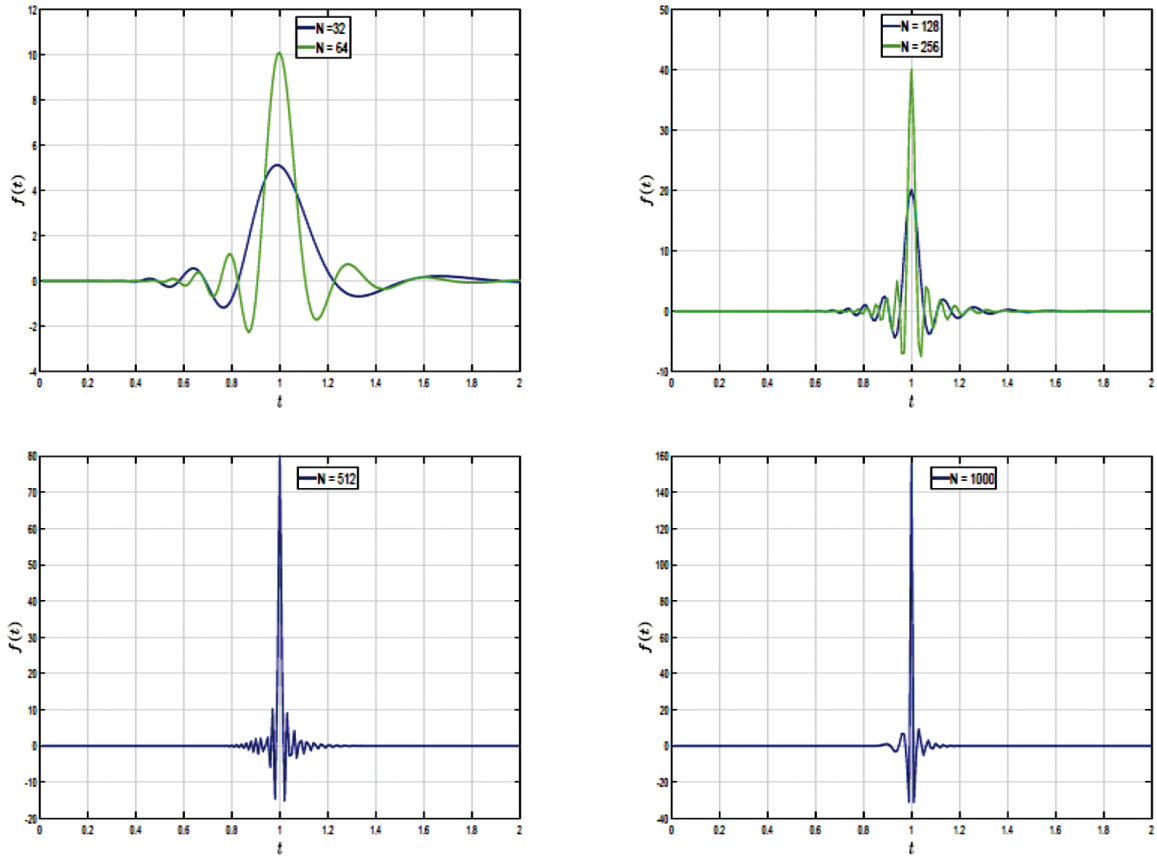


Рис. 8. Аппроксимация дельта функции Дирака, a = 1; уровень точности N и количество членов L равны, L=N: 32, 64, 128, 256, 512 и 1000; обратите внимание на различия в масштабах на четырех графиках

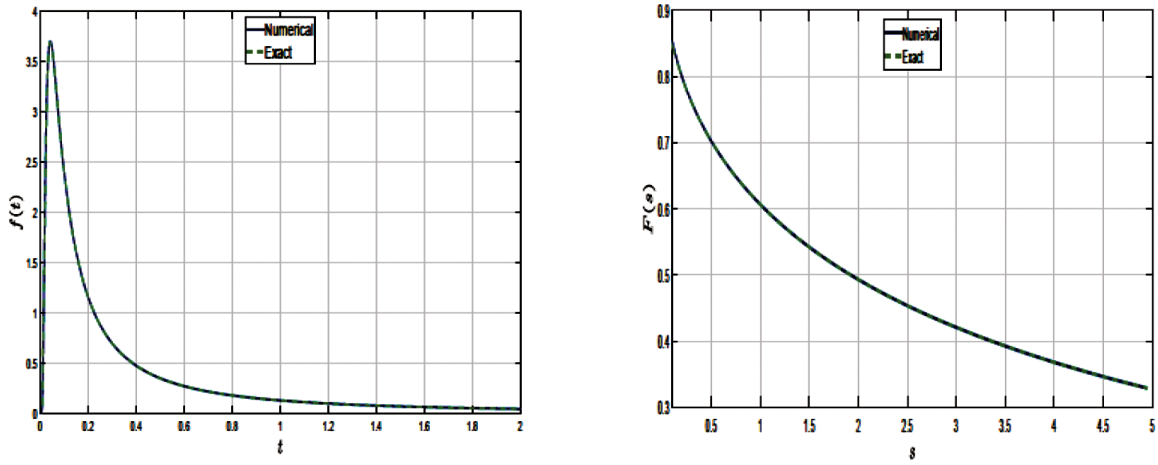


Рис. 9. Исходное преобразование Лапласа $C_{03}(s)$=exp(–as^{α}); вычисляется его обратное преобразование (левый график) и численная аппроксимация $\widetilde{C}_{03}(s) = \mathcal{L}\left\{\mathcal{L}^{-1}\left\{\exp\left(-as^{\alpha}\right)\right\}\right\}$ (правый график)

Численное инвертирование преобразования Лапласа $C_{03}(s)$=e^{-as}, как известно, эквивалентно аппроксимации дельта функции Дирака. На рис. 7 показана аппроксимация дельта функции Дирака с параметром a = 1, вычисленная с двойной точностью.

На левом графике используется одинаковое количество членов разложения и уровня точности, L=N. Эта аппроксимация принимает отрицательные значения, в то время как дельта-функция строго положительна. На правом графике N = 16 и L = 64. При рассмотрении численной инверсии важно обратить внимание на точность в зависимости от количества членов разложения и уровня точности. Мы сравниваем инверсии с помощью реализации Гавера-Стефеста и наблюдаем, как повышается точность инверсий при увеличении числа членов разложения и уровня точности (знаков). Однако существует ограничение на добавление дополнительных членов [12]. При увеличении числа членов разложения

до $L = 64$ мы обнаруживаем, что численная инверсия становится неустойчивой и в нашей функции преобладает численная ошибка (правый график).

Использование расширенной точности (рис. 8) позволяет преодолеть численные ограничения, которые возникают при работе с двойной точностью. Таким образом, мы можем использовать большее количество термов. В этих примерах используется одинаковое количество членов разложения и уровня точности, $L=N$. Для повышения точности аппроксимации мы увеличили число знаков N до 32, 64, 128, 512 и 1000.

На рис. 9 показаны обратное преобразование Лапласа (левый график) и численное двойное преобразование Лапласа (правый график) для $C_{03}(s)=\exp(-as^{\alpha})$, оцененные для $a = 0{,}5$ и $\alpha = 0{,}5$. Аналитическое решение обратного преобразования Лапласа, соответствующее (21), представлено на графике как точное. Аппроксимация дана с двойной точностью, а погрешности равны $E=6{,}6\times10^{-4}$ и $1{,}3\times10^{-2}$, соответственно для левого и правого графиков.

На рис. 10 представлен скриншот инверсии преобразования Лапласа для $C_{03}(s)=\exp(-as^{\alpha})$, оцененной для тех же a и α с уровнем точности 64. Отметим, что точность аппроксимации улучшилась, и погрешность составила порядка 10^{-18}.

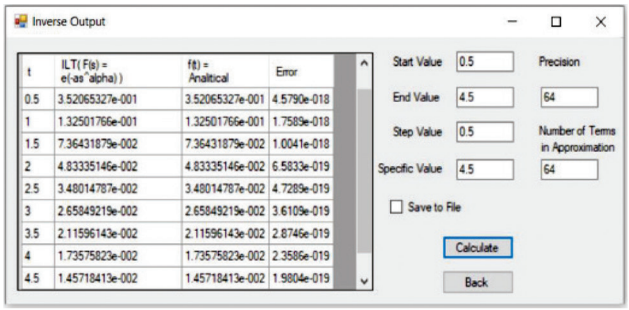


Рис. 10. Скриншот для обратного преобразования Лапласа функции $C_{03}=\exp(-as^{\alpha})$, оцененного для $a = 0{,}5$ и $\alpha = 0{,}5$, с уровнем точности 64 знака

В табл. 2 показана погрешность $\varepsilon_{03}(s)=\left|C_{03}(s)-\tilde{\tilde{C}}_{03}(s)\right|$ для численного приближения $\tilde{\tilde{C}}_{03}(s)=\mathcal{L}\{\mathcal{L}^{-1}\{\exp(-as^{\alpha})\}$, оцененная для $a = 0{,}5$ и $\alpha = 0{,}5$, при различных уровнях точности 16 и 64.

Табл. 2. Численная погрешность $\varepsilon_{03}(s)=\left|C_{03}(s)-\tilde{\tilde{C}}_{03}(s)\right|$ для численного приближения $\tilde{\tilde{C}}_{03}(s)=\mathcal{L}\{\mathcal{L}^{-1}\{\exp(-as^{\alpha})\}$, оцененная для $a = 0{,}5$ и $\alpha = 0{,}5$, при различных уровнях точности: 16 и 64 знаков.

s	Численное решение	Ошибка, $L = 16$	Ошибка, $L = 64$
0,5	0,7022	$9{,}23\times10^{-6}$	$2{,}76\times10^{-6}$
1	0,6065	$4{,}03\times10^{-7}$	$9{,}13\times10^{-10}$
2	0,4931	$6{,}81\times10^{-7}$	$3{,}51\times10^{-17}$
3	0,4206	$4{,}38\times10^{-7}$	$3{,}69\times10^{-23}$
4	0,3679	$7{,}82\times10^{-8}$	$1{,}97\times10^{-24}$
5	0,3269	$2{,}25\times10^{-7}$	$3{,}94\times10^{-25}$

7. Распределение времени ожидания в *M*/*G*/1

Модель $M/G/1$ предполагает пуассоновское поступление с интенсивностью λ и прозвольным распределением времени обслуживания $S = 1/\mu$, где μ – интенсивность обслуживания. Интенсивность трафика $\rho = \lambda/\mu = \lambda S < 1$.

Важно выполнение условия $\rho < 1$, иначе система становится нестабильной.

Коэффициент вариации времени обслуживания $c_s=\sigma/b$, где $b=E[S]$ – среднее время и σ – стандартное отклонение.

Если $c_S=1$, мы имеем модель $M/M/1$ с преобразованием Лапласа-Стилтьеса времени обслуживания

$$B^*(s) = \mu/(\mu + s).$$

Рассмотрим функцию плотности вероятности ФПВ (probability density function, PDF) и кумулятивную функцию распределения КФР (cumulative distribution function, CDF).

Для модели $M/M/1$, ФПВ и КФР времени ожидания определяются соответственно [17]:

$$w_q(t) = \mu(1-\rho)e^{-\mu(1-\rho)t}, \quad t > 0, \text{ ФПВ, } M/M/1, \qquad (22)$$

$$W_q(t) = 1-\rho e^{-\mu(1-\rho)t}, t \ge 0, \text{ КФР, } M/M/1. \qquad (23)$$

Если коэффициент $c_S>1$, то время ожидания можно эффективно аппроксимировать гиперэкспоненциальным распределением, используя для него определение по параллельным стадиям.

Пусть время обслуживания S соответствует гиперэкспоненциальному распределению H_2, ФПВ которого определяется выражением (33), а КФР задается формулой (34).

Преобразование Лапласа для ФПВ представлено в уравнении (32), что позволяет получить преобразование Лапласа для КФР как

$$F(s) = C(s)/s = \frac{1}{s}\sum_{i=1}^{2}\frac{p_i\mu_i}{\mu_i + s}. \qquad (24)$$

Первая и вторая производные от $C(s)$ вычисляются следующим образом:

$$\frac{dC(s)}{ds} = -\sum_{i=1}^{2}\frac{p_i\mu_i}{(\mu_i + s)^2}, \qquad (25)$$

$$\frac{d^2C(s)}{ds^2} = 2\sum_{i=1}^{2}\frac{p_i\mu_i}{(\mu_i + s)^3}. \qquad (26)$$

Математическое ожидание $E[S] = -\frac{dC(s)}{ds}|_{s=0}$ и дисперсия $Var[S]=E[S^2]-(E[S])^2$ случайной переменной S следующие:

$$E[S] = \frac{p_1}{\mu_1} + \frac{p_2}{\mu_2}, \qquad (27)$$

$$Var[S]=\frac{p_1(2-p_1)}{\mu_1^2}+\frac{p_2(2-p_2)}{\mu_2^2}-\frac{2p_1p_2}{\mu_1\mu_2}, \quad (28)$$

$$E[S^2]=\frac{d^2C(s)}{ds^2}|_{s=0}=\frac{2p_1}{\mu_1^2}+\frac{2p_2}{\mu_2^2}. \quad (29)$$

Чтобы удовлетворить условие (27), пусть

$$\mu_1=2p_1E[S], \quad \mu_2=2p_2E[S]. \quad (30)$$

Подставляя (27), (29) и (30) в $c_S^2=\frac{(\sigma[S])^2}{(E[S])^2}=\frac{E[S^2]-(E[S])^2}{(E[S])^2}$, получим параметры гиперэкспоненциального распределения [6]:

$$p_1=\frac{1}{2}\left(1+\sqrt{\frac{c_S^2-1}{c_S^2+1}}\right),\ p_2=1-p_1,\ \mu_1=\frac{2p_1}{E[S]},\ \mu_2=\frac{2p_2}{E[S]}. \quad (31)$$

8. Решение задач производительности в модели *M*/*G*/1.

Пример 4. Рассматриваются два варианта модели *M*/*G*/1.

Вариант 1. Приведено преобразование Лапласа для ФПВ распределения времени обслуживания.

Найти $\tilde{f}_{04}(t)=\mathcal{L}^{-1}\{C_{04}(s)\}$ и $\tilde{C}_{04}(s)=\mathcal{L}\{\mathcal{L}^{-1}\{C_{04}(s)\}\}$, где

$$C_{04}(s)=\sum_{i=1}^{2}\frac{p_i\mu_i}{\mu_i+s},\ (0\le p_1\le 1,\ 0\le p_2\le 1,\ p_1+p_2=1), \quad (32)$$

$$f_{04}(t)=\sum_{i=1}^{2}p_i\mu_i e^{-\mu_i t}\ \ (t>0). \quad (33)$$

Вариант 2. Идентичен варианту 1, но теперь для КФР.

Найти $\tilde{F}_{04}(t)=\mathcal{L}^{-1}\{F_{04}(s)\}$ и $\tilde{F}_{04}(s)=\mathcal{L}\{\mathcal{L}^{-1}\{F_{04}(s)\}\}$, где

$$F_{04}(s)=C_{04}(s)/s=\frac{1}{s}\sum_{i=1}^{2}\frac{p_i\mu_i}{\mu_i+s}, \quad (34)$$

$$F_{04}(t)=1-\sum_{i=1}^{2}p_i e^{-\mu_i t}, \quad (t>0). \quad (35)$$

Таким образом, было рассмотрено несколько вариантов для модели *M*/*G*/1. Первый – преобразование Лапласа для ФПВ распределения времени обслуживания и второй, идентичный, для КФР. Модель *M*/*G*/1 описывается с помощью λ=0,8, матожидание *E*[*S*]=1,0, коэффициент вариации c_s = 1,5; 2,5 и 4,5.

На рис. 11 показано обратное преобразование Лапласа $C_{04}(s)$, оцененное для ФПВ (левый график), и обратное преобразование Лапласа $(C_{04}(s))/s$ оцененное для КФР (правый график). Погрешности составляют $E=3{,}52\times10^{-5}$ и $E=1{,}2\times10^{-5}$ соответственно.

9. Распределение времени ожидания в модели *M*/*D*/1

Пусть время обслуживания имеет плотность распределения E_k со средним 1/μ и ФПВ

$$f(t)=\frac{(\mu k)^k t^{k-1}e^{-k\mu t}}{(k-1)!}\quad (0<t<\infty). \quad (36)$$

Преобразование Лапласа-Стилтьеса

$$B^*(s)=\left(\frac{\mu k}{s+\mu k}\right)^k. \quad (37)$$

Плотность распределения E_k можно трактовать как распределение Эрланга с параметром *k*. Модель *M*/*D*/1 можно рассматривать как частный случай *M*/E_k/1 так как когда $k\to\infty$ и $\mu\to\infty$ таким образом, что $k\mu^{-1}\to b$ ($0<b<\infty$), время обслуживания E_k детерминировано с константой *b*. Интенсивность трафика $\lambda b<1$. Теперь $B^*\to e^{-bs}$ как

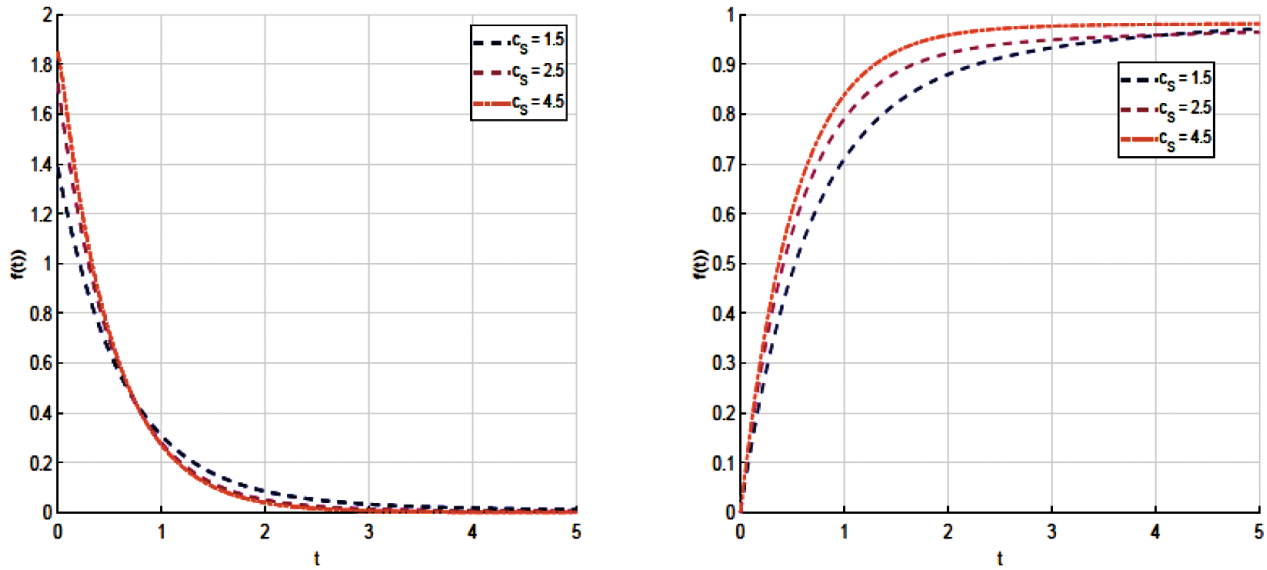


Рис. 11. Обратное преобразование Лапласа функции $C_{04}(s)$, оцененной для ФПВ (левый график), и $(C_{04}(s))/s$, оцененной для КФР (правый график); модель *M*/*G*/1 имеет λ=0,8, матожидание *E*[*S*]=1,0, коэффициенты вариации c_s = 1,5; 2,5 и 4,5.

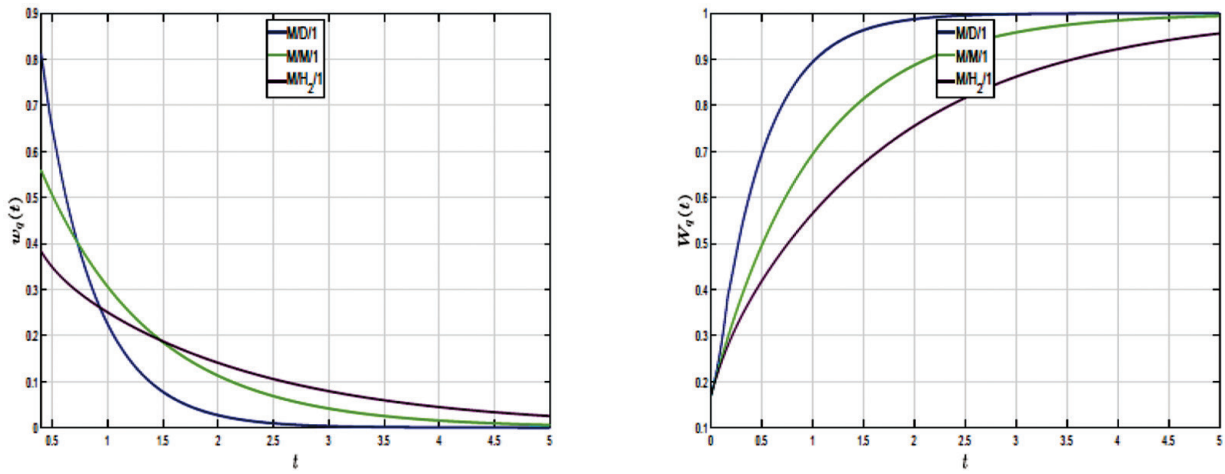


Рис. 12. ФПВ и КФР времени ожидания для $M/M/1$, $M/D/1$ и $M/H_2/1$

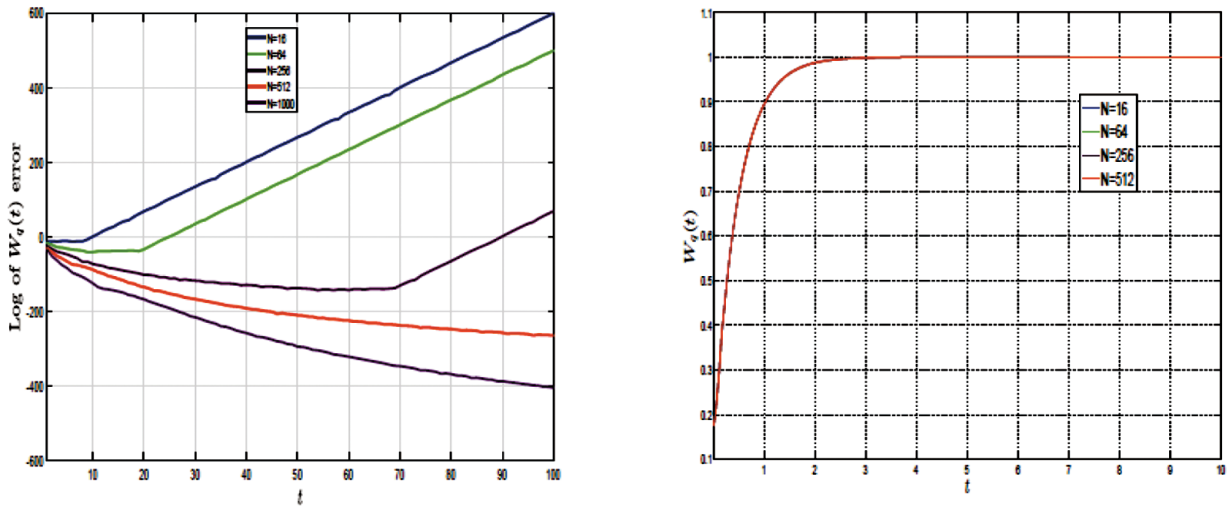


Рис. 13. $M/D/1$: ошибки Log $W_q(t)$ (левый график) и оценка для $W_q(t)$ по инверсии Гавера-Стефеста (правый график)

$k\to\infty$. ФПР времени ожидания имеет преобразование Лапласа [17]:

$$w_q(s)=\frac{(1-\rho)s}{s-\lambda\left[1-e^{-bs}\right]}. \qquad (38)$$

Пример 5. Численно оценить распределение времени ожидания $W_q(t)$ для различных моделей обслуживания в модели $M/G/1$.

Преобразование Лапласа для $W_q(t)$ задается уравнением преобразования Поллачека-Хинчина (P-X) [17]

$$W_q(s)=\frac{w_q(s)}{s}=\frac{(1-\rho)}{s-\lambda\left[1-B^*(s)\right]}, \text{ где} \qquad (39)$$

$$B^*(s)=\int_0^\infty dF(t)=\int_0^\infty e^{-st}f(t)\,dt. \qquad (40)$$

$B^*(s)$ – это преобразование Лапласа-Стилтьеса функции $F(t)$, где $F(t)$ является КФР времени обслуживания, λ и b – средние значения интенсивности прибытия и времени обслуживания соответсвенно, $\rho=\lambda b$ – интенсивность трафика.

Как и в случае с $M/G/1$, рассматриваются следующие модели обслуживания:

$$M/M/1: \quad B^*(s)=\frac{\mu}{s+\mu}, \qquad (41)$$

$$M/E_k/1: \quad B^*(s)=\left(\frac{\mu}{s+\mu}\right)^k, \qquad (42)$$

$$M/D/1: \quad B^*(s)=e^{-bs}, \qquad (43)$$

$$M/H_2/1: \quad B^*(s)=\sum_{i=1}^{2}\frac{p_i\mu_i}{\mu_i+s}. \qquad (44)$$

Для модели $M/H_2/1$ интенсивность поступления λ=5,0. Распределение времени обслуживания H_2 оценивается для μ=6, $b=1/\mu$ и c_s=1,5. Для этой модели интенсивность трафика $\rho=\lambda/\mu$, а КФР в момент времени 0 имеет вид $F(0)=1-\rho$. Алгоритм Гавера-Стефеста использован для инвертирования преобразования Лапласа для $B^*(s)$, которое определяется с помощью (39). Для моделей

$M/D/1$, $M/H_2/1$ и $M/M/1$, ФПВ и КФР времени ожидания показаны на рис. 12.

Для модели $M/D/1$ время обслуживания детерминировано и равно значению b. Для детерминированного обслуживания $B^*(s)$ определяется формулой (43). Мы сравниваем $W_q(t)$, вычисленное путем инвертирования в (39), с $W_q(t)$, аналитически полученным в [17]:

$$W_q(t) = (1-\rho)\sum_{i=0}^{[t/b]} e^{-\lambda(ib-t)}\frac{(ib-t)^i}{i!}\lambda^i, \qquad (45)$$

где $[x]$ – наибольшее целое число, меньшее или равное x.

На рис. 13 показаны результаты для модели $M/D/1$ при $\lambda = 5{,}0$, $\mu = 6{,}0$ ($b=1/\mu$ и $\rho=\lambda/\mu = 0{,}8$). На рисунке показаны ошибки, по аналитической оценке, в логарифмическом масштабе $\mathrm{Log}W_q(t)$ (левый график). Оценка для $W_q(t)$(правый график) получена с помощью алгоритма Гавера-Стефеста.

Нам не удалось получить численное решение для следующих уровней точности: $N = 16$, если $t>10$; $N = 64$, если $t>26$; $N = 256$, если $t>90$. Только для $N = 512$ и $N = 1000$ мы получаем правильный результат на всем диапазоне $0<t\le100$.

Инверсии $W_q(t)$ представлены на правом графике. Даже при использовании двойной точности мы получаем правильное решение и не можем визуально различить кривые с разной точностью для $N = 16$; 64; 256 и 512.

На рис. 14 для модели $M/D/1$ показаны численные результаты распределения времени ожидания $W_q(t)$ с двойной точностью ($N = 16$) по аналитическому решению (45) и по инверсии Гавера-Стефеста. В аналитическом решении доминируют шумы после $t>9$.

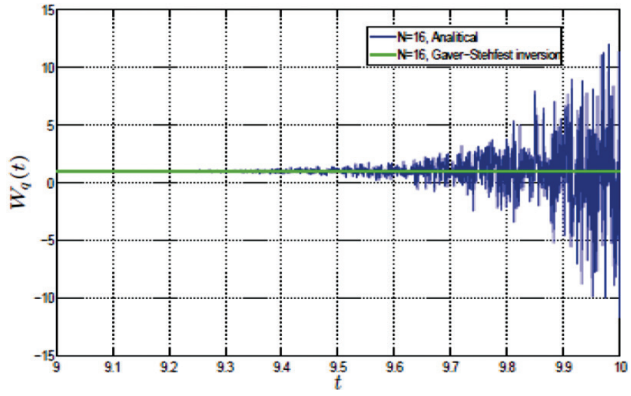


Рис. 14. $W_q(t)$ для модели $M/D/1$ КФР времени ожидания получена аналитически, а также с использованием инверсии Гавера-Стефеста. В аналитическом решении доминируют шумы после $t>9$.

Наиболее распространенным распределением времени обслуживания является экспоненциальное, и в этом случае распределение времени ожидания можно получить в аналитической форме. Для более общих случаев аналитические решения уравнения преобразования (P-X) для модели $M/G/1$ являются математически неразрешимыми.

Следующий конкретный пример используется для сравнения аналитического решения и инверсии Гавера-Стефеста. Рассмотрим систему $M/H_2/1$ с распределением времени обслуживания [7]

$$B(t) = \frac{1}{4}\lambda e^{-\lambda t} + \frac{3}{4}(2\lambda)e^{-2\lambda t}, \qquad (46)$$

где λ – интенсивность поступления, $b=5/(8\lambda)$ и $\rho=\lambda b=5/8$. Для численных решений мы использовали $\lambda=5$.

Соответствующее преобразование Лапласа

$$B^*(s) = \left(\frac{1}{4}\right)\frac{\lambda}{\lambda+s} + \left(\frac{3}{4}\right)\frac{2\lambda}{2\lambda+s}. \qquad (47)$$

Используя $B^*(s)$ и уравнение преобразования (P-X) (10.4), получим $W_q(s)$ и $W_q(t)$ для плотности времени ожидания [7]:

$$w_q^*(s) = (1-\rho)\left[1 + \frac{\lambda/4}{(3/2)\lambda+s} + \frac{3\lambda/4}{(1/2)\lambda+s}\right], \qquad (48)$$

$$w_q(t) = \frac{3}{8}u_0(t) + \frac{3\lambda}{32}e^{-(3/2)\lambda t} + \frac{9\lambda}{32}e^{-(1/2)\lambda t} \quad t\ge 0, \qquad (49)$$

где $u_0(t)$ – единичная импульсная функция.

Аналитическое решение для КФР времени ожидания может быть легко найдено как:

$$W_q^*(s) = (1-\rho)\left[\frac{1}{s} + \frac{\lambda/4}{((3/2)\lambda+s)s} + \frac{3\lambda/4}{((1/2)\lambda+s)s}\right], \qquad (50)$$

$$W_q(t) = (1-\rho)\left[\frac{8}{3} - \frac{1}{6}e^{-(3/2)\lambda t} - \frac{3}{2}e^{-(1/2)\lambda t}\right], \quad t\ge 0. \qquad (51)$$

На рис. 15 показаны численные результаты распределения времени ожидания для $M/H_2/1$ по аналитическому решению и инверсии Гавера-Стефеста для ФПВ (левый график) и КФР (правый график). Отличить визуально аналитические результаты от результатов инверсии Гавера-Стефеста практически невозможно.

10. Требования к точности и достоверности анализа $M/D/1$ с большим временем ожидания

Результаты аппроксимации двойного преобразования для распределения времени ожидания $W_q(s)$ в $M/D/1$ показаны на рис. 16 и 17. Для преобразования Лапласа при инверсии используется техника двойного преобразования

$$\tilde{\tilde{W}}_q(s) = \mathcal{L}\left\{\mathcal{L}^{-1}\left\{W_q(s)\right\}\right\}. \qquad (52)$$

Точное решение $W_q(s)$ сравнивается с $\tilde{\tilde{W}}_q(s)$ после применения метода двойного преобразования. Инверсия преобразования Лапласа реализована алгоритмом Гавера-Стефеста, а для численного прямого преобразования Лапласа используется составное правило Симпсона.

Аппроксимация для распределения времени ожидания в $M/G/1$ удобна при малой интенсивности потока и небольших значениях t, обеспечивая подходящую аппроксимацию с двойной точностью.

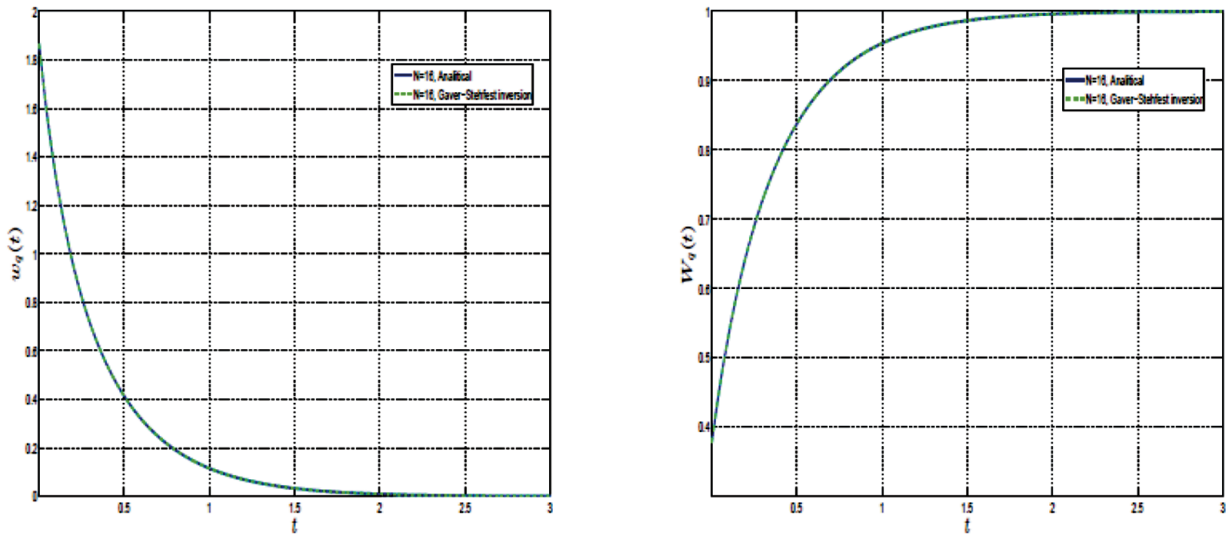


Рис. 15. Распределение времени ожидания для $M/H_2/1$ по аналитическому решению и инверсии Гавера-Стефеста для ФПВ (левый график) и КФР (правый график)

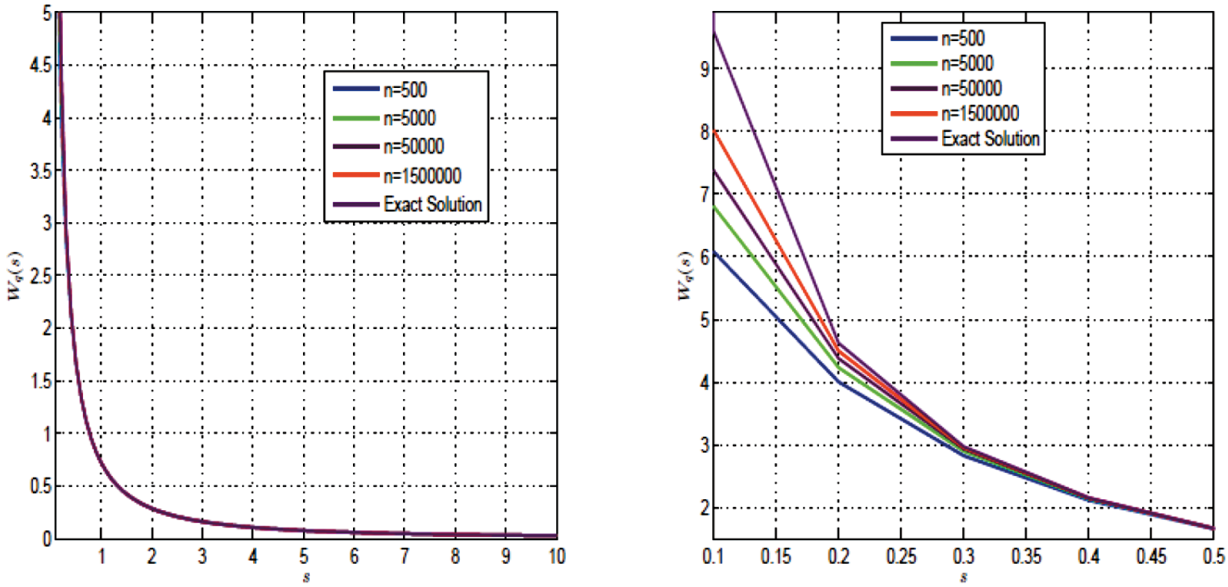


Рис. 16. Аппроксимация двойного преобразования для распределения времени ожидания $W_q(s)$ в $M/D/1$: двойная точность ($N = 16$) с различным количеством подинтервалов n = 500, 5000, 50000, 150000 и диапазонах [0,1; 10] (левый график) и [0,1; 5] (правый график)

Фигуры соответствуют широкому диапазону малых параметров преобразования Лапласа s, соответствующих большому значению t.

На рис. 16 приведены кривые для уровня двойной точности ($N = 16$) с различным количеством подинтервалов n = 500, 5000, 50000 и 150000 при вычислении преобразования Лапласа. Похоже, что для s отсутствует эффект от увеличения n на интервале [0,1; 10] (левый график), но кривые отличаются для s на меньшем интервале [0,1; 0,5] (правый график).

На рис. 17 показано влияние уровня точности N. Количество подинтервалов n = 500. При двойной точности метод работает плохо, а значительное улучшение наблюдается при увеличении уровня точности до 256.

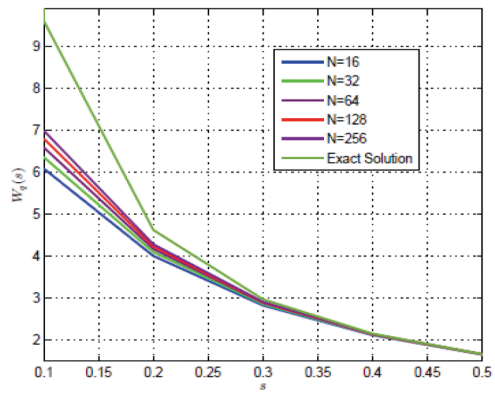


Рис. 17. Аппроксимация двойного преобразования для распределения времени ожидания $W_q(s)$ для $M/D/1$ с расширенной точностью вычислений, число подынтервалов n = 500

Выводы

Вычисления с произвольной точностью, также известные как расширенная точность или арифметика высокой точности, необходимы в различных областях, где стандартные вычисления с двойной точностью с плавающей запятой, которые обычно обеспечивают точность до 15-17 десятичных знаков, оказываются недостаточными.

Точность и стабильность численного преобразования Лапласа и его инверсии играют ключевую роль в ряде приложений вычислительных вероятностных моделей. В данной работе мы предложили и оценили различные численные методы реализации преобразования Лапласа и его инверсии в арифметических системах с повышенной точностью.

Рассматриваются два возможных способа выполнения преобразования. Если примеры включают функции с известными инверсиями, эффективность моделей с расширенной точностью может быть подтверждена сравнением с аналитическим решением. Наиболее реалистичные и сложные задачи включают функции с аналитически неизвестными инверсиями.

Таким образом, для поиска вычислительно эффективных методов численного преобразования Лапласа и его инверсии был предложен подход двойного преобразования. В этом подходе выполняются прямые преобразования Лапласа численно инвертированных преобразований для сравнения с исходной функцией. Численное прямое преобразование Лапласа реализуется с использованием составного правила Симпсона.

Точность может быть проверена сравнением с исходной формой преобразования Лапласа. Мы наблюдаем улучшение точности инверсий с увеличением числа членов разложения и уровня заданной точности, что приводит к более устойчивым решениям.

Вычислительная эффективность, в зависимости от уровня заданной точности, продемонстрирована на примере распределения времени ожидания в моделях *M*/*G*/1.

Список литературы

1. Abate J., Valko P. Multi-precision Laplace transform inversion // International Journal for Numerical Methods in Engineering. 2004. Vol. 60. Pp. 979-993.

2. Atkinson K. An Introduction to Numerical Analysis: 2nd ed. John Wiley & Sons, 1989.

3 Bailey D. High-Precision Software Directory. 2024 URL: https://www.davidhbailey.com/dhbsoftware/ (дата обращения 04.10.2025).

4. Cohen A. Numerical Methods for Laplace Transform Inversion. Springer, 2007.

5. Edwards C., Penney C. Differential Equations and Boundary Value Problems: 5th ed. Computing and Modeling, 2015.

6. Kao E. An Introduction to Stochastic Processes. Duxbury Press, 1997.

7. Клейнрок Л. Теория Массового Обслуживания. Том I. М.: Машиностроение, 1979.

8. Kreyszig E. Advanced Engineering Mathematics: 10th ed. John Wiley & Sons, 2011. 1280 p.

9. Krougly Z., Davison M., Aiyar S. The role of high precision arithmetic in calculating numerical Laplace and inverse Laplace transforms // Applied Mathematics. 2017. Vol. 8. Pp. 562-589.

10. Krougly Z., Jeffrey D. Implementation and application of extended precision in Matlab / In: N. Mastorakis et al (Eds.). Proc. of the Applied Computing Conference ACC'09, WSEAS Press. 2009. Pp. 103-108.

11. Krougly Z., Stanford D. Iterative algorithms for performance evaluation of closed network models // Performance Evaluation. 2005. Vol. 61. Pp. 41-64.

12. Krougly Z., Jeffrey D., Tsarapkina D. Software implementation of numerical algorithms in arbitrary precision / In: 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2013). N. Bjorner et al. (Eds.). IEEE Computer Society. 2014. Pp. 132-138.

13. Kuhlman K. Review of inverse Laplace transform algorithms for Laplace-space numerical approaches // Numerical Algorithms. 2013. Vol. 63. Pp. 339-355.

14. Kuznetsov A. On the convergence of Gaver-Stehfest algorithm // SIAM J. Numer. Anal. 2013. Vol. 51. Pp. 2984-2998.

15. Murli A., Rizzardi M. Algorithm 682 Talbot's method for the Laplace inversion problem // ACM Transactions on Mathematical Software. 1990. Vol. 16. Pp. 158-168.

16. Nadarajah S., Kotz S. On the Laplace transform of the Pareto distribution // Queueing System. 2006. Vol. 54. Pp. 243-244.

17. Shortle J., Thompson J., Gross D. et al. Fundamentals of Queueing Theory: 5th ed. Wiley, New York, 2018.

18. Stehfest H. Алгоритм 368: Численная инверсия преобразования Лапласа // Communications of the ACM. 1970. Vol. 13(1). Pp. 47-49.

References

1. Abate J., Valko P. Multi-precision Laplace transform inversion. *International Journal for Numerical Methods in Engineering* 2004;60:979-993.

2. Atkinson K. An Introduction to Numerical Analysis: 2nd ed. John Wiley & Sons; 1989.

3. Bailey D. High-Precision Software Directory. (accessed 04.10.2025). Available at: https://www.davidhbailey.com/dhbsoftware.

4. Cohen A. Numerical Methods for Laplace Transform Inversion. Springer; 2007.

5. Edwards C., Penney C. Differential Equations and Boundary Value Problems: 5th ed. Computing and Modeling; 2015.

6. Kao E. An Introduction to Stochastic Processes. Duxbury Press; 1997.

7. Kleinrock L. Queueing systems. Volume 1. Moscow: Mashinostriyeniye; 1979.

8. Kreyszig E. Advanced Engineering Mathematics: 10th ed. John Wiley & Sons; 2011.

9. Krougly Z., Davison M., Aiyar S. The role of high precision arithmetic in calculating numerical Laplace and inverse Laplace transforms. *Applied Mathematics* 2017;8:562-589.

10. Krougly Z., Jeffrey D. Implementation and application of extended precision in Matlab. In: Mastorakis N. et al., editors. Proc. of the Applied Computing Conference ACC'09, WSEAS Press; 2009. Pp. 103-108.

11. Krougly Z., Stanford D. Iterative algorithms for performance evaluation of closed network models. *Performance Evaluation* 2005;61:41-64.

12. Krougly Z., Jeffrey D., Tsarapkina D. Software implementation of numerical algorithms in arbitrary precision. In: Bjorner N. et al., editors. 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2013). IEEE Computer Society; 2014. Pp. 132-138.

13. Kuhlman K. Review of inverse Laplace transform algorithms for Laplace-space numerical approaches. *Numerical Algorithms* 2013;63:339-355.

14. Kuznetsov A. On the convergence of Gaver-Stehfest algorithm. SIAM J. Numer. Anal. 2013;51:2984-2998.

15. Murli A., Rizzardi M. Algorithm 682 Talbot's method for the Laplace inversion problem. *ACM Transactions on Mathematical Software* 1990;16:158-168.

16. Nadarajah S., Kotz S. On the Laplace transform of the Pareto distribution. *Queueing System* 2006;54:243-244.

17. Shortle J., Thompson J., Gross D. et al. Fundamentals of Queueing Theory: 5th ed. Wiley (New York); 2018.

18. Stehfest H. Algorithm 368: Numerical inversion of Laplace transforms. *Communications of the ACM* 1970;13(1):47-49.

Сведения об авторе

Зиновий Круглый, Факультет Прикладной Математики, Западный Университет, Лондон, Онтарио, Канада, e-mail: zkrougly@uwo.ca.

About the author

Zinovi Krougly, Department of Applied Mathematics, Western University, London, Ontario, Canada N6A5B7, e-mail: zkrougly@uwo.ca.

Вклад автора

Исследование проведено автором самостоятельно в полном объеме.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

УДК 629.039.58
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-17-28

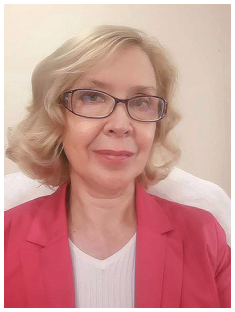
К выбору методов оценки статистических параметров надежности элементов систем для использования в вероятностном анализе безопасности

On the choice of methods for estimating statistical parameters of system component reliability for use in probabilistic safety analysis

Горюнов О.В.[1]*, Кузьмина И.Б.[1]
Goriunov O.V.[1]*, Kuzmina I.B.[1]

[1] *АО «РЭИН Инжиниринг», Санкт-Петербург, Российская Федерация*
[1] *JSC REIN Engineering, Saint Petersburg, Russian Federation*
* *ovgoriunov@mail.ru*

Горюнов О.В.



Кузьмина И.Б.

Резюме. Цель. *Проработать анализ факторов, которые могут повлиять на выбор метода(ов) оценки интенсивности отказов элементов систем при использовании его/их результатов в целях анализа надежности и выполнения вероятностного анализа безопасности.* **Методы.** *В статье применяются методы математического анализа, теории вероятностей.* **Результаты.** *Представлены результаты применения ряда методов для выборки N = 23 (групп) и выборок объемом N = 12 и N = 6. Выборки N = 12 и N = 6 составлены из вариационного ряда исходной выборки (N = 23) по следующему правилу, принятому для целей демонстрации подхода: для N = 12 – все четные, для N = 6 – каждый 4-й, что обеспечивало «подобность» выборок. В качестве специфических данных рассмотрено два варианта z = 0, t = 11,2 и z = 4, t = 11,2.* **Заключение.** *Представлен краткий обзор методов, используемых на практике для оценки характеристик интенсивности отказов элементов систем блока АЭС. Отмечены особенности представленных подходов, представлены рекомендации по использованию методов в практике подготовки исходных данных для выполнения задач анализа. Для случая отсутствия отказов в группе рекомендуется применять неинформативный метод Джеффриса. В рамках анализа надежности рекомендуется применять методы моментов, метод Морозова В.Б. и/или метод бутстрэпа.*

Abstract. Aim. *To analyse the factors that may affect the choice of the method(s) for assessing the failure rate of system components when using the results for reliability analysis and probabilistic safety analysis.* **Methods.** *The paper uses methods of mathematical analysis, probability theory.* **Results.** *The paper presents the results of applying a number of methods to a sample of N = 23 (groups) and samples of N = 12 and N = 6. Samples N = 12 and N = 6 are made up of a static series of the initial sample (N = 23) according to the following rule adopted for the purpose of demonstrating the method: for N = 12, all even, for N = 6, every 4th, that' ensured the "similarity" of the samples. Two variants, i.e. z = 0, t = 11.2 and z = 4, t = 11.2, were considered as specific data.* **Conclusions.** *The paper presents a brief overview of the practical methods for assessing the failure rate characteristics of a nuclear power unit's system components. The authors highlight the specific features of the presented approaches, provide recommendations for their application in the preparation of input data for analysis. For the case of no failures in a group, it is recommended using the Jeffreys noninformative method. Relibaility analysis should use the method of moments, the V.B. Morozov's method and/or the bootstrap method.*

Ключевые слова: *интенсивность отказов, вероятностный анализ безопасности, анализ надежности*
Keywords: *failure rate, probabilistic safety analysis, reliability analysis*

Для цитирования: *Горюнов О.В., Кузьмина И.Б. К выбору методов оценки статистических параметров надежности элементов систем для использования в вероятностном анализе безопасности // Надежность. 2025. №4. С. 17-28. https://doi.org/10.21683/1729-2646-2025-25-4-17-28*
For citation: *Goriunov O.V., Kuzmina I.B. On the choice of methods for estimating statistical parameters of system component reliability for use in probabilistic safety analysis. Dependability 2025;4: 17-28. https://doi.org/10.21683/1729-2646-2025-25-4-17-28*

Поступила: *25.03.2025* / **После доработки:** *07.09.2025* / **К печати:** *28.09.2025*
Received on: *25.03.2025* / **Revised on:** *07.09.2025* / **For printing:** *28.09.2025*

Введение

Известной задачей при разработке вероятностного анализа безопасности (ВАБ) является обеспечение качества исходных данных – интенсивностей отказов (параметр надежности элементов систем). Элементы АЭС относятся к категории высоконадежного оборудования, выпускаются относительно малыми сериями, часто эксплуатируются в режиме «горячего резерва» (в системах безопасности), что обуславливает крайне **малую статистическую выборку событий отказов**. Частным случаем является получение оценок показателей надежности для проектируемого блока при полном отсутствии специфической для этого блока эксплуатационной информации по отказам элементов систем.

Однотипные элементы систем АЭС могут эксплуатироваться в составе различных систем и при различных условиях, что может повлиять на статистические выборки по количествам отказов и, в итоге, на оценку интенсивности отказов. Использование статистических методов оценки интенсивности отказов должно быть обосновано с тем, чтобы обеспечить достаточный уровень доверия к результатам ВАБ. Применение различных статистических методов на практике приводит к различным результатам, которые обусловлены различными влияющими факторами: объем выборки, однородность выборки и др. Некорректный учет таких влияющих факторов приводит к некорректным результатам, влияющим на итоговые параметры надежности систем и результаты вероятностного анализа безопасности.

С целью проработки анализа факторов, которые могут повлиять на выбор метода(ов) оценки интенсивности отказов элементов систем при использовании его/их результатов в целях ВАБ, представляется **актуальным** выполнение анализа методов расчета характеристик интенсивностей отказов оборудования λ (среднее значение m и соответствующий фактор ошибки[1] EF) и предложение ряда рекомендаций для выбора наиболее подходящего метода оценки.

Основными **факторами, влияющими на результаты оценки интенсивности отказов элементов систем,** являются:

1. Объем выборки (количество элементов/групп элементов оборудования[2], для каждой из которых определено количество отказов);
2. Однородность выборки[3];
3. Метод статистической оценки.

[1] $EF = \lambda_{0,95} / \lambda_{0,50}$, где λ_P – квантиль распределения величины λ, соответствующий вероятности P.

[2] В данной статье начальная группировка элементов оборудования, для которых собираются данные по отказам, не рассматривается. Предполагается, что уже имеются данные по количествам отказов в каждой группе. Данные по количествам отказам являются исходной информацией для определения функции распределения для λ.

[3] Под однородностью выборки понимается соответствие всех элементов выборки одной функции распределения.

Дальнейшая дискуссия фокусируется на обсуждении влияния указанных факторов на результаты статистического анализа.

1. Малые выборки

Общепринятой верхней границы малой выборки не существует. В ряде научно-технической литературы малой выборкой называют выборку с количеством элементов в ней $N < 9…30$ [1, 2]. В общем случае, выборку можно принять малой, если ее обработка методами, основанными на группировке наблюдений, приводит к существенной потере информации [3].

При наличии малой выборки невозможно получить точную оценку функции распределения (ФР) параметров надежности, что можно показать на основе распределения Колмогорова [4]; невозможно различать близкие гипотезы (особенно простые) при малых выборках с помощью непараметрических критериев согласия [5]; не удается однозначно идентифицировать вид ФР, т.к. не отклоняются гипотезы о принадлежности выборки целому ряду законов.

В случае проверки простых гипотез, предельными распределениями статистик критериев Колмогорова и Смирнова можно пользоваться при $N > 20$ [6]. При небольших объемах выборки ($N \leq 20$) наблюдается существенная зависимость распределения статистики от N.

Обработка малой выборки требует индивидуального подхода, разработки специальных методов. Положительный результат верификации однородности малых выборок позволяет объединить выборки, тем самым обоснованно увеличив ее объем [6].

2. Верификация однородности

При решении задач статистического анализа имеет чрезвычайно важное значение проблема наличия в выборке аномальных данных (выбросов). Присутствие единственного аномального наблюдения может приводить к оценкам, которые совершенно не согласуются с другими данными в выборке (например, см. [1]).

Основным показателем ошибочности элемента в выборке может служить его отклонение от остальных наблюдений, при этом, как правило, сомнительны крайние элементы вариационного ряда. Верификацию отсутствия ошибочных данных в выборке, которые необходимо исключить из рассмотрения, можно выполнять на основе ряда критериев, например: критерий трех сигм; критерий Ирвина [7]; τ-критерий [2, 8]; критерий Романовского; критерий Морозова [7] и др.

Выявленные аномальные значения должны быть исключены из дальнейшего рассмотрения.

Результаты применения **методов статистической оценки** как определенных алгоритмов, напрямую обрабатывающих выборочные данные, зависят от качества входных данных и особенностей применяемого метода. Указанные методы разделяют на:

• параметрические – обладают максимальной эффективностью в рамках определенной модели функции распределения $F(x, \theta)$, где x – значения, принимаемые случайной величиной; θ – параметр распределения;

• непараметрические – применимы к широкому классу распределений, т.к. функцию распределения из этих классов нельзя задать с помощью конечного числа параметров.

Используемые методы статистических оценок должны характеризоваться критериями качества:

I. Состоятельность. Оценка $\theta_N(x_1, \ldots, x_N)$ сходится по вероятности к истинному значению θ, т.е. $\theta_N \to \theta$ при $N \to \infty$, $P(|\theta_N - \theta| < \varepsilon) = 1$ для любого $\varepsilon > 0$. В противном случае оценка не имеет практического смысла;

II. Несмещенность. Математическое ожидание величины θ_N равно истинному значению θ, $M[\theta_N] = \theta$, т.е. отсутствует систематическое занижение или завышение оценки;

III. Эффективность. Оценка θ_N при заданном объеме выборки N имеет наименьшую возможную дисперсию. Оценка является эффективной, если для несмещенной оценки θ_N достигается равенство Рао-Крамера: $M[(\theta_N - \theta)^2] = (I_N(\theta))^{-1}$, где $I_N(\theta)$ – информация Фишера [10, 11]. Несмещенная оценка будет эффективной, если функцию правдоподобия $L(\theta; \vec{x})$ можно представить в виде [11]

$$L(\theta; \vec{x}) = C(\vec{x}) \cdot \exp\left(\int (\theta_N(\vec{x}) - \omega) \cdot I_N(\omega) \, d\omega\right), \qquad (1)$$

где $C(\vec{x})$ – некая функция, ω – переменная интегрирования.

В соответствии с (1) форма записи функции плотности распределения влияет на получение эффективных несмещенных оценок, что рекомендуется учитывать в расчетах: показательное $\lambda \cdot \exp(-\lambda x)$, Пуассона $\frac{(\lambda t)^x}{x!} e^{-\lambda t}$, гамма $k^k x^{k-1} \frac{e^{-xk/m}}{m^k \Gamma(k)}$.

Критерии качества (I, II, III), обозначенные выше, характеризуют исключительно применяемый математический метод оценивания, который не соотносится с имеющейся статистической базой.

Общими для каждой группы данных принимаются следующие допущения:

• наработка до отказа элемента подчиняется экспоненциальному закону распределения вероятностей с параметром λ (вероятность отказа за время t: $P(t)=1-e^{-\lambda t}$);

• интенсивность отказов λ каждого элемента постоянна во времени;

• в момент отказа элемента он заменяется новым, идентичным отказавшему элементу;

• абсолютная погрешность исходных данных пренебрежимо мала;

• наработки до отказа – независимые величины.

Из представленных выше допущений следует, что:

1) $\lambda = 1/M[t]$, где $M[t]$ – средняя наработка до отказа t;

2) распределение числа отказов r за время наблюдения T описывается законом Пуассона [12; 13]

$$P(r; \lambda T) = \frac{(\lambda T)^k}{k!} e^{-\lambda T}; \qquad (2)$$

3) $\lambda = M[r]/T$;

4) достаточная статистика[1] – суммарное число отказов.

Рассмотрим ряд подходов к оценке интенсивности отказов и сравним результаты, полученные на основе их применения для различных объемов исходных данных.

Группирование данных выполняют с целью снижения уровня неоднородности. Статистические характеристики групп могут быть оценены на основе распределения Пуассона. Методы применимы для каждой группы в отдельности и в целом для объединенных групп данных.

3. Параметрические подходы к оценке параметров надежности элементов систем на основе однородных выборок

Применение параметрических подходов требует верификации однородности выборки, поскольку предполагается, что рассматриваемая выборка из одного распределения.

3.1. Метод моментов (ММ)

Метод был предложен К. Пирсоном (1894) и является исторически первым общим методом построения оценок [4, 13]. Пусть $\{x_k\}$, $k = 1,..., N$ – выборка параметрического семейства функций распределения $F(x; a_1, \ldots, a_N)$. Оценки параметров a_n, $n = 1,\ldots,m$ – решение системы уравнений:

$$\frac{1}{N}\sum_{k=1}^{N} x_k^n = \int_0^{\infty} x^n dF(x; \vec{a}_N), n = 1, \ldots, m.$$

В соответствии с законом больших чисел $M\left[\frac{1}{N}\sum_{k=1}^{N} g(x_k)\right] \to M[g(x)]$ при $N \to \infty$, что обеспечивает состоятельность оценок, однако свойство несмещенности и эффективности для оценок a_N в общем виде не выполняется, поэтому **обычно ММ применяется в случае больших выборок.**

3.2. Метод максимального правдоподобия (ММП)

Метод предложен Р. Фишером (1912 г.). Идея метода заключается в том, что мы максимизируем вероятность

[1] **Доста́точная стати́стика**- набор функций (называемых статистиками) от результатов наблюдений над случайной величиной, который содержит ту же информацию о параметре семейства распределений вероятностей этой случайной величины, что и сами результаты наблюдений

получения имеющейся выборки в результате наблюдений. Результаты выборки рассматривают как одну из возможных реализаций N-мерной случайной величины с независимыми компонентами, имеющими одну и ту же функцию плотности распределения $f(x; \theta)$.

Функция правдоподобия имеет вид $L(\theta;\vec{x})=\prod_{k=1}^{N} f(x_k;\theta)$.

В качестве оценки θ_N принимается значение, при котором функция правдоподобия достигает своего максимума [4, 10, 12, 13]. Оценки ММП асимптотически нормальны: $\theta_N \sim N(\theta, 1/I_N(\theta))$.

Для обхода ограничения $\lambda k \neq 0$ в случае применения ММП для гамма распределения можно использовать распределение $g(x; m, \eta+1)$ [14; 15], для которого $x \geq 0$, но необходимо показать корректность такого предположения.

3.3. Метод максимального произведения спейсингов (МПС)

Метод предложен Ченом и Амином в 1983 г. Метод спейсингов (method of maximal spacing) предлагает для оценивания параметра(ов) распределения максимизировать функцию

$$S\left(x_{(1)},\ldots,x_{(N)};\theta_N\right)=\prod_{k=1}^{N} D_k,$$

где $D_k = P(x(k) \leq X \leq x(k+1); \theta)$ – спейсинг; $x(k)$ – вариационный ряд (упорядоченная по возрастанию выборка $\{x_k\}$). Тогда значение θ_N, максимизирующее S, называют оценкой методом спейсингов. Мотивировкой метода является то обстоятельство, что в силу условия $\sum_{k=1}^{N} D_k = 1$ максимум функции $\sum_{k=1}^{N} \ln D_k$ достигается, когда все $D_k=1/N$.

Эта оценка состоятельна, а в случае регулярных оценок асимптотически эффективна. Большим недостатком является затруднительность аналитических вычислений, большая часть задач решается численно.

3.4. Метод Морозова В.Б.

В работе [16] представлено углубленное и систематическое изложение метода, развивающего идеи работы [17]. В рамках байесовского подхода для однотипных элементов разных систем родственных энергоблоков АЭС выполняется конструирование некоторого обобщенного распределения, которое учитывает вариативность параметра надежности относительно более широкой популяции, по сравнению с той группой, к которой принадлежит данный элемент в энергоблоке анализируемой АЭС.

В общем виде подход может быть изложен следующим образом. Оценку для математического ожидания материнского распределения можно получить в классе линейных оценок максимума правдоподобия

$$z = \sum_{k=1}^{N} w_k x_k, \qquad (3)$$

где x_k – оценка математического ожидания в k-ой группе, w_k – коэффициенты разложения. Полагая, что ФР x_k имеет один параметр $F(x; a)$, безусловное математическое ожидание величины x_k обозначим $M[x]=M[M[x|a]]=m$. Соответственно

$$M[z] = m\sum_{k=1}^{N} w_k,$$

откуда следует условие несмещенности $\sum_{k=1}^{N} w_k = 1$. Обозначая $D[M[x|a]]=D$, безусловную оценку (3) можно записать в виде:

$$D[z] = \sum_{k=1}^{N} w_k^2 \left(M\left[D\left[x_k \mid a\right]\right] + D\right) = \sum_{k=1}^{N} w_k^2 D_k.$$

При этом условие эффективности имеет вид [18]: $w_n = \dfrac{D_n^{-1}}{\sum_{k=1}^{N} D_k^{-1}}$. Параметры m, D являются функциями параметров материнского распределения $f(a;\vec{\omega})$. Учитывая, что

$$f(x) = \int f(x \mid a)\cdot f(a;\vec{\omega})\, da,$$

где $f(a;\vec{\omega})$ – априорная плотность распределения, сопряженная распределению функции правдоподобия; $f(x|a)$ – условная плотность распределения случайной величины x, вид которой считается известным; указанные параметры могут быть оценены на основе ММП.

Учитывая, что m, D являются характеристиками $M[x|a]$, а не случайную величину a, оценку дисперсии параметра a предлагается постулировать в виде взвешенной суммы дисперсий в отдельных группах с весовыми коэффициентами w_k:

$$D[a]=ND[z],$$

что приводит к необходимости корректировки параметров распределения $f(a;\vec{\omega})$.

Для случая распределения Пуассона (1) сопряженным априорным распределением является гамма распределение $g(\lambda; \omega_1, \omega_2)$, параметры которого имеют вид

$$\omega_1 = \frac{\tau}{N}\sum_{j=1}^{N} \frac{r_j}{T_j+\tau};\ \ \omega_2 = \frac{\tau}{N}\sum_{j=1}^{N} \frac{T_j}{T_j+\tau},$$

где r_j, T_j – результаты группирования данных, параметр τ определяется из советующего уравнения ММП.

3.5. Оценки на основе смещенных оценок (метод Михайлова В.С.)

Для плана однородных испытаний с восстановлением случайная величина Σr_k имеет пуассоновское распределение

$$P\left(\sum r_k = m \mid \lambda \sum T_k\right) = \frac{\left(\lambda \sum T_k\right)^m}{m!} e^{-\lambda \sum T_k}.$$

При этом достаточной статистикой является число наблюденных отказов Σr_k. На основе использования интегральных характеристик в работе [19] получена эффективная оценка средней наработки до отказа в классе смещенных оценок, представимых в виде $T = \frac{\sum T_k}{r+1} + \sum T_k \cdot f(r)$. При этом оценка параметра λ имеет вид:

$$r = 0, \lambda = \left(2\sum T_k\right)^{-1}, r \neq 0, \lambda = \frac{r+1}{\sum T_k}.$$

3.6. Байесовский подход

В докладе [20] отмечается, что отношение к методу Байеса иногда сродни «религиозному». При таком отношении группа ВАБ верит, что все проблемы, связанные с недостатком данных, могут быть всегда решены с помощью байесовского подхода. В результате не уделяется должного внимания применимости обобщенных данных и априорной информации к АЭС, являющейся предметом анализа. Априорные значения, используемые в процессе уточнения данных, часто не согласуются со специфическими данными АЭС с точки зрения как определений исходного события / оборудования, так и численных значений.

Можно показать, что, в общем случае, оптимальной несмещенной оценкой случайной величины, минимизирующей средний квадрат ошибки, является условное математическое ожидание: $\theta_N = M[\theta|u]$, при этом такая оценка будет Байесовской.

Байесовский подход предполагает, что неизвестный параметр θ выбран случайным образом из распределения с плотностью $q(\theta)$ (априорная плотность). Выбор априорного распределения может быть либо субъективным (базирующимся на доступной априорной информации), либо объективным (необходимо сформулировать критерий, соответствующий отсутствию априорной информации и максимизирующий информационный вклад последующих наблюдений). Различают информативные и неинформативные априорные распределения.

Информативные распределения имеют определенную структуру, выбираемую исходя из имеющихся знаний об объекте исследований. Байесовское оценивание в этом случае, фактически, уточняет, на основе наблюдений, знания, заложенные в априорных распределениях. Для построения информативной ФР необходима представительная статистика.

Неинформативное распределение – специальный вид априорного распределения, который содержит максимально малое количество информации о параметре по отношению к той информации, которая может быть получена из опыта.

3.6.1. Неинформативный подход

В случае **малых выборок** (ограниченное количество или отсутствие обобщенных данных) обоснованность использования конкретного априорного распределения является дискуссионной. Одним из практических подходов в этом случае является использование правила Джеффриса (Jeffreys, 1946), основанного на идее инвариантности относительно ре-параметризации. При этом объективное априорное распределение определяется на основе информации Фишера как $q(\theta) \sim \sqrt{I_1(\theta)}$. В частности, для распределения Пуассона и показательного распределения $q(\theta) \sim \theta^{-1/2}$ [21-24].

3.6.2. Информативный подход

Априорную функцию распределения в отношении истинного значения параметра λ можно описать на основе структуры функции правдоподобия распределением, которое является сопряженным к функции правдоподобия. В частности, для показательного распределения и распределения Пуассона сопряженная ФР – гамма распределение $g(\lambda;\ r\ ,T)$. Параметры (r, T) считаются известными – оцененными на основе одного из представленного выше методов на основе доступной представительной статистики. Полагая, что специфические данные по количеству отказов за время наблюдения (z, t) известны, плотность апостериорного распределения λ находится по теореме Байеса следующим образом:

$$f(\lambda) = \frac{q(\lambda)L(z,t|\lambda)}{\int_0^\infty q(\lambda)\mathrm{L}(z,t|\lambda)\,d\lambda} = (t+T)^{r+z}\frac{\lambda^{r+z-1}\ \mathrm{e}^{-\lambda(T+t)}}{\Gamma(r+z)}. \quad (4)$$

Формулу (4) можно применять итерационно после поступления каждой новой порции данных.

Недостатком байесовского подхода является его чувствительность к выбору априорной информации – необходимость постулировать как существование априорного распределения для неизвестного параметра, так и знание его формы.

3.6.3. Метод минимакса

Каждой возможной ошибке определения значения параметра надежности можно сопоставить определенный неотрицательный вес в форме функции потерь. Наиболее часто используются следующие функции потерь [10, 25]:

- линейная по модулю $\Pi(\theta_N, \theta) = |\theta_N - \theta|$;
- квадратичная $\Pi(\theta_N, \theta) = (\theta_N - \theta)^2$;
- прямоугольная $\Pi(\theta_N, \theta) = \mathrm{H}([\theta_N - \theta] - \varepsilon)$, $\varepsilon > 0$,

где θ – истинное значение оцениваемого параметра; θ_N – оценка параметра θ. Среднее значение функции потерь как функции от совокупности случайных величин θ, θ_N определяется выражением:

$$M\left[\Pi(\theta_N,\theta)\right] = \int\left(\int q(u)W(\vec{x}|u)\,du\right)\int\Pi(\theta_N,\theta)W(\theta|\vec{x})\,d\theta d\vec{x}. \quad (5)$$

При этом функционал

$$J(z(\vec{x}),\vec{x}) = \int\Pi(z(\vec{x}),\theta)W(\theta|\vec{x})\,d\theta \quad (6)$$

называется апостериорным риском. Значение θ_N, минимизирующее функционал (6), является оптимальной

оценкой параметра θ. Результаты, соответствующие различным видам функции потерь для распределения Пуассона (2) и информативной ($z \neq 0$, $t \neq 0$) или неинформативной априорной функции ($z = -1/2$, $t = 0$), представлены в табл. 1.

Табл. 1. Результаты оптимальной оценки для различных видов функций потерь

Функция потерь	Оптимальная оценка θ_N
Квадратичная $\Pi(\theta_N, \theta) = (\theta_N - \theta)^2$	$\frac{\sum r_k + z}{\sum T_k + t}$
Линейная по модулю $\Pi(\theta_N, \theta) = \lvert\theta_N - \theta\rvert$	$\frac{z_{0,5}\left(\sum r_k + z\right)}{\sum T_k + t}$
Прямоугольная $\Pi(\theta_N, \theta) = H([\theta_N - \theta] - \varepsilon)$	$\frac{\sum r_k + z - 1}{\sum T_k + t}$

Причем на практике при выборе функции потерь следует учитывать неравенства

$$\frac{\sum r_k + z}{\sum T_k + t} > \frac{z_{0.5}\left(\sum r_k + z\right)}{\sum T_k + t} > \frac{\sum r_k + z - 1}{\sum T_k + t}.$$

3.6.4. Случай неизвестного априорного распределения

Для случая, когда **априорное распределение неизвестно**, но задано конечное количество ограничений, накладываемых на некоторые функционалы от априорного распределения в работе [26] предложен альтернативный подход на основе оценки апостериорного риска: выбирается такая априорная плотность распределения, которая обеспечивает максимум функции апостериорного риска (6). При этом априорное распределение принимается на основе формы функции правдоподобия для ФР (2) – в форме гамма распределения $g(\lambda; r+1, T)$. Параметр формы $r+1$ принимается с целью исключения возможной неопределенности при $r = 0$.

Полагая известными специфические данные объекта исследования (z, t) и априорное значение математического ожидания $\lambda_0 = (r+1)/T$ (например, на основе метода моментов или ММП) – получим, что для функции потерь в форме **квадратичной функции** максимум апостериорной дисперсии

$$\max\left\{\lambda_0^2 \cdot \frac{z + r + 1}{\left(z + \lambda_0 t\right)^2}\right\}$$

достигается при $r = 0$ если $\lambda_0 \le (2z+1)/t$, в противном случае при $r = \lambda_0 t - 2z - 1$, а $M[\lambda] = \lambda_0/2$ при $\lambda_0 t > z$ и $M[\lambda] = z/t$ при $\lambda_0 t < z$. Метод требует наличия специфических данных (z, t), причем случай $z = 0$ допускается ($M[\lambda] = \lambda_0/2$). Для случая очень надежных элементов ($z/t << 1$), результаты расчетов будут приводить к наилучшим характеристикам надежности.

4. Параметрические подходы к оценке параметров распределений на основе неоднородных выборок

Стандартные методы оценивания любой статистики выборочных данных построены на предположении, что выборка взята из однородной совокупности с простой структурой закона распределения. На практике, выборки часто формируются под влиянием различных причин и условий, и могут быть представлены в виде объединения некоторого множества однородных выборок, каждая из которых имеет простую структуру.

Неоднородные данные можно попытаться свести к однородным применяя определенные преобразования, например, если x_k подчиняется нормальному распределению $N(m_k, A \cdot s_k)$, то значение параметра A можно оценить по выборке $z_k = (x_k - m_k)/s_k \sim N(0, A)$ [27]. Для пуассоновских и экспоненциальных наблюдений использование линейных преобразований не позволяет получить требуемую редукцию к случаю однородных наблюдений.

Обработка неоднородных выборок теми же методами, какие используются для однородных, недопустима, так как она может привести не только к большим ошибкам, но и к бессмысленным результатам. Представленные ниже методы «работают» с исходно неоднородной выборкой. При этом никакой работы по приведению неоднородной к однородной не выполняется.

Линейная суперпозиция разнородных распределений

При наличии N различных выборок (групп), которые подчиняются различным распределениям $f_k(x)$, $k = 1 \ldots N$, плотность распределения объединения (не суммирования) указанных выборок может быть определена в форме линейной суперпозиции маргинальных плотностей:

$$f(x) = \sum_{k=1}^{N} w_k f_k(x) \qquad (7)$$

где w_k – коэффициенты разложения, $\sum_{k=1}^{N} w_k = 1$ – условие нормировки. Математическое ожидание объединения определяется выражением

$$m = \sum_{k=1}^{N} w_k m_k,$$

где m_k – математическое ожидание k-й выборки. Дисперсия суперпозиции (7) имеет вид:

$$D = \sum_{k=1}^{N} w_k D_k + \sum_{k=1}^{N} w_k \left(m_k - m\right)^2,$$

где D_k – дисперсия k-й выборки.

Коэффициенты w_k можно определить различными способами в зависимости от исходных данных и целей (эффективность, однородность и т.д.). Оценки, полученные на основе (7), будут состоятельными и несмещенными.

Пример. ***Надежность элементов неоднородной выборки.*** Предполагая, что все элементы, попавшие в выборку, имеют различия в производителе, условиях

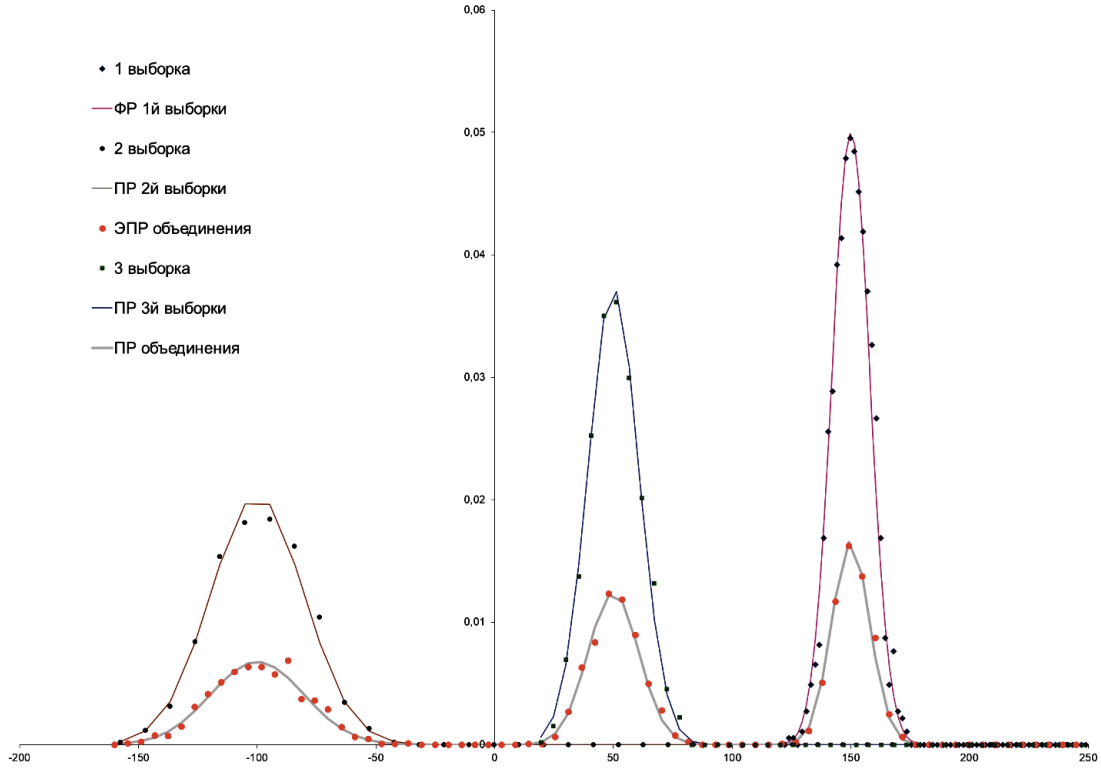


Рис. 1. Результаты объединения разнородных выборок

работы, режиме эксплуатации, классе безопасности и др. – все рассматриваемые элементы можно разделить на m групп по указанным признакам. При этом каждая группа элементов будет характеризоваться своим значением λ_k, $k = 1,\ldots,m$. Тогда вероятность безотказной работы за время t будет определяться выражением:

$$P(t) = \sum_{k=1}^{m} v_k e^{-\lambda_k t},$$

где v_k – доля элементов общей совокупности, которая характеризуется конкретным параметром λ_k. Задача оптимизации при этом не стоит: v_k известны.

При условии $\lambda_k t << 1$ зависимость $P(t)$ можно записать в виде $P(t) = 1 - \Lambda t$, где Λ – интенсивность отказа неоднородной объединенной выборки (общей совокупности):

$$\Lambda = \sum_{k=1}^{m} v_k \lambda_k.$$

В качестве примера на рис. 1 представлены результаты моделирования: плотность распределения объединения[1] трех различных выборок (по 1000 элементов в выборке), имеющих нормальное распределение с различными параметрами МО и дисперсии. На результирующий вид плотности функции распределения (ПР) интенсивности отказов (кривая «ПР объединения» на рис. 1) влияет долевой состав «новой» выборки.

Результирующая плотность распределения объединения m выборок принимает вид (7) с $v_n = N_n / \sum_{k=1}^{m} N_k$, где N_k – объем k-й выборки. Проведение эксперимента для других непрерывных распределений одного семейства также подтверждает справедливость выражения (7).

[1] Объединение нескольких выборок с различными функциями распределения.

5. Непараметрические подходы к оценке

Бутстрэп (Bootstrap) метод представлен в работах Б. Эфрона (1979 г.) [28]. Бутстрэп – процедура управления выборкой, где рандомизация перенесена с опыта на процедуру обработки данных. Преимуществом методов бутстрэп является увеличение статистики без увеличения входных данных, а также отсутствия требований к наличию какой-либо априорной информации о законе распределения (см. рис. 2). Метод не выдвигает требования по верификации однородности выборки и дает состоятельные оценки.

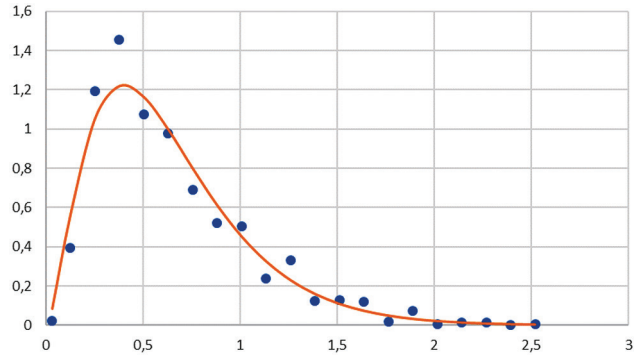


Рис. 2. Эмпирическая плотность распределения математического ожидания, полученная бутстрэп методом на основе выборки $N = 7$ [16]

Полученные на основе бутстрэп метода эмпирические функции распределения математического ожидания позволяют, на основе свойств характеристических функций (ХФ), оценить параметры «исходного» распределения.

Лемма. Пусть $\{X_k\}$ – независимые однородные данные и нам известна функция распределения случайной величины $z = \frac{1}{N}\sum_{k=1}^{N} X_k$, что позволяет определить ХФ $z(t)$. Применяя свойства ХФ, получим, что

$$\varphi_z(t) = \left[\varphi_X\left(\frac{t}{N}\right)\right]^N.$$

Т.о., зная $z(t)$, можно определить $X(t)$ и все характеристики СВ X:

$$\varphi_X\left(\frac{t}{N}\right) = \left[\varphi_z(t)\right]^{1/N} \rightarrow \varphi_X(t) = \left[\varphi_z(Nt)\right]^{1/N}.$$

В частности, если z починяется гамма распределению $g(z; s, \tau)$, то

$$\varphi_X(t) = \left(1 - \frac{itN}{\tau}\right)^{-s/N},$$

т.е. $X \sim g(x; s/N, \tau/N)$. И, соответственно, $M[X] = s/\tau$; $D[X] = N \cdot D[z]$, $D[z] = s/\tau^2$.

Табл. 2. Результаты применения методов статистической оценки

№	Метод	Математическое ожидание	D[1] (дисперсия)	EF
1	Метод моментов Пуассона (r_k, T_k)	$\frac{\sum r_k}{\sum T_k}$	$\frac{r}{T^2}$	$\frac{z_{0,95}(r)}{r}$
2	Метод моментов Гамма ($\lambda_k > 0$)	$\frac{1}{N}\sum_{k=1}^{N}\lambda_k$	–	$\frac{z_{1-\alpha/2}(k^*)}{k^*}$
3	ММП Показательное	$\frac{\sum r_k}{\sum T_k}$	$\frac{r}{T^2}$	$\frac{z_{0,95}(r+1)}{r+1}$
4	ММП Пуассона	$\frac{\sum r_k}{\sum T_k}$	$\frac{r}{T^2}$	$\frac{z_{0,95}(r)}{r}$
5	ММП Гамма распределение $\{\lambda_k \neq 0\}$	$\frac{1}{N}\sum_{k=1}^{N}\lambda_k$	–	$\frac{z_{0,95}(\mu^*)}{\mu^*}$
6	Метод Морозова В.Б. [16]	$\sum_{k=1}^{N} w_k \frac{r_k}{T_k}$	–	$\frac{z_{0,95}(\omega_1)}{\omega_1}$
7	Метод Михайлова В.С. ($r = 0$) Метод Михайлова В.С. ($r \neq 0$)	$\frac{1/2}{\sum T_k}$ $\frac{\sum r_k + 1}{\sum T_k}$	$\frac{r+1}{T^2}$	$\frac{z_{0,95}(r+1)}{r+1}$
8	Байес (неинф.распределение Джеффриса) Байес (инф.распределение)	$\frac{\sum r_k + 1/2}{\sum T_k}$ $\frac{a+z}{b+t}$	$\frac{r+1/2}{T^2}$ $\frac{a+z}{(b+t)^2}$	$\frac{z_{0,95}(r+1/2)}{r}$ $\frac{z_{0,95}(a+z)}{a+z}$
9	Минимакса $\Pi(z, Z) = H([z - Z] - \varepsilon)$	$\frac{\sum r_k + z - 1}{\sum T_k + t}$	$\frac{r+z-1}{(T+t)^2}$	$\frac{z_{0,95}(r+z-1)}{r+z-1}$
10	$r \neq 0, \lambda_0 t > z$ $r \neq 0, \lambda_0 t < z$	$\frac{\lambda_0}{2}$ $\frac{z}{t}$	$\frac{\lambda_0^2}{4(\lambda_0 t - z)}$ $\frac{z}{t^2}$	$\frac{z_{0,95}(\lambda_0 t - z)}{\lambda_0 t - z}$ $\frac{z_{0,95}(z)}{z}$
11	Суперпозиция распределений (гамма-распределение $\lambda_k = g(r_k + 1/2; T_k)$)	$\frac{1}{N}\sum_{k=1}^{N}\lambda_k$	–	$\frac{1}{m}\int_0^{x_{0,95}} f(x)\,dx$
12		$\frac{1}{T_\Sigma}\sum_{k=1}^{N} T_k\lambda_k$	–	
13	Бутстрэп (гамма)	$\frac{1}{N}\sum_{k=1}^{N}\frac{r_k}{T_k}$	$\frac{Nm}{\tau}$	$\frac{z_{0,95}(s/N)}{s/N}$

[1] Пустые ячейки соответствуют случаю, когда в явном виде записать выражение не представится возможным

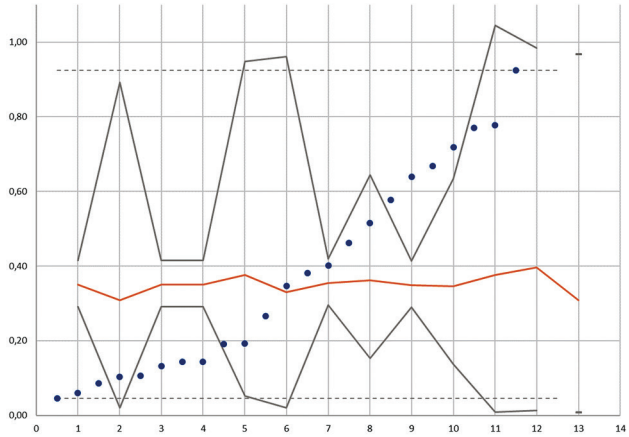


Рис. 3 Результаты оценки характеристик параметра интенсивности отказов, полученные на основе различных методов оценки, для выборки $N = 23$ (количество отказов $z \neq 0$).

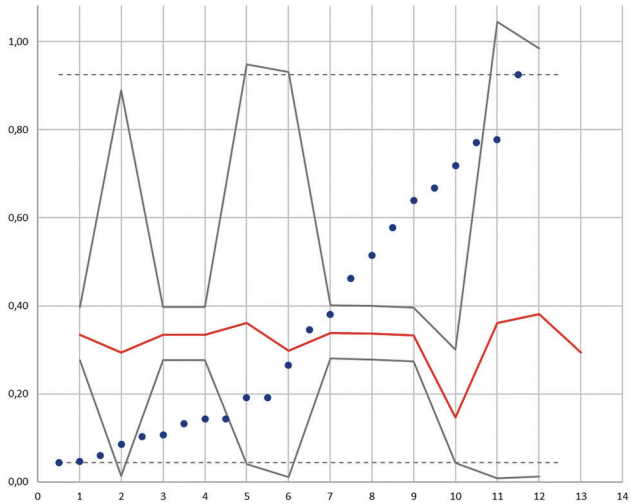


Рис. 4 Результаты оценки характеристик параметра интенсивности отказов, полученные на основе различных методов оценки, для выборки $N = 23$ (количество отказов $z = 0$).

Для гамма-распределения лемма позволяет получить явное выражение для распределения случайной величины X. Для других распределений соответствующие доверительные границы могут быть получены численными методами.

Обобщение результатов

Результаты применения методов оценки параметра интенсивности отказов представлены в табл. 2. Обозначения, используемые в Таблице 2 приведены в описании методов выше.

Из табл. 2 видно, что представленные методы приводят к оценке параметров постулированного распределения, которые характеризуются близкими значениями математического ожидания. При этом EF, как характеристика неопределенности, тем выше, чем меньше 0,95·z, поскольку $\frac{\partial}{\partial r}\frac{z_{0,95}(r)}{r} < 0$.

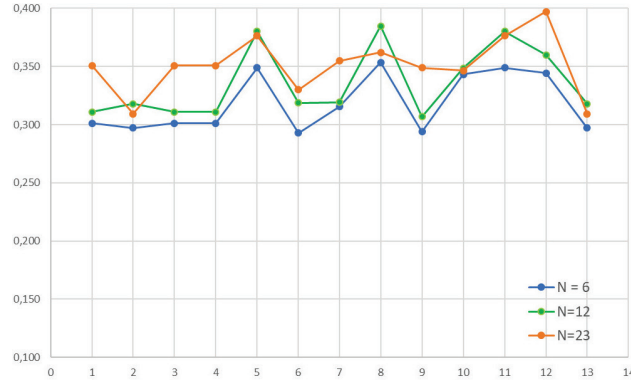


Рис. 5 Результаты оценки среднего значения, полученные на основе различных методов оценки, для выборок $N = 6$, $N = 12$, $N = 23$ (количество отказов $z \neq 0$).

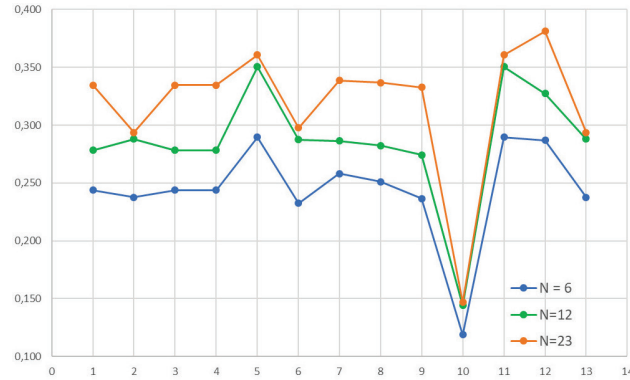


Рис. 6 Результаты оценки среднего значения, полученные на основе различных методов оценки, для выборок $N = 6$, $N = 12$, $N = 23$ (количество отказов $z = 0$).

6. Результаты расчетов

Результаты применения, представленных выше методов, для выборки $N = 23$ (групп) и выборок объемом $N = 12$ и $N = 6$ представлены на рис. 3–6. Выборки $N = 12$ и $N = 6$ составлены из вариационного ряда исходной выборки ($N = 23$) по следующему правилу, принятому для целей демонстрации подхода: для $N = 12$ – все четные, для $N = 6$ – каждый 4-й, что обеспечивало «подобность» выборок. В качестве специфических данных рассмотрено два варианта $z = 0$, $t = 11{,}2$ и $z = 4$, $t = 11{,}2$. Ось абсцисс на рис. 3–6 соответствует нумерации методов в соответствии с табл. 2.

Для каждой выборки, использованной в расчетах была выполнена верификация однородности, выявленные ошибочные значения были исключены из расчетов. Точками на рис. 3 и 4 представлены значения выборки ($N = 23$); соответствующие методу оцененные границы доверительного интервала $\lambda_{0,05}$ и $\lambda_{0,95}$ представлены серыми линиями, соответственно; пунктирные линии отражают максимальное и минимальное значения выборки; красная линия соответствует оценке математических ожиданий.

Заключение

С целью анализа факторов, которые могут повлиять на выбор метода(ов) при использовании его/их результатов в целях ВАБ, был выполнен анализ методов расчета интенсивностей отказов оборудования на различных выборках. Представлен ряд факторов, влияющих на результаты обработки данных.

Представлен краткий обзор методов, используемых на практике для оценки характеристик интенсивности отказов элементов систем блока АЭС. Отмечены особенности представленных подходов, представлены рекомендации по использованию методов в практике подготовки исходных данных для выполнения задач анализа.

Результаты оценки интенсивностей отказов представлены для выборок $N = 23$, $N = 12$ и $N = 6$ на основе применения различных методов.

Результаты расчетов позволяют сделать следующие выводы:

• применение рассмотренных методов приводит к относительно близким оценкам значений математических ожиданий;

• неопределенность, характерная для представленных методов, существенно различается в зависимости от применяемого метода оценки;

• методы № 2, 5, 6, 11, 12, 13 показали наиболее удовлетворительные результаты с точки зрения числа элементов выборки, попадающих в доверительный интервал;

• методы № 2, 6, 8, 10, 13 показали устойчивость среднего значения при уменьшении объема выборки;

• методы № 1, 3, 4, 7, 9 показали наименее корректные результаты, поскольку значительная часть данных выходит за рамки оцененного доверительного интервала.

Также можно отметить, что Метод минимакса (№ 10 в табл. 2) чувствителен к специфической информации наблюдения, что делает его неприемлемым для практического применения. Метод линейной суперпозиции (№ 11, 12) приводит, в силу своей специфики, к наибольшему доверительному интервалу и наибольшему значению математического ожидания, но малочувствителен к неоднородности выборки.

Для случая отсутствия отказов или непредставительной выборки в группе, для оценки рекомендуется применять неинформативный метод Джеффриса.

На основе выполненных расчетов, в рамках анализа надежности, рекомендуется применять методы моментов (№ 2), метод Морозова В.Б. (№ 6) и/или метод бутстрэпа (№ 13).

Список литературы

1. Fisher N.I. Statistical analysis of circular data. Cambridge: Cambridge University Press, 2000. 237 p.

2. Доспехов Б.А. Методика полевого опыта (с основами статистической обработки результатов исследований): Изд. 4-е, перераб. и доп. М.: Колос, 1979. 416 с.

3. Гаскаров Д.В., Шаповалов В.И. Малая выборка. М.: Статистика, 1978. 248 с.

4. Ллойд Э., Ледерман У. (ред.). Справочник по прикладной статистике. Том 1. М.: Финансы и статистика, 1989. 510 с.

5. Лемешко Б.Ю., Постовалов С.Н. О зависимости распределений статистик непараметрических критериев и их мощности от метода оценивания параметров // Заводская лаборатория. Диагностика материалов. 2001. Т. 67. № 7. С. 62-71.

6. Р 50.1.037-2002 правила проверки согласия опытного распределения с теоретическим, ч. II, Непараметрические критерии, М.: Гостандартинформ, 2002.

7. Морозов В.Б. О формировании групп однородности однотипного оборудования АЭС при объединении статистических данных в рамках модели Пуассона, 2024 («в печати»)

8. ГОСТ 10518-88. Системы электрической изоляции. Общие требования к методам ускоренных испытаний на нагревостойкость. М.: Гос. ком. СССР по стандартам, 1988. 29 с.

9. Пустыльник Е.И. Статистические методы анализа и обработки наблюдений, М.: Наука, 1968. 290 с.

10. Левин Б.Р. Теоретические основы статистической радиотехники. М.: 1989, 656 с.

11. Б.Л. ван дер Варден. Математическая статистика. М.: Изд-во иностранной литературы, 1960. 435 с.

12. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. М.: Наука, 1965. 526 с.

13. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся втузов: 13-изд., испр. М.: Наука, Гл.ред.физ.-мат.лит., 1986. 544 с.

14. ГОСТ 11.011-83. Прикладная статистика. Правила определения оценок и доверительных границ для параметров гамма-распределения. М.: Гос. ком. СССР по стандартам, 1985. 50 с.

15. Волковицкий С.О., Любарский А.В., Солдатов В.С., Жукова Е.В. Рациональная методология оценки параметрической неопределенности, использованная в ВАБ Калининской и Нововоронежской АЭС // Вестник Госатомнадзора России. 2004. №3. С. 3-7.

16. Морозов В.Б., Морозова М.А. О методах оценки интенсивности отказов оборудования для вероятностного анализа безопасности проектируемой АЭС при объединении данных от различных источников // Надежность и качество сложных систем. 2024. № 1. С. 39-48. DOI: 10.21685/2307-4205-2024-1-5

17. Morozov V.A. Treatment of Uncertainties for Component Reliability or Initiator Frequency Estimates Based on Combining Data Sources with the Potential of Non-Homogeneity // Proceedings of the International Topical Meeting on Probabilistic Safety Assessment PSA-99. Washington, DC, 1999. Pp. 377–379.

18. Закс Ш. Теория статистических выводов. М.: Мир, 1975. 779 с.

19. Михайлов В.С. Нахождение эффективной оценки средней наработки на отказ // Надежность. 2016. № 4. С. 40-42. DOI: 10.21683/1729-2646-2016-16-4-40-42

20. Любарский А.В., Токмачев Г.В. Уроки, полученные при проведении экспертиз ВАБ АЭС с ВВЭР. Сборник трудов международной конференции PSAM7-ESREL'04, 14-18 июня 2004 г., Берлин, Германия, том 1, стр.32-38.

21. Зельнер А. Байесовские методы в эконометрии М.: Статистика, 1980. 440 с.

22. РБ-100-15. Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций. Утв. приказом Федеральной службы по экологическому, технологическому и атомному надзору от 28 января 2015 г. № 26.

23. Бард Й. Нелинейное оценивание параметров. М.: Статистика, 1979. 349 с.

24. Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants. IAEA-TECDOC-1511 IAEA, Vienna, 2006. URL: https://www-pub.iaea.org/MTCD/publications/PDF/te_1511_web.pdf (дата обращения 01.10.2025).

25. Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants. IAEA-TECDOC-1511 IAEA, Vienna, 2006. URL: https://www-pub.iaea.org/MTCD/publications/PDF/te_1511_web.pdf (дата обращения 01.10.2025).

26. Куликов Е.И., Трифонов А.П. Оценка параметров сигналов на фоне помех. М.: Сов. радио, 1978. 296 с.

27. Савчук В.П., Байесовские условно минимаксные оценки надежности технических систем // Автомат. и телемех. 1986. Вып. 8. С. 156-162.

28. Боровоков А.А. Математическая статистика. СПб.: Лань, 2010. 704 с.

29. Эфрон Б. Нетрадиционные методы многомерного статистического анализа: Сб.статей. М.:Финансы и статистика, 1988. 263 с.

References

1. Fisher N.I. Statistical analysis of circular data. Cambridge: Cambridge University Press; 2000.

2. Dospekhov B.A. [Methodology of field testing (including foundations of statistical processing of research results): 4th ed., revised and extended]. Moscow: Kolos; 1979. (in Russ.)

3. Gaskarov D.V., Shapovalov V.I. [Small sample]. Moscow: Statistika; 1978. (in Russ.)

4. Lloyd E., Lederman W., editors. Handbook of applied statistics. Volume 1. Moscow: Finansy i statistika; 1989.

5. Lemeshko B.Y., Postovalov S.N. [On the dependence of distributions and power of nonparametric criteria statistics on the method of parameter estimation]. *Industrial laboratory. Diagnostics of materials* 2001;67(7):62-71. (in Russ.)

6. R 50.1.037-2002 [Rules for verifying the agreement of an experimental distribution with a theoretical one, Part II, Nonparametric criteria]. Moscow: Gostandartinform; 2002. (in Russ.)

7. Morozov V.B. [On defining homogeneity groups of same-type nuclear power plant equipment when combining statistical data within a Poisson model]; 2024 (preprint).

8. GOST 10518-88. Electric insulation systems and other polymer systems. General requirements for methods of accelerated tests for thermal endurance. Moscow: USSR State Committee for Standardisation; 1988. (in Russ.)

9. Pustylnik E.I. [Statistical methods for analysing and processing observations]. Moscow: Nauka; 1968. (in Russ.)

10. Levin B.R. [Theoretical foundations of statistical radio engineering]. Moscow: 1989. (in Russ.)

11. B.L. Waerden. Mathematische Statistik. Moscow: Izdatelstvo inostrannoy literatury; 1960.

12. Gnedenko B.V., Belyaev Yu.K., Solovyov A.D. [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965. (in Russ.)

13. Bronstein I.N., Semendyaev K.A. [Handbook of mathematics for engineers and students of higher education institutions: 13th ed., revised]. Moscow: Nauka, Main Office for Literature of Physics and Mathematics; 1986. (in Russ.)

14. GOST 11.011-83. Applied statistics. Regulations for determination of estimates and confidence limits for parameters of gamma distribution. Moscow: USSR State Committee for Standardisation; 1985. (in Russ.)

15. Volkovitsky S.O., Lyubarsky A.V., Soldatov V.S., Zhukova E.V. [A rational methodology for estimating parametric uncertainty used in the Kalininskaya and Novovoronezhskaya nuclear power plants]. *Vestnik Gosatomnadzora Rossii* 2004;3:3-7. (in Russ.)

16. Morozov V.B., Morozova M.A. On methods for assessing equipment failure rates for probabilistic safety analysis of nuclear power plants at design stage when pooling data from various sources. *Reliability and quality of complex systems* 2024;(1):39-48. (in Russ.). DOI: 10.21685/2307-4205-2024-1-5

17. Morozov V.A. Treatment of Uncertainties for Component Reliability or Initiator Frequency Estimates Based on Combining Data Sources with the Potential of Non-Homogeneity. In: Proceedings of the International Topical Meeting on Probabilistic Safety Assessment PSA-99. Washington, DC; 1999. Pp. 377–379.

18. Zacks S. The theory of statistical inference. Moscow: Mir; 1975.

19. Mikhailov V.S. [Efficient estimation of mean time to failure]. *Dependability* 2016;4:40-42. (in Russ.) DOI: 10.21683/1729-2646-2016-16-4-40-42.

20. Lyubarsky A.V., Tokmachev G.V. [Lessons learned from expert evaluations of the PSA of VVER-based NPPs]. In: Proceedings of the international conference PSAM7-ESREL'04, June 14-18; 2004; Berlin (Germany); Volume 1. Pp. 32-38. (in Russ.)

21. Zelner A. [Bayesian methods in econometrics]. Moscow: Statistics; 1980. (in Russ.)

22. RB-100-15. [Recommendations on the procedure for analysing the dependability of safety-critical systems and elements of nuclear power plants and their functions]. Approved by Order No. 26 of the Federal Service for Environmental, Technological and Nuclear Supervision dated January 28, 2015. (in Russ.)

23. Bard Y. Nonlinear parameter estimation. Moscow: Statistika; 1979. (in Russ.)

24. Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants. IAEA-TECDOC-1511 IAEA. Vienna; 2006. (accessed 01.10.2025). Available at: https://www-pub.iaea.org/MTCD/publications/PDF/te_1511_web.pdf.

25. Kulikov E.I., Trifonov A.P. [Estimation of signal parameters against interference]. Moscow: Sovietskoye radio; 1978. (in Russ.)

26. Savchuk V.P. Bayesian minimax estimates of systems reliability. *Avtomat. i Telemekh.* 1986;8:156-162. (in Russ.)

27. Borovkov A.A. [Mathematical statistics]. Saint Petersburg: Lan; 2010. (in Russ.)

28. Efron B. [Unconventional methods of multivariate statistical analysis: collected papers]. Moscow: Finansy i statistika; 1988. (in Russ.)

Сведения об авторах

Горюнов Олег Владимирович, кандидат технических наук, руководитель направления, ORCID: 0000-0001-6414-8619, e-mail: ovgoriunov@mail.ru, АО «РЭИН Инжиниринг», 194044, Россия, г. Санкт-Петербург, Выборгская наб., 45Е.

Кузьмина Ирина Борисовна, эксперт, кандидат технических наук,, e-mail: IrBoKuzmina@rosatom.ru, АО «РЭИН Инжиниринг», 115114, Россия, г. Москва, ул. Летниковская, д.10, стр. 5.

About the authors

Goryunov, Oleg V., Candidate of Technical Sciences, Head of the department, ORCID: 0000-0001-6414-8619, e-mail: ovgoriunov@mail.ru, RHEIN Engineering JSC, 45E Vyborgskaya nab., Saint Petersburg, Russia, 194044.

Kuzmina, Irina B., expert, Candidate of Technical Sciences,, e-mail: IrBoKuzmina@rosatom.ru , JSC "RHEIN Engineering", 115114, Russia, Moscow, Letnikovskaya str., 10, building 5

Вклад авторов

Горюнов О.В. и **Кузьмина И.Б.** совместно выполнили анализ методов оценки статистических параметров надёжности и провели сравнительные расчёты на различных выборках, сформулировали рекомендации по выбору методов для использования в вероятностном анализе безопасности.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

УДК 519.216
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-29-35

Исследование оценок параметров распределения по малой выборке

A study of small-sample estimates of distribution parameters

Воловик А.В.[1]*
Volovik A.V.[1]*

[1] *АО «ОДК-Климов», Санкт-Петербург, Российская Федерация*
[1] *JSC "UEC-Klimov", Saint Petersburg, Russian Federation*
* *volovik_aleksandr@mail.ru*

Воловик А.В.

Резюме. Цель. *Оценка параметров распределения по малой выборке представляет самостоятельную нетривиальную задачу, при решении которой путем максимизации функции правдоподобия можно получить сильно смещенный результат. В статье проанализированы свойства некоторых оценок параметров бета-распределения 1-го рода по малой выборке.* **Методы.** *Сравнение оценок параметров бета-распределения по малой выборке различными методами проведено имитационным моделированием при числе испытаний $N = 10^4$.* **Результаты.** *Оценки параметров методом максимального правдоподобия действительно дают сильно смещенный результат для выборок малого объема. Бутстреп-метод, по сравнению с методом максимального правдоподобия, дает менее смещенные оценки с меньшей дисперсией. Наиболее приемлемый (близкий к исходным значениям) результат получен с использованием математического ожидания (или медианы) и дисперсии.* **Выводы.** *Для выборок малого объема вряд ли можно рекомендовать какой-либо конкретный способ оценки параметров. Наиболее целесообразным представляется нейросетевой анализ малых выборок. С помощью нейросетевого объединения нескольких способов оценки можно существенно улучшить ее точность.*

Abstract. Aim. *Evaluating distribution parameters based on small samples is an unconventional problem in itself. Solving it by maximizing the likelihood function may produce highly biased results. The paper analyses the properties of some small-sample estimates of beta distribution parameters of the 1-st kind.* **Methods.** *The comparison of small-sample estimates of beta distribution parameters using various methods involved simulation with the number of tests $N = 10^4$.* **Results.** *Parameter estimation using the maximum likelihood method does produce a highly biased result for small samples. The bootstrap method, as compared to the maximum likelihood method, produces less biased estimates with a smaller variance. The most acceptable (close to the initial values) result was obtained using the mathematical expectation (or median) and variance.* **Conclusion.** *For small samples, no particular method of parametre estimation can be recommended. The neural network analysis appears to be the best suited for small samples. Neural network integration of a number of methods of estimation may significantly improve its accuracy.*

Ключевые слова: *малая выборка, плотность распределения, статистика, гипотеза, оценка параметра, бутстреп-метод, правдоподобие, нейросетевой анализ.*
Keywords: *small sample, distribution density, statistics, hypothesis, parameter estimation, bootstrap method, likelihood, neural network analysis.*

Для цитирования: *Воловик А.В. Исследование оценок параметров распределения по малой выборке // Надежность. 2025. №4. С. 29-35. https://doi.org/10.21683/1729-2646-2025-25-4-29-35*
For citation: *Volovik, A.V. A study of small-sample estimates of distribution parameters. Dependability 2025;4: 29-35. https://doi.org/10.21683/1729-2646-2025-25-4-29-35*

Поступила: *21.06.2025* / **После доработки:** *20.07.2025* / **К печати:** *28.09.2025*
Received on: *21.06.2025* / **Revised on:** *20.07.2025* / **For printing:** *28.09.2025*

Введение

Предложенный в [1] комбинаторный способ идентификации малой выборки предполагает знание параметров распределения проверяемой гипотезы для вероятностного интегрального преобразования [2] исходной выборки в выборку, наблюдения которой распределены равномерно в интервале [0;1].

Оценка параметров распределения по малой выборке представляет самостоятельную нетривиальную задачу [3, 4], при решении которой путем максимизации функции правдоподобия можно получить сильно смещенный результат [5].

В монографии [6] подробно рассмотрены проблемы оценки параметров бета-распределения. В частности, рядом исследований установлено, что метод моментов дает более близкие к истинным значениям оценки параметров бета-распределения по сравнению с методом максимального правдоподобия.

В данной статье исследованы оценки параметров классического бета-распределения 1-го рода по малой выборке, произведенные наиболее известными способами.

1. Метод

Классическое бета-распределение 1-го рода имеет плотность [7, 8, 9]

$$f(x)=\frac{1}{B(\lambda,\mu)}x^{\lambda-1}(1-x)^{\mu-1},\ 0\le x\le 1,\ \lambda>0,\ \mu>0, \quad (1)$$

где $B(\lambda,\mu)=\dfrac{\Gamma(\lambda)\Gamma(\mu)}{\Gamma(\lambda+\mu)}$ – бета-функция; λ, μ – параметры распределения; $\Gamma(\cdot)$ – гамма-функция.

На рис. 1 показана плотность бета-распределения с комбинациями параметров, которые использовались в [1] при исследовании мощности комбинаторного критерия равномерности.

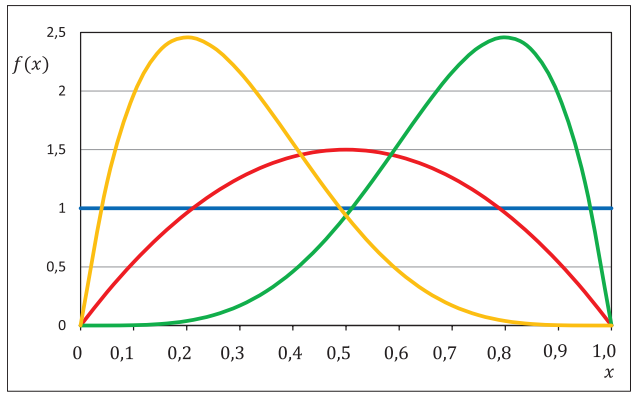


Рис. 1. Плотность бета-распределения при параметрах:
λ = 1 и μ = 1; λ = 1,5 и μ = 1,5;
λ = 1,5 и μ = 1; λ = 1 и μ = 1,5;

Сравнение оценок параметров бета-распределения по малой выборке различными методами проведено имитационным моделированием при числе испытаний $N=10^4$.

Одними из традиционных оценок параметров распределений служат оценки максимального правдоподобия, которые максимизируют функцию [2]

$$l(X_1,X_2,\ldots,X_n\,|\,\lambda,\mu)=\prod_{i=1}^{n}f(X_i\,|\,\lambda,\mu).$$

При этом в общем случае нет гарантий, что для конечных выборок оценки максимального правдоподобия окажутся несмещенными [2]. В табл. 1 приведены

Табл. 1. Результаты оценки параметров методом максимального правдоподобия

Параметры исходного бета-распределения	Оценки параметров	Объем выборки, n											
		2	3	4	5	6	7	8	9	10	11	12	1000
λ=1,0 μ=1,0	$M(\hat{\lambda})$	4,46	3,19	2,47	2,01	1,81	1,63	1,52	1,44	1,37	1,33	1,30	1,00
	$D(\hat{\lambda})$	12,73	8,69	5,57	3,43	2,42	1,62	1,18	0,87	0,62	0,54	0,42	0,002
	$M(\hat{\mu})$	4,47	3,17	2,50	2,00	1,81	1,63	1,51	1,44	1,37	1,33	1,29	1,00
	$D(\hat{\mu})$	12,74	8,55	5,67	3,32	2,48	1,58	1,15	0,85	0,67	0,54	0,43	0,002
λ=1,5 μ=1,5	$M(\hat{\lambda})$	5,24	4,01	3,36	2,98	2,62	2,43	2,27	2,16	2,05	1,99	1,95	1,50
	$D(\hat{\lambda})$	11,88	9,28	7,13	5,40	3,73	2,88	2,21	1,74	1,29	1,17	0,90	0,004
	$M(\hat{\mu})$	5,33	4,03	3,35	2,98	2,63	2,43	2,27	2,16	2,05	2,00	1,95	1,50
	$D(\hat{\mu})$	12,15	9,46	6,95	5,38	3,80	2,89	2,15	1,72	1,32	1,15	0,93	0,004
λ=1,0 μ=1,5	$M(\hat{\lambda})$	3,93	2,83	2,30	1,94	1,75	1,59	1,49	1,43	1,36	1,32	1,27	0,94
	$D(\hat{\lambda})$	10,53	6,69	4,35	2,66	1,99	1,36	0,94	0,75	0,57	0,50	0,39	0,018
	$M(\hat{\mu})$	5,73	4,31	3,51	3,05	2,75	2,49	2,31	2,21	2,10	2,03	1,96	1,41
	$D(\hat{\mu})$	13,29	10,95	7,99	5,96	4,54	3,25	2,38	1,89	1,55	1,28	1,01	0,028
λ=1,5 μ=1,0	$M(\hat{\lambda})$	5,63	4,30	3,56	3,09	2,70	2,49	2,34	2,17	2,10	2,02	1,97	1,36
	$D(\hat{\lambda})$	13,21	11,02	8,17	6,08	4,36	3,28	2,60	1,86	1,50	1,21	1,04	0,047
	$M(\hat{\mu})$	3,86	2,82	2,27	1,96	1,73	1,59	1,50	1,40	1,36	1,31	1,29	0,94
	$D(\hat{\mu})$	10,28	6,63	4,12	2,71	1,84	1,41	1,01	0,70	0,60	0,47	0,39	0,01

оценки параметров методом максимального правдоподобия при рассмотренных выше параметрах исходного бета-распределения (*M*-математическое ожидание, *D*-дисперсия).

Из табл. 1 видно, что, действительно, для выборок с несимметричным распределением ($\lambda \neq \mu$) оценки параметров методом максимального правдоподобия оказываются смещенными даже при $n = 1000$.

Результатом метода двух начальных моментов является оценка по математическому ожиданию и дисперсии. Для бета-распределения с плотностью (1) математическое ожидание и дисперсия имеют, соответственно, вид [8, 10]

$$m = \frac{\lambda}{\lambda + \mu};\ s^2 = \frac{\lambda\mu}{(\lambda+\mu)^2(\lambda+\mu+1)}. \qquad (2)$$

Найдя по выборочным данным оценки $\hat{m}$ и $\hat{s}^2$, и, решая систему уравнений (2), можно определить оценки параметров $\hat{\lambda}$ и $\hat{\mu}$ бета-распределения (1).

В табл. 2 приведены результаты оценки параметров бета-распределения по оценкам математического ожидания и дисперсии.

Как видно из табл. 2, смещение оценок при малых выборках по данному методу намного ниже, чем у метода максимального правдоподобия.

Сущность обобщенного метода моментов [10] заключается в использовании для оценки параметров закона распределения, в отличие от известного метода моментов, не только прямых степенных, но и моментов других типов, например, логарифмических. Для этого необходимо прологарифмировать плотность распределения. Затем в полученном аналитическом выражении определить слагаемые, которые являются функциями случайных величин ($\varphi_1(x)$, $\varphi_2(x)$ и т.д.). Вид функциональных зависимостей определяет тип используемых моментов (степенной, логарифмический, экспоненциальный и т.д.) и их порядок.

Далее полученные аналитические выражения соответствующих моментов приравнивают к значениям соответствующих выборочных моментов. После чего оценки параметров распределения, как и в методе моментов, определяются в результате решения полученной системы уравнений. Количество уравнений в системе соответствует числу оцениваемых параметров.

В результате логарифмирования плотности (1) получены функции $y_1=\varphi_1(x)=\ln x$ и $y_2=\varphi_2(x)=\ln(1-x)$. После их усреднения имеем систему уравнений [10]

$$M[\ln x] = \frac{1}{n}\sum_{i=1}^{n}\ln x_i;$$

$$M\left[ln(1-x)\right] = \frac{1}{n}\sum_{i=1}^{n}\ln(1-x_i),$$

из решения которой находятся оценки параметров $\hat{\mu}$ и $\hat{\lambda}$.

Для оценки теоретических моментов необходимо определить плотности распределений случайных величин y_1 и y_2. Для этого введем в рассмотрение обратные функции $x_1 = e^{y_1}$ и $x_2 = 1 - e^{y_2}$. Тогда плотности распределений случайных величин y_1 и y_2 запишутся следующим образом [2]

$$g_1(y_1) = f\left(e^{y_1}\right)\left|\left(e^{y_1}\right)'\right| = \frac{1}{B(\lambda,\mu)}e^{\lambda y_1}\left(1-e^{y_1}\right)^{\mu-1}, \qquad (3)$$

Табл. 2. Результаты оценки параметров по математическому ожиданию и дисперсии

Параметры исходного бета-распределения	Оценки параметров	Объем выборки, *n*											
		2	3	4	5	6	7	8	9	10	11	12	1000
λ=1,0 μ=1,0	$M(\hat{\lambda})$	1,76	1,61	1,53	1,45	1,39	1,36	1,32	1,29	1,26	1,24	1,21	1,00
	$D(\hat{\lambda})$	1,10	0,94	0,80	0,69	0,61	0,54	0,48	0,43	0,37	0,35	0,31	0,002
	$M(\hat{\mu})$	1,77	1,61	1,53	1,46	1,38	1,35	1,32	1,29	1,26	1,24	1,21	1,00
	$D(\hat{\mu})$	1,11	0,94	0,82	0,72	0,60	0,54	0,49	0,43	0,39	0,35	0,31	0,002
λ=1,5 μ=1,5	$M(\hat{\lambda})$	2,00	1,92	1,90	1,86	1,84	1,82	1,82	1,80	1,78	1,76	1,75	1,50
	$D(\hat{\lambda})$	0,92	0,81	0,71	0,66	0,60	0,57	0,53	0,50	0,47	0,43	0,41	0,005
	$M(\hat{\mu})$	2,00	1,94	1,91	1,86	1,84	1,82	1,82	1,80	1,77	1,75	1,75	1,50
	$D(\hat{\mu})$	0,91	0,82	0,73	0,66	0,60	0,56	0,53	0,50	0,46	0,43	0,42	0,005
λ=1,0 μ=1,5	$M(\hat{\lambda})$	1,54	1,40	1,36	1,30	1,29	1,26	1,24	1,20	1,20	1,20	1,17	1,00
	$D(\hat{\lambda})$	0,98	0,75	0,62	0,52	0,45	0,41	0,36	0,31	0,29	0,26	0,24	0,002
	$M(\hat{\mu})$	2,21	2,08	2,03	1,97	1,93	1,89	1,87	1,83	1,82	1,80	1,78	1,50
	$D(\hat{\mu})$	0,91	0,89	0,82	0,77	0,71	0,66	0,61	0,58	0,55	0,52	0,49	0,005
λ=1,5 μ=1,0	$M(\hat{\lambda})$	2,21	2,10	2,01	1,98	1,95	1,88	1,87	1,84	1,80	1,80	1,78	1,50
	$D(\hat{\lambda})$	0,92	0,88	0,82	0,76	0,72	0,65	0,61	0,57	0,54	0,51	0,48	0,005
	$M(\hat{\mu})$	1,52	1,41	1,36	1,32	1,30	1,26	1,25	1,22	1,19	1,19	1,18	1,00
	$D(\hat{\mu})$	0,97	0,75	0,63	0,52	0,46	0,39	0,36	0,32	0,28	0,26	0,24	0,002

$$g_2(y_2) = f\left(1-e^{y_2}\right)\left|\left(1-e^{y_2}\right)'\right| = \frac{1}{B(\lambda,\mu)} e^{\mu y_2}\left(1-e^{y_2}\right)^{\lambda-1}. \quad (4)$$

Отсюда получаем обобщенные моменты

$$M_{y_1} = \frac{1}{B(\lambda,\mu)} \int_{-\infty}^{0} y_1 e^{\lambda y_1}\left(1-e^{y_1}\right)^{\mu-1} dy_1, \quad (5)$$

$$M_{y_2} = \frac{1}{B(\lambda,\mu)} \int_{-\infty}^{0} y_2 e^{\mu y_2}\left(1-e^{y_2}\right)^{\lambda-1} dy_2. \quad (6)$$

Решая систему уравнений

$$\begin{cases} M\left[\ln x\right] = M_{y_1}; \\ M\left[ln\left(1-x\right)\right] = M_{y_2} \end{cases} \quad (7)$$

относительно переменных μ и λ, получим оценки параметров $\hat{\mu}$ и $\hat{\lambda}$.

Результаты оценки параметров обобщенным методом моментов приведены в табл. 3.

Из табл. 3 видно, что, несмотря на заявленную в [10] «малую погрешность оценивания параметров распределений при малых выборках», для бета-распределения данный метод неприемлем для действительно малых ($n < 10$) выборок.

В последнее время находит применение бутстреп-метод оценки параметров [4]. Основная идея этого метода состоит в многократном извлечении случайным образом выборки заданного размера из исходной совокупности наблюдений и расчете по ним требуемых оценок с последующим осреднением. В табл. 4 приведены результаты оценки параметров бета-распределения бутстреп-методом.

Из табл. 4 видно, что бутстреп-метод для выборок малого объема дает также смещенный результат с достаточно большим рассеиванием.

Есть мнение [11], что в случае отклонения распределения от симметричного закона среднее значение использовать некорректно, так как оно является слишком чувствительным параметром к так называемым «выбросам». В этом случае для характеристики центральной тенденции в выборке должен применяться другой параметр – медиана. Медиана – это значение признака, справа и слева от которого находится равное число наблюдений (по 50%). Этот параметр (в отличие от среднего значения) устойчив к «выбросам» [11].

Медиана непрерывного распределения вероятностей M есть значение, удовлетворяющее соотношению [12]

$$F(M)=0{,}5,$$

где $F(x)$ – функция распределения генеральной совокупности.

Разумное приближение значения медианы бета-распределения для $\lambda,\mu \geq 1$ задается формулой [13]

$$M \approx \frac{\lambda - \frac{1}{3}}{\lambda + \mu - \frac{2}{3}}. \quad (8)$$

В табл. 5 приведены результаты оценки параметров бета-распределения по медиане и дисперсии аналогично системе уравнений (2), в которой вместо оценки математического ожидания используется оценка медианы (8).

Из табл. 5 видно, что оценки по медиане и дисперсии вместо математического ожидания и дисперсии дают

Табл. 3. Результаты оценки параметров обобщенным методом моментов

Параметры исходного бета-распределения	Оценки параметров	Объем выборки, n											
		2	3	4	5	6	7	8	9	10	11	12	1000
λ=1,0 μ=1,0	$M(\hat{\lambda})$	17,66	6,27	3,26	2,26	1,84	1,67	1,54	1,45	1,37	1,34	1,30	1,00
	$D(\hat{\lambda})$	870,56	204,55	46,59	10,76	4,32	2,09	1,61	0,98	0,64	0,56	0,46	0,0017
	$M(\hat{\mu})$	17,42	6,27	3,16	2,31	1,87	1,67	1,53	1,45	1,37	1,33	1,30	1,00
	$D(\hat{\mu})$	846,07	204,46	40,01	13,37	6,77	2,16	1,41	1,06	0,64	0,53	0,46	0,0017
λ=1,5 μ=1,5	$M(\hat{\lambda})$	20,58	8,56	4,94	3,48	2,87	2,54	2,95	2,19	2,07	1,99	1,94	1,50
	$D(\hat{\lambda})$	901,77	261,21	82,34	31,58	12,88	5,72	3,57	2,51	1,55	1,23	0,97	0,004
	$M(\hat{\mu})$	20,81	8,57	4,93	3,47	2,87	2,53	2,31	2,20	2,08	2,01	1,95	1,50
	$D(\hat{\mu})$	924,49	265,97	86,94	28,51	11,39	6,61	3,31	2,30	1,55	1,25	0,98	0,004
λ=1,0 μ=1,5	$M(\hat{\lambda})$	15,34	5,59	3,14	2,18	1,84	1,66	1,51	1,41	1,37	1,31	1,28	1,00
	$D(\hat{\lambda})$	643,93	147,67	36,20	8,53	4,10	2,29	1,14	0,77	0,64	0,51	0,40	0,002
	$M(\hat{\mu})$	23,54	9,11	5,11	3,52	2,94	2,63	2,34	2,21	2,13	2,03	1,98	1,50
	$D(\hat{\mu})$	1157	313,80	87,07	25,07	12,28	7,95	3,14	2,51	1,76	1,48	1,09	0,004
λ=1,5 μ=1,0	$M(\hat{\lambda})$	23,04	9,12	5,17	3,68	2,92	2,57	2,35	2,20	2,09	2,04	1,97	1,50
	$D(\hat{\lambda})$	1147	307,74	98,54	33,41	10,73	5,37	3,69	2,21	1,71	1,27	1,02	0,004
	$M(\hat{\mu})$	14,99	5,87	3,19	2,25	1,83	1,63	1,50	1,41	1,35	1,32	1,28	1,00
	$D(\hat{\mu})$	640,87	146,95	45,42	10,72	3,95	2,72	1,19	0,80	0,63	0,47	0,38	0,002

Табл. 4. Результаты оценки параметров бутстреп-методом

Параметры исходного бета-распределения	Оценки параметров	Объем выборки, n											
		2	3	4	5	6	7	8	9	10	11	12	1000
λ=1,0 μ=1,0	$M(\hat{\lambda})$	3,02	2,66	2,37	2,18	2,02	1,90	1,77	1,70	1,64	1,58	1,53	1,01
	$D(\hat{\lambda})$	3,51	3,25	2,92	2,57	2,28	2,01	1,74	1,53	1,38	1,22	1,08	0,005
	$M(\hat{\mu})$	3,04	2,65	2,36	2,15	2,01	1,88	1,77	1,69	1,65	1,56	1,52	1,01
	$D(\hat{\mu})$	3,51	3,24	2,91	2,53	2,25	1,97	1,73	1,51	1,38	1,16	1,06	0,004
λ=1,5 μ=1,5	$M(\hat{\lambda})$	3,33	3,06	2,88	2,70	2,59	2,51	2,43	2,33	2,27	2,23	2,19	1,51
	$D(\hat{\lambda})$	2,96	2,87	2,67	2,50	2,32	2,15	1,98	1,84	1,70	1,58	1,49	0,009
	$M(\hat{\mu})$	3,31	3,03	2,87	2,71	2,59	2,50	2,44	2,34	2,28	2,24	2,19	1,51
	$D(\hat{\mu})$	2,94	2,84	2,64	2,52	2,31	2,13	2,03	1,85	1,71	1,59	1,49	0,009
λ=1,0 μ=1,5	$M(\hat{\lambda})$	2,57	2,30	2,09	2,93	1,82	1,73	1,67	1,61	1,56	1,48	1,47	1,00
	$D(\hat{\lambda})$	3,26	2,75	2,34	2,00	1,71	1,51	1,34	1,19	1,05	0,88	0,84	0,004
	$M(\hat{\mu})$	3,68	3,38	3,11	2,90	2,78	2,61	2,53	2,46	2,39	2,30	2,25	1,51
	$D(\hat{\mu})$	2,83	2,99	2,92	2,85	2,69	2,48	2,32	2,20	2,01	1,85	1,72	0,010
λ=1,5 μ=1,0	$M(\hat{\lambda})$	3,72	3,36	3,12	2,91	2,76	2,66	2,54	2,44	2,37	2,30	2,24	1,51
	$D(\hat{\lambda})$	2,76	2,98	3,01	2,84	2,65	2,52	2,33	2,20	2,00	1,87	1,73	0,01
	$M(\hat{\mu})$	2,55	2,31	2,09	1,95	1,85	1,74	1,68	1,58	1,55	1,51	1,46	1,00
	$D(\hat{\mu})$	3,23	2,75	2,31	2,01	1,74	1,48	1,33	1,14	1,04	0,94	0,84	0,004

Табл. 5. Результаты оценки параметров по медиане и дисперсии

Параметры исходного бета-распределения	Оценки параметров	Объем выборки, n											
		2	3	4	5	6	7	8	9	10	11	12	1000
λ=1,0 μ=1,0	$M(\hat{\lambda})$	1,45	1,31	1,24	1,19	1,17	1,15	1,14	1,12	1,10	1,10	1,08	1,00
	$D(\hat{\lambda})$	1,22	0,98	0,81	0,66	0,57	0,51	0,44	0,39	0,34	0,32	0,28	0,002
	$M(\hat{\mu})$	1,46	1,32	1,25	1,20	1,16	1,15	1,13	1,13	1,11	1,10	1,09	1,00
	$D(\hat{\mu})$	1,24	0,98	0,82	0,68	0,57	0,50	0,44	0,40	0,35	0,32	0,29	0,002
λ=1,5 μ=1,5	$M(\hat{\lambda})$	1,68	1,62	1,62	1,60	1,61	1,61	1,61	1,59	1,60	1,60	1,58	1,50
	$D(\hat{\lambda})$	1,14	0,96	0,83	0,74	0,64	0,61	0,55	0,51	0,48	0,45	0,42	0,005
	$M(\hat{\mu})$	1,69	1,62	1,63	1,59	1,61	1,61	1,61	1,59	1,60	1,60	1,58	1,50
	$D(\hat{\mu})$	1,15	0,95	0,84	0,73	0,66	0,62	0,55	0,51	0,48	0,46	0,42	0,005
λ=1,0 μ=1,5	$M(\hat{\lambda})$	1,32	1,23	1,19	1,16	1,17	1,14	1,14	1,12	1,12	1,11	1,12	1,02
	$D(\hat{\lambda})$	0,98	0,74	0,58	0,50	0,44	0,39	0,33	0,31	0,28	0,26	0,24	0,003
	$M(\hat{\mu})$	1,84	1,72	1,69	1,64	1,67	1,63	1,65	1,62	1,61	1,60	1,62	1,50
	$D(\hat{\mu})$	1,29	1,12	0,98	0,86	0,78	0,70	0,66	0,60	0,55	0,51	0,48	0,005
λ=1,5 μ=1,0	$M(\hat{\lambda})$	1,84	1,73	1,69	1,66	1,65	1,64	1,62	1,63	1,61	1,61	1,61	1,50
	$D(\hat{\lambda})$	1,30	1,12	1,00	0,88	0,78	0,72	0,65	0,60	0,55	0,52	0,49	0,005
	$M(\hat{\mu})$	1,30	1,23	1,19	1,17	1,15	1,14	1,14	1,13	1,11	1,11	1,11	1,02
	$D(\hat{\mu})$	0,94	0,74	0,59	0,51	0,42	0,39	0,34	0,33	0,27	0,26	0,24	0,003

менее смещенный результат для выборок малого объема даже в случае симметричного распределения. Хотя являются и менее эффективными из-за бóльшего рассеивания. На рис. 2 и 3 приведены графики зависимостей оценок математического ожидания $M(n)$ и дисперсии $D(n)$ параметра λ бета-распределения от объема n используемых для этого выборок, реализованных рассмотренными выше методами, для случая λ=1,5 и μ=1,0.

Из рис. 2 и 3 видно, что наименее удачным для выборок малого (n<10) объема является обобщенный метод моментов. Оценки параметров методом максимального правдоподобия действительно дают сильно смещенный результат для выборок малого объема [5]. При этом и дисперсия оценки параметра является высокой по сравнению с остальными методами. Так, при параметрах λ=μ=1,5 и объеме выборки n=2 в одной реализации слу-

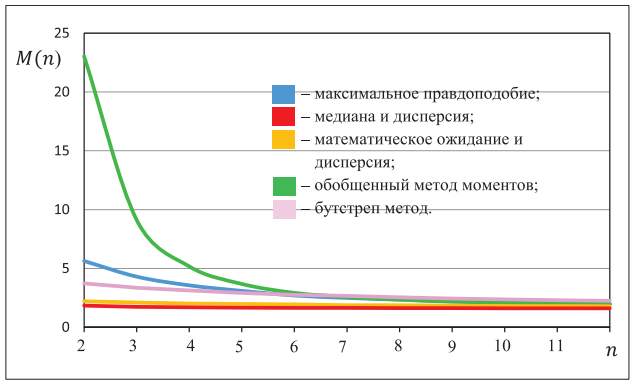


Рис. 2. Графики оценок математического ожидания параметра λ

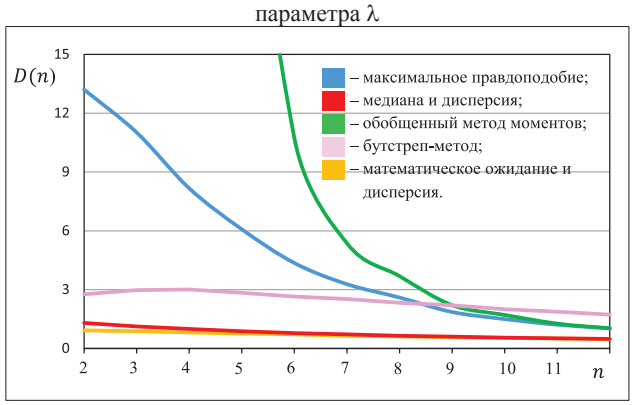


Рис. 3. Графики оценок дисперсии параметра различными методами

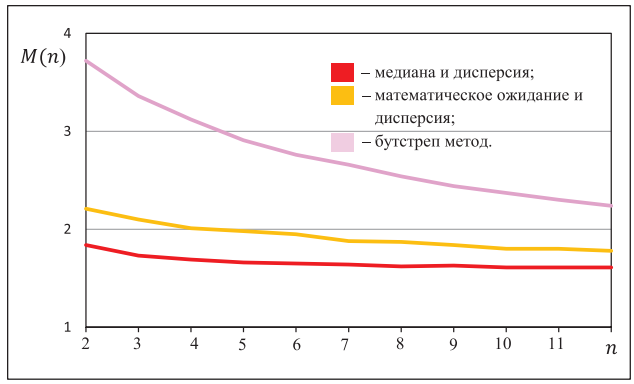


Рис. 4. Графики оценок математического ожидания параметра λ тремя методами

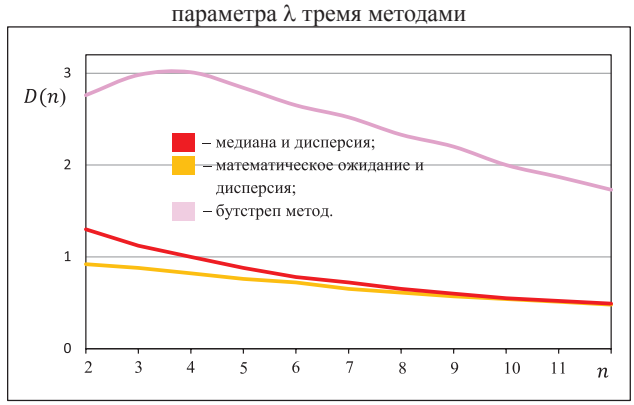


Рис. 5. Графики оценок дисперсии параметра тремя методами

чайные величины бета-распределения приняли значения X_1=0,36 и X_2=0,69. Методом максимального правдоподобия оценки параметров при этом составили $\hat{\lambda} = 4,6$ и $\hat{\mu} = 4,1$. В то время, как оценки по медиане и дисперсии $\hat{\lambda} = 1,7$ и $\hat{\mu} = 1,6$ представляются более адекватными.

На рис. 4 и 5 для наглядности приведены графики тех же зависимостей без метода максимального правдоподобия и обобщенного метода моментов, как наиболее грубых для выборок объемом n<10.

Из рис. 4 и 5 видно, что наиболее близкими к исходным значениям являются оценки по медиане и дисперсии. Однако наименьшей дисперсией обладают оценки по математическому ожиданию и дисперсии.

Таким образом, наиболее приемлемыми оценками параметров несимметричных бета-распределений по малой выборке являются оценки по математическому ожиданию (или медиане) и дисперсии.

2. Результат

Наименее удачным для выборок малого (n<10) объема является обобщенный метод моментов. Оценки параметров методом максимального правдоподобия действительно дают сильно смещенный результат для выборок малого объема [5]. При этом, и дисперсия оценки параметра является высокой по сравнению с остальными методами. Так, при параметрах λ=μ=1,5 и объеме выборки n=2 в одной реализации случайные величины бета-распределения приняли значения X_1=0,36 и X_2=0,69. Методом максимального правдоподобия оценки параметров при этом составили $\hat{\lambda} = 4,6$ и $\hat{\mu} = 4,1$. В то время, как оценки по медиане и дисперсии $\hat{\lambda} = 1,7$ и $\hat{\mu} = 1,6$ представляются более адекватными.

Оценки по двум начальным моментам ожидаемо практически совпадают с оценками по математическому ожиданию и дисперсии т.к. последние явно выражаются через первые два начальных момента.

Бутстреп-метод, по сравнению с методом максимального правдоподобия, дает менее смещенные оценки с меньшей дисперсией. Таким образом, наиболее приемлемый (близкий к исходным значениям) результат получен с использованием математического ожидания (или медианы) и дисперсии.

Заключение

В результате исследования выявлено, что для выборок малого объема вряд ли можно рекомендовать какой-либо конкретный способ оценки параметров. Наиболее целесообразным представляется нейросетевой анализ малых выборок [15]. С помощью нейросетевого объединения нескольких способов оценки можно существенно улучшить ее точность.

Список литературы

1. Воловик А.В. Комбинаторный способ идентификации малой выборки// Надежность. 2024. № 2. С. 3-7. DOI: 10.21683/1729-2646-2024-24-2-3-7

2. Джонсон Н., Лион Ф. Статистика и планирование эксперимента в технике и науке. Методы обработки данных / Под ред. Э.К. Лецкого. М.: Мир, 1980. 610 с.

3. Гаскаров Д.В., Шаповалов В.И. Малая выборка. М.: Статистика, 1978. 248 с.

4. Орлов А.И. Эконометрика. М.: Экзамен, 2002. 410 с.

5. Попукайло В.С. Поддержка принятия решений по пассивным выборкам малого объема / Дисс. доктора информатики. УДК 004.415.2. Кишинев, 2017. 168 с.

6. Джонсон Н.Л. Одномерные непрерывные распределения: в 2 ч. Ч. 2. М.: БИНОМ. Лаборатория знаний, 2010-2012. 600 с.

7. Лемешко Б.Ю., Блинов П.Ю. Критерии проверки отклонения распределения от равномерного закона. Руководство по применению. Новосибирск: НГТУ, 2015. 182 с.

8. Корн Г., Корн Т. Справочник по математике. Для научных работников и инженеров. М.: Наука, 1974. 832 с.

9. Вадзинский Р.Н. Справочник по вероятностным распределениям. СПб.: Наука, 2001. 295 с.

10. Громов Ю.Ю., Карпов И.Г. Законы распределения непрерывной случайной величины с максимальной энтропией. Обобщенный метод моментов // Научно-технические ведомости СПбГПУ 1. 2009. С. 37-41.

11. Реброва О. Среднее или все же медиана // «Троицкий вариант». 2011. № 90. с. 13.

12. ГОСТ Р 50779.24-2005 (ИСО 8595:1990) Статистические методы. Статистическое представление данных. Оценка медианы. М.: Стандартинформ, 2005. II, 6 с.

13. Керман, Джуни (2011). «Аппроксимация в замкнутой форме для медианы бета-распределения»[электронный ресурс]. URL: https://arxiv.org/abs/1111.0433 (дата обращения: 29.9.2025).

14. Лемешко Б.Ю., Гильдебрант С.Я., Постовалов С.Н. К оцениванию параметров надежности по цензурированным выборкам // Заводская лаборатория. Диагностика материалов. 2001. Т. 67. № 1. С. 52-64.

15. Волчихин В.И. и др. Нейросетевой анализ нормальности малых выборок биометрических данных с использованием хи-квадрат критерия и критериев Андерсона-Дарлинга // Инженерные технологии и системы. 2019. Том 29. № 2. С. 205-217.

References

1. Volovik A.V. A combinatorial method of small sample identification. *Dependability* 2024;24(2):3-7. (in Russ.). DOI: 10.21683/1729-2646-2024-24-2-3-7

2. Johnson N., Leone F. Statistics and Experimental Designs and Engineering and the Physical Sciences. Mathods of Data Processing. Moscow: Mir; 1980.

3. Gaskarov D.V., Shapovalov V.I. [Small sample]. Moscow: Statistika; 1978. (in Russ.)

4. Orlov A.I. [Econometrics]. Moscow: Examen; 2002. (in Russ.)

5. Popukailo V.S. [Decision support for small-size passive samples]. A Doctor of Computer Science dissertation. UDC 004.415.2. Chisinau; 2017. (in Russ.)

6. Johnson N.L. Continuous Univariate Distributions: in 2 volumes. Volume 2. Moscow: BINOM. Laboratoriya znaniy; 2010-2012.

7. Lemeshko B.Yu., Blinov P.Yu [Criteria for testing a distribution for deviation from a uniform law. An application guide]. Novosibirsk: NSTU; 2015. (in Russ.)

8. Korn G., Korn T. Mathematical handbook. Moscow: Nauka; 1974.

9. Vadzinsky R.N. Handbook of Probability Distributions. St. Petersburg: Nauka; 2001. (in Russ.)

10. Gromov Yu.Yu., Karpov I.G. [Distribution laws of a continuous random variable with maximum entropy. Generalized method of moments]. *Nauchno-tekhnicheskie vedomosti SPBGPU 1* 2009:37-41. (in Russ.)

11. Rebrova O. [Average or median though]. *Troitsky variant* 2011;90:13. (in Russ.)

12. GOST R 50779.24-2005 (ISO 8595:1990): Interpretation of statistical data. Estimation of a median. Moscow: Standartinform; 2005. (in Russ.)

13. Kerman J. A closed-form approximation for the median of the beta distribution. (accessed 29.9.2025). Available at: https://arxiv.org/abs/1111.0433.

14. Lemeshko B.Yu., Hildebrant S.Ya., Postovalov S.N. [On the assessment of reliability parameters based on censored samples]. *Industrial Laboratory. Diagnostics of Materials* 2001;67(1):52-64. (in Russ.)

15. Volchikhin V.I. et al. The neural network analysis of normality of small samples of biometric data through using the Chi-square test and Anderson–Darling criteria. *Inzhenernyye tekhnologii i sistemy* 2019;29(2):205-217. (in Russ.)

Сведения об авторе

Воловик Александр Васильевич – кандидат технических наук, ведущий инженер-конструктор АО «ОДК-Климов». Адрес: д. 16 корп. А, кв.128, ул. Центральная, пос. Шушары, тер. Детскосельский, Санкт-Петербург, Российская Федерация, 196634, тел. 8-951-651-83-39, e-mail: volovik_aleksandr@mail.ru.

About the author

Alexander V. Volovik, Candidate of Engineering, Lead Design Engineer, JSC "UEC-Klimov". Address: 16 bldg. A, apt. 128, Tsentralnaya, Shushary, ter. Detskoselsky, Saint Petersburg, 196634, Russian Federation, tel. 8 (951) 651 83 39, e-mail: volovik_aleksandr@mail.ru.

Вклад автора в статью

Исследование проведено автором самостоятельно в полном объеме.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

1980

Разрабатывается автоматизированная система роспуска грузовых вагонов на сортировочных горках КГМ РИИЖТ.

1990

Внедрение автоматизированных информационных систем АСОУП, ДИСПАРК, ДИСТПС, «Грузовой экспресс», новые системы локомотивной сигнализации для скоростного движения АЛС-ЕН.

1960

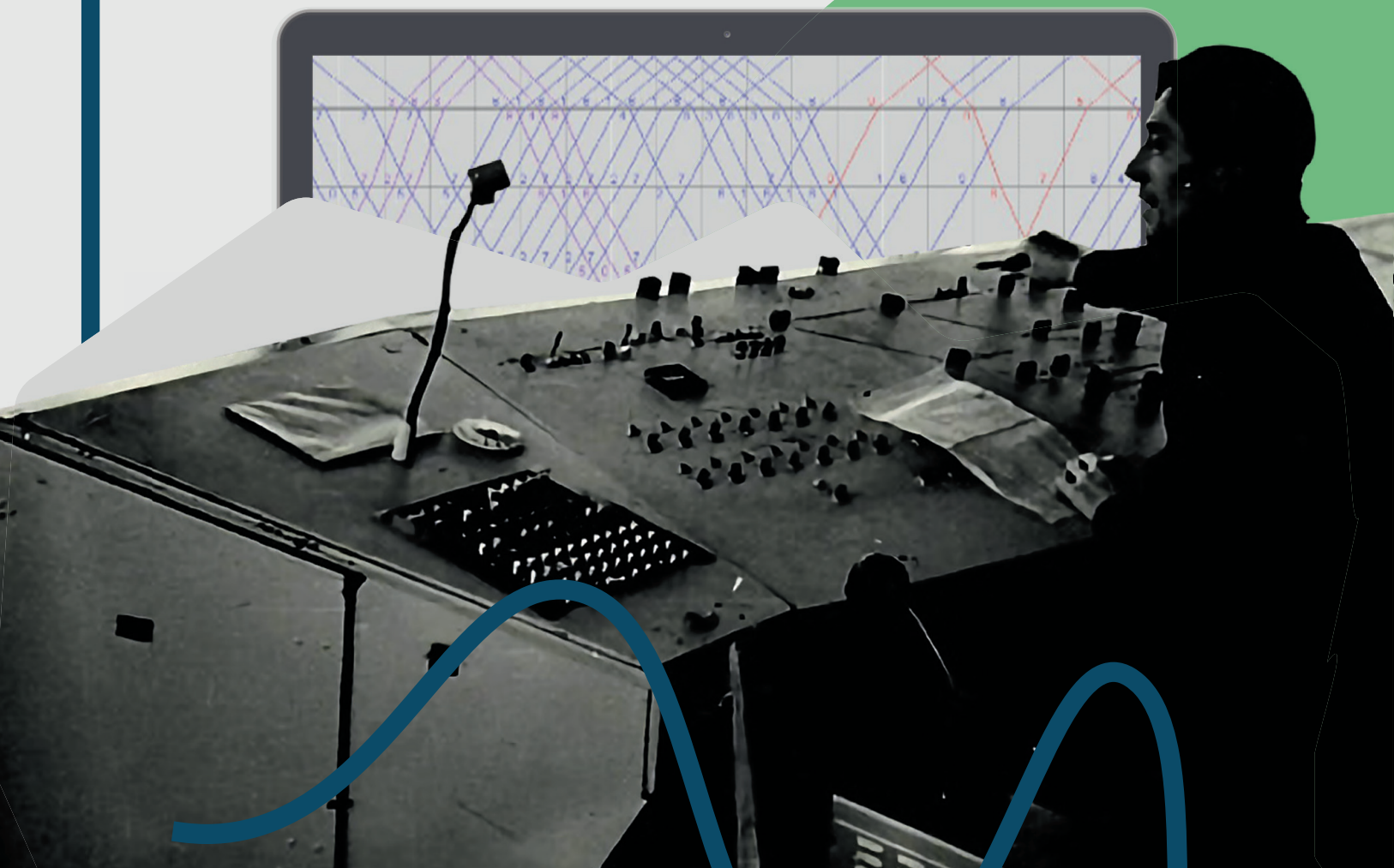
Разработаны и внедрены отечественные системы автоматической локомотивной сигнализации.

1956

14 февраля 1956 года Министр путей сообщения СССР Б.П. Бещев подписал приказ о создании Конструкторского бюро Главного управления сигнализации и связи (КБ ЦШ).

1970

Создание устройств диспетчерской централизации, сигнализации и автоблокировки. Развитие направления автоматизации технологических процессов.



2000

Достижения в сфере создания бортовых устройств безопасности для тягового, моторвагонного и специального подвижного состава. Началось массовое внедрение систем КЛУБ, КЛУБ-У, КЛУБ-П.

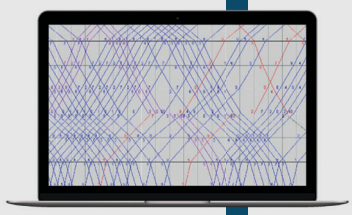
НИИАС

2010

Старт разработок в области комплексной интеллектуальной системы управления железнодорожным транспортом (ИСУЖТ). Решение локальных функциональных задач: анализ надежности, управление рискамии ресурсами.

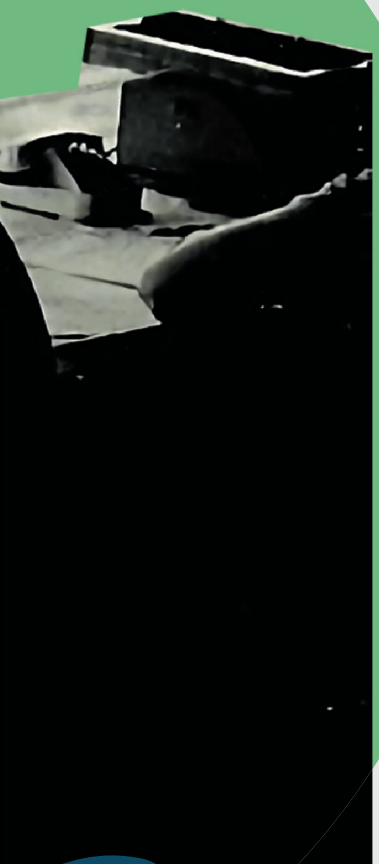
2020

Внедрение цифровых решений в области железнодорожного транспорта. Развитие систем интервального регулирования движением поездов. Разработка беспилотного управления поездами и бортовых систем безопасности.



2025

Внедрение единой программно-аппаратной экосистемы, включающей новейшие средства автоматизации, механизации и роботизации.



niias.ru

vniias_official

УДК 004.891.2
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-38-42

Надежность информации
Reliability of information

Цветков В.Я.[1] *проф., д.т.н.*
Tsvetkov V.Ya.[1] *Professor, Doctor of Engineering*

[1] *АО «НИИАС» – ведущий отраслевой научно-технологический институт холдинга «РЖД» в области автоматизации и управления сложными технологическими процессами на железнодорожном транспорте, Москва, Россия. Начальник отдела. tsvetkov-vy@rut-miit.ru. ORCID 0000-0003-1359-9799*
[1] *JSC NIIAS is JSC RZD's lead research and development institute that specialises in the automation and management of complex industrial processes in railway transportation, Moscow, Russia. Head of Unit. ORCID 0000-0003-1359-9799 tsvetkov-vy@rut-miit.ru*


Цветков В.Я.

Резюме. *Несмотря на широкое применение информации и информационного моделирования, надежность информации пока мало исследована.* **Цель.** *Предложен метод анализа надежности информации как нового вида надежности. Построена модель параметров надежности информации.* **Методы.** *В статье применяются методы категориального качественного и сравнительного анализа.* **Результаты.** *В результате исследования определены специфические характеристики надежности информации, отличающие ее от других видов надежности.* **Заключение.** *Предлагаемый подход анализа надежности информации позволяет повысить качество и надежность информационных процессов и повысить надежность результатов информационной обработки.*
Abstract. *Despite the widespread use of information and information modeling, the reliability of information has not yet been thoroughly studied.* **Aim.** *The paper suggests a method for analysing the reliability of information as a new type of reliability. A model of information reliability parameters has been defined.* **Methods.** *The paper uses methods of categorical qualitative and comparative analysis.* **Results.** *The research has defined special features of the reliability of information that distinguish it from other types of reliability.* **Conclusion.** *The proposed method of analysing the reliability of information allows improving the quality and reliability of information processes and the reliability of information processing results.*

Ключевые слова: *надежность информации, валидность, достоверность информации, процессуальная надежность, семантическая надежность.*
Keywords: *reliability of information, validity, fidelity of information, procedural reliability, semantic reliability.*

Для цитирования: *Цветков В.Я. Надежность информации // Надежность. 2025. №4. С. 38-42. https://doi.org/10.21683/1729-2646-2025-25-4-38-42*
For citation: *Tsvetkov V.Ya. Reliability of information. Dependability 2025;4: 38-42. https://doi.org/10.21683/1729-2646-2025-25-4-38-42*

Поступила: *10.06.2025* / **После доработки:** *11.06.2025* / **К печати:** *28.09.2025*
Received on: *10.06.2025* / **Revised on:** *11.06.2025* / **For printing:** *28.09.2025*

Введение

Надежность информации или «информационная надежность» является новой постановкой задачи исследования надежности. Надежность информации качественно отличается от надежности изделий и продукции. В российской литературе термин «надежность информации» мало употребляют и иногда заменяют термином «достоверность информации». За рубежом, наоборот, «надежность информации» обсуждаемый и анализируемый термин [1–3]. ГОСТ 27.002-2015 [4] дает общее определение надежности. Он определяет ее не как характеристику, а как свойство. Это свойство заключается в способности объекта «выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования» [4]. Здесь есть качественное различие. Характеристика – это независимое понятие и, в отдельных случаях, существительное. Свойство есть атрибут, привязанный к другому объекту, и существующий только в связке с этим объектом. Термину надежность в ГОСТе [4] сопоставляется термин «dependability». Для обозначения надежности в зарубежной литературе чаще применяют и другой термин «reliability». В то же время словосочетание «dependability and reliability» переводят как «надежность и безотказность». То есть налицо не полное соответствие зарубежных аналогов отечественным.

1. Виды надежности

Прежде чем исследовать надежность информации, целесообразно рассмотреть виды надежности и их особенности. В России различают надежность в технике [3, 4] и надежность строительных конструкций [6]. Оба вида надежности не применимы к оценке надежности информации. Методически выделяют два вида надеж-

ности – надежность как устойчивость и надежность как внутренняя согласованность. Эти подходы близки к оценке надежности информации. Относительно близкой к надежности информации является надежность экспертного оценивания, в частности, экспертного оценивания в медицине [7, 8]. Исследование надежности медицинских тестов позволяет выделить два вида надежности: процессуальная модель надежности теста как процесса; надежность результатов тестирования или субстанциональная модель надежности. В сфере образования также применяют тестирование, для которого применимы эти оценки. Анализ надежности тестирования в медицине близок к анализу надежности тестирования в образовании. Тестирование можно рассматривать как вид информационного моделирования. В области тестирования выделяют следующие виды надежности:

1. «Межэкспертная надежность» оценивает степень согласия между двумя или более экспертами в их оценках [9]. В сфере информации это оценка степени соответствия между разными сообщениями;

2. «Надежность повторного тестирования» оценивает степень, в которой результаты теста совпадают от одного тестового задания к другому. Данные собираются от общего тестового задания, которое использует одинаковые методы и сходные условия тестирования [10]. Это включает в себя надежность внутри тестового задания. В сфере информации это оценка степени комплементарности частных тестов;

3. «Межметодная надежность» оценивает степень согласованности результатов тестов при наличии различий в используемых методах или инструментах. Это позволяет исключить межэкспертную надежность. При работе с тестовыми формами ее называют надежностью параллельных форм [11]. В сфере информации это сравнительная оценка разных методов;

4. «Надежность внутренней согласованности» оценивает согласованность результатов отдельных частных тестов в рамках интегрального теста [11]. В сфере информации это оценка комплементарности тестирования;

5. Временная надежность или актуальность. Это типичный вид информационной надежности. Для информации характерно старение и потеря соответствия информации изменяющимся условиям реального мира. Поэтому оценка временной надежности данных и информации соответствует характеристике «актуальность». Актуальная информация – надежная информация;

6. Когнитивная надежность тестирования или информационного моделирования. Участие эксперта в тестировании или в любом экспертном оценивании сопровождается влиянием когнитивных или антропогенных факторов, которые вносит эксперт. Когнитивная надежность тестирования оценивается логикой эксперта, включая когнитивную логику [12]. Когнитивная логика зависит от уровня интеллекта субъекта или объекта, осуществляющего тестирование, моделирование или экспертное оценивание [13, 14].

Хотя надежность информации не подразумевает валидность содержания информации, она накладывает ограничение на общую валидность теста [7, 8]. Валидность связана с семантикой, то есть с достоверностью информации. В аспекте информации это требование надежности данных. При этом возникает двойственность: валидность данных и валидность теста. В аспекте надежности возникает тройственность; надежность данных; надежность тестирования (процессуальная надежность), надежность результата тестирования.

Известен пример из тестирования МФЮА, где оператор, готовивший тесты, сбил ответы после 185 вопроса из 440 применявшихся в тестировании. В результате правильные ответы студентов на вопросы после 185 были квалифицированы как неправильные. Здесь имело место частичная потеря валидности данных. Надежность тестирования не изменилась. Но результат тестирования стал не валидный и не надежный. Этого бы удалось избежать, если бы тестирование проводил специалист, который мог бы обнаружить ошибку в тестовом ответе. Но нынешняя тенденция тестирования направлена на то, что тестирование по физике может принимать преподаватель по астрономии или по физкультуре, лишь бы он умел читать.

Общий вывод: надежный в процессуальном отношении тест может дать не валидный и не надежный результат при не валидных исходных данных. Другими словами, надежность теста не обеспечивает надежность результата при не валидных и не надежных данных. Такая ситуация характерна для информационного поля. Надежный информационный продукт может дать не надежный результат при не валидности исходных данных

Тест, как процесс, который является процессуально абсолютно надежным, может быть не валидным как средство измерения характеристик человека. В то же время тест, который не является надежным, не может быть валидным [15]. Например, если весы последовательно измеряют вес объекта на 100 граммов больше истинного веса, то взвешивание (процессуальная надежность) будут надежными, но результаты не будут валидными (поскольку возвращаемый вес не является истинным весом – не валидный). Чтобы весы были валидными, они должны определять истинный вес объекта и пройти эталонирование. Этот пример показывает, что совершенно надежная процессуальная мера не обязательно является валидной, если она не калибрована и не эталонирована. Калибровка или эталонирование процесса создает валидность результата при надежном инструментарии.

Основной отправной точкой для многих теорий надежности тестов является идея о том, что тестовые показатели отражают влияние двух видов факторов [15]:

1. Факторы, характеризующие стабильность: стабильные характеристики индивидуума или атрибута, которые измеряют;

2. Факторы, характеризующие изменчивость: характеристики объекта, личности или ситуации, которые могут повлиять на результаты теста, но не имеют ничего общего с измеряемым атрибутом.

Важными для измерений и тестирования являются факторы первого типа. Эти факторы включают:

– временные общие характеристики;
– временные частные характеристики;
– характеристики, не зависящие от времени;
– характеристики ситуации, то есть окружения объекта или условия процесса;
– факторы случайности, то есть помехи или фон.

2. Надежность и валидность

Надежность и валидность в данном разделе рассматриваются с позиций тестирования и надежности информации. Надежность измерений не подразумевает валидность результата. Можно точным измерительным прибором получить не валидный результат, если измеряется, например, не тот участок, какой необходимо, а соседний. Валидность результата можно трактовать как семантическую надежность. Для информации это специальный вид надежности, который в технических средствах не встречается. Наличие систематической ошибки прибора дает не правильный, а смещенный результат. Другими словами, процессуальная надежность не гарантирует валидность и равнозначна семантической надежности. Например, надежная мера, которая последовательно измеряет что-то, не обязательно измеряет то, что должно измеряться. Существует множество надежных тестов определения способностей человека. Но не все они будут валидны для прогнозирования производительности труда человека. В силу этого при тестировании субъектов определяют надежность и валидность.

При исследовании инструментария (метода) оценки некого фактора, инструмента сбора данных или технологии предоставления услуг характеристики валидности и надежности обычно используют для обоснования этого инструментария. Валидный инструментарий измеряет правильные значения (семантику). Надежный инструментарий – это тот, который в одних и тех же условиях дает одинаковый результат. Валидный инструментарий обеспечивает точность или достоверность семантики. Надежный инструментарий обеспечивает повторяемость процесса. Эти две характеристики дополняют друг друга и обеспечивают надежность измерений и вычислений.

Валидность и надежность можно оценить разными способами. Различают следующие виды валидности информации: конструктивная, контентная, функциональная, критериальная, семантическая. *Конструктивная валидность* имеет место для ситуации, в которой практические тесты, выведенные из теории, используются для измерения некоторой модели или информационной конструкции, которая определяется этой теорией. Конструктивная валидность важна при оценке модели, которую нельзя наблюдать напрямую, например, интеллект. Вместо этого надо построить теорию о том, как целевая переменная модели, которую надо измерить, будет взаимодействовать с другими переменными. Конструктивную валидность можно оценить с помощью матрицы признаков и методов, факторного анализа и моделирования структурных уравнений, среди прочих статистических подходов.

Контентная валидность информации имеет аналогом термин «репрезентативная выборка». Она обычно оценивается путем определения того, охватывает ли тест (используемая информация) репрезентативную выборку целевой области, которую предполагается измерить или оценить. Например, можно опросить 20 отличников по предметам и 100 троечников. По объему вторая выборка более представительна, но не имеет контентную валидность. Контентная валидность оценивается путем привлечения экспертов по предметной области для оценки тестовых элементов в соответствии с целями тестирования или моделирования.

Функциональная валидность – это оценка того, выполняет ли тест или инструментарий заданные функции. Эта валидность оценивается путем привлечения экспертов, разбирающихся в функциональных возможностях теста.

Сравнительная валидность сравнивает результаты одного инструментария с результатами другого инструментария, который известен как валидный (эталон). Существуют и другие нюансы определения валидности, а также ряд типов валидности, которые связаны с тем, насколько хорошо разработаны научные исследования, но они выходят за рамки обсуждения в этой статье.

Семантическая валидность оценивается как соответствие содержательности данных требованиям решаемой задачи. Например, при измерении площадей единицы измерения должны иметь размерность площади, а не объема. При ретроспективном анализе данные, за прошедшие 10 лет могут быть не валидны, а валидны данные за последние 3 года.

3. Терминологические отношения.

Одной из проблем анализа надежности информации является полисемия значений информации и многозначность толкования английских терминов. Валидность информации связана с такой характеристикой, как и достоверность информации. Для технических средств такая характеристика исключается.

Термину «валидность» ставят в соответствие ряд родственных терминов, большинство из которых не столько синонимы, сколько сопутствующие или связанные термины: soundness (обоснованность); reasonableness (разумность); rationality (рациональность); logical (логичность); justifiability (оправданность); defensibility (защищенность); sustainability (устойчивость); plausibility (правдоподобность); viability (жизнеспособность); bona fides (добросовестность); effectiveness (эффективность); cogency (убедительность); credibility (достоверность доверие); believability (правдоподобность); force (сила); strength (прочность); weight (вес); foundation (основание); substance (субстанциональность); substantiality (существенность); authority (авторитетность); reliability (надежность).

Иногда термин «валидность» употребляют в смысле достоверности. Однако достоверность, кроме валидности, имеет другие значения: reliability (надежность, достоверность, прочность); authenticity (подлинность, достоверность); veracity (правдивость, достоверность, точность, правдивое высказывание).

Поэтому достоверность информации во многих случаях соответствует валидности информации.

О достоверности информации говорят меньше, чем о достоверности данных [3, 16].

Терминологические проблемы надежности информации связаны с тем, что английский термин «Reliability» переводится на русский язык и как «надежность», и как «достоверность». При обратном переводе достоверность чаще всего переводится как Reliability. В то же время в английском есть близкие термины authenticity «подлинность», и veracity «правдивость». Эти проблемы обусловлены недостаточной стандартизацией терминологии в русскоязычной литературе.

4. Особенности надежности информации и ее отличия от других видов надежности.

В ГОСТе [4] дается перечень объектов, о которых идет речь в определении надежности: от сборочной единицы до программного обеспечения и персонала. Информация в этот перечень не входит. Общей характеристикой объектов является возможность функционирования и характеристика наработки на отказ. Для информации характеристика наработки на отказ не применима.

В аспекте исследования надежности информации можно рассмотреть такие виды: процессуальную надежность, надежность результата, надежность исходных данных. Надежность результата можно интерпретировать как семантическую надежность. Надежность исходных данных трактуют как достоверность данных.

Обобщенной характеристикой информации является описание и способность информирования, то есть передачи сведений. Особенностью информации является полисемия и наличие более 30 видов информации (генетическая; компьютерная; вербальная; СМИ; информация, которую передают насекомые; информация, которую передают растения друг другу или насекомым; другие виды информации [17].

Надежность информации отличается от надежности информационных систем. Информация в чистом виде не существует, а имеет представления в виде сообщения, в виде информационного потока, в виде описания или документа. Для надежности информации не применимо понятие «наработка на отказ», что свойственно надежности технических средств. Для надежности информации применимы понятия: актуальность, достоверность, дискретность, помехозащищенность, которые не применимы для описания надежности технических средств.

Надежность информации снижается при появлении информационных семантических разрывов. Семантический разрыв можно трактовать как вид информационной неопределенности. Информационная неопределенность объективная характеристика информации, которая отсутствует в технических изделиях и проектах.

Семантический разрыв [18] означает качественное различие между содержательными описаниями объекта в разных формальных представлениях. Например, описание на естественном языке и описание на формальном языке (логика); описание на естественном языке и формульное представление [19]. Также неточный перевод с одного языка на другой является семантическим разрывом. В информатике семантический разрыв соответствует ситуации, когда наблюдения и задачи передаются в вычислительную среду с потерей содержательности. «Семантический разрыв» означает либо потерю логической последовательности процесса в рассуждениях (потеря процессуальной надежности), либо уменьшение или существенное исключение смысловой содержательности модели или сообщения при их преобразовании (потеря семантической надежности).

Заключение

Надежность информации качественно отличается от надежности технических объектов и даже от надежности программного обеспечения. Понятие «надежность информации», также как понятие «информация», является полисемическим. Существует много видов надежности информации, которые дополняют друг друга. Надежность информации не является одной характеристикой, а представляет собой совокупность различных видов надежности. Некоторые виды надежности информации имеют прямые синонимы. Например, временная надежность информации может трактоваться как актуальность. Надежность содержательности информации может трактоваться как семантическая надежность. Надежность содержательности информации при дискретизации может трактоваться как надежность по информативности. Надежность визуальных моделей может трактоваться как надежность представления визуальной информации. Надежность информации, получаемой при тестировании, связана с когнитивными факторами и когнитивной логикой. Надежность информации снижается при наличии семантических разрывов. Надежность информации является новым видом надежности и требует дальнейших исследований.

Список литературы

1. Weikum G. Towards guaranteed quality and dependability of information services // Datenbanksysteme in Büro, Technik und Wissenschaft: 8. GI–Fachtagung Freiburg im Breisgau, 1-3. März 1999. Springer Berlin Heidelberg, 1999. Pp. 379-409.

2. Distefano S., Puliafito A. Information dependability in distributed systems: The dependable distributed storage system // Integrated Computer-Aided Engineering. 2014. Vol. 21. No. 1. Pp. 3-18.

3. Ceolin D. et al. Assessing trust for determining the reliability of information. In: Situation awareness with systems of systems. Pp. 209-228. Springer New York, 2013.

4. ГОСТ 27.002-2015. Надежность в технике. Термины и определения. М.: Стандартинформ, 2016. IV, 24 с.

5. ГОСТ Р 27.102-2021. Надежность в технике. М.: Российский институт стандартизации, 2021. IV, 36 с.

6. ГОСТ 27751-2014. Надежность строительных конструкций. М.: Стандартинформ, 2015. II, 14 с.

7. Fitzner K. Reliability and validity a quick review // The Diabetes Educator. 2007. Vol. 33. No. 5. Pp. 775-780.

8. Cohen L., Manion L., Morrison K. Validity and reliability // Research methods in education. Routledge, 2017. Pp. 245-284.

9. Durand V.M., Barlow D.H. Essentials of abnormal psychology. Wadsworth/Thomson Learning, 2003.

10. Gaski J.F. Introducing the Marketing Accountability Standards Board (MASB) and its Common-Language Marketing Dictionary: Background, Description, Vision, and Prospects // Journal of Macromarketing. 2021. Vol. 41. No. 4. Pp. 521-526.

11. Zhu W. Reliability: What type, please! // Journal of Sport and Health Science. 2013. Vol. 2. No. 1. Pp. 62-64.

12. Savnykh V.P., Tsvetkov V.Ya. Cognitive logic's principles. В сб.: Artificial Intelligence in Intelligent Systems. Proceedings of Computer Science On-line Conference. Сер. "Lecture Notes in Networks and Systems". Zlín, Czech Republic, 2021. С. 288-296.

13. Kudzh S.A., Tsvetkov V.Ya. Cognitive expert assessment // В сб.: Artificial Intelligence in Intelligent Systems. proceedings of Computer Science On-line Conference. Сер. "Lecture Notes in Networks and Systems". Zlín, Czech Republic, 2021. С. 742-749.

14. Tsvetkov V.Ya. Cognitive Science of Information Retrieval // European Journal of Psychological Studies. 2015. Vol. 1(5). Pp. 37-44.

15. Davidshofer K.R., Murphy C.O. Psychological testing: principles and applications. Pearson, 2005. P. 624.

16. Berti-Equille L., Borge-Holthoefer J. Veracity of Data. Springer Nature, 2022.

17. Иванников А.Д., Тихонов А.Н., Цветков В.Я. Основы теории информации. М.: МАКС Пресс, 2007. 356 с.

18. Tsvetkov V.Ya. Information Interaction as a Mechanism of Semantic Gap Elimination // European researcher. 2013. Vol. 4-1(45). Pp. 782-786.

19. Чехарин Е.Е. Когнитивное моделирование как метод устранения семантического разрыва // Образовательные ресурсы и технологии. 2016. № 1(13). С. 103-109.

References

1. Weikum G. Towards guaranteed quality and dependability of information services. Datenbanksysteme in Büro, Technik und Wissenschaft: 8. GI–Fachtagung Freiburg im Breisgau, 1-3 März 1999. Springer Berlin Heidelberg; 1999. Pp. 379-409.

2. Distefano S., Puliafito A. Information dependability in distributed systems: The dependable distributed storage system. *Integrated Computer-Aided Engineering* 2014;21(1):3-18.

3. Ceolin D. et al. Assessing trust for determining the reliability of information. In: Situation awareness with systems of systems. Springer New York; 2013. Pp. 209-228.

4. GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

5. GOST R 27.102-2021. Dependability in technics. Dependability of item. Terms and definitions; 2021. (in Russ.)

6. GOST 27751-2014. Reliability for constructions and foundations. General principles; Moscow. (in Russ.)

7. Fitzner K. Reliability and validity a quick review. *The Diabetes Educator* 2007;33(5):775-780.

8. Cohen L., Manion L., Morrison K. Validity and reliability. Research methods in education. Routledge; 2017. Pp. 245-284.

9. Durand V.M., Barlow D.H. Essentials of abnormal psychology. Wadsworth/Thomson Learning; 2003.

10. Gaski J.F. Introducing the Marketing Accountability Standards Board (MASB) and its Common-Language Marketing Dictionary: Background, Description, Vision, and Prospects. *Journal of Macromarketing* 2021;41(4). Pp. 521-526.

11. Zhu W. Reliability: What type, please! *Journal of Sport and Health Science* 2013;2(1):62-64.

12. Savnykh V.P., Tsvetkov V.Ya. Cognitive logic's principles. In: Artificial Intelligence in Intelligent Systems. Proceedings of Computer Science On-line Conference. Сер. "Lecture Notes in Networks and Systems". Zlín (Czech Republic); 2021. Pp. 288-296.

13. Kudzh S.A., Tsvetkov V.Ya. Cognitive expert assessment. In: Artificial Intelligence in Intelligent Systems. Proceedings of Computer Science On-line Conference. Сер. "Lecture Notes in Networks and Systems". Zlín (Czech Republic); 2021. Pp. 742-749.

14. Tsvetkov V.Ya. Cognitive Science of Information Retrieval. *European Journal of Psychological Studies* 2015;1(5):37-44.

15. Davidshofer K.R., Murphy C.O. Psychological testing: principles and applications. Pearson; 2005. P. 624.

16. Berti-Equille L., Borge-Holthoefer J. Veracity of Data. Springer Nature; 2022.

17. Ivannikov A.D., Tikhonov A.N., Tsvetkov V.Ya. Fundamentals of the information theory. Moscow: MAKS Press; 2007.

18. Tsvetkov V.Ya. Information Interaction as a Mechanism of Semantic Gap Elimination. *European researcher* 2013;4-1(45):782-786.

19. Chekharin E.E. Cognitive modeling as method elimination semantic gap. *Education Resourses and Technologies* 2016;1(13):103-109. (in Russ.)

Сведения об авторе

Цветков Виктор Яковлевич, доктор технических наук, доктор экономических наук, профессор, область научных интересов – дистанционное зондирование, геоинформатика, управление в экономических системах, принятие решений, информатика, образование, Российский университет транспорта (РУТ МИИТ), Москва, Россия, e-mail: cvj2@mail.ru.

About the author

Viktor Ya. Tsvetkov, Doctor of Engineering, Doctor of Economics, Professor, research interests: remote sensing, geoinformatics, management in economic systems, decision-making, computer science, education, Russian University of Transport (RUT MIIT), Moscow, Russia, e-mail: cvj2@mail.ru.

Вклад автора

Исследование проведено автором самостоятельно в полном объеме.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Надежность, том 25, №4, 2025 / Dependability 4, 2025
Методы и системы защиты информации.
Информационная безопасность

УДК 004.056
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-43-51

Оценка защищенности от информационных атак на интеллектуальные транспортные системы с многоуровневой системой защиты информации

Evaluation of cyber security of intelligent transportation systems with a multi-level information protection system

Алексеев В.М.[1], Баранов Л.А.[1], Чичков С.Н.[1]*
Alekseev V.M.[1], Baranov L.A.[1], Chichkov S.N.[1]*

[1] Российский университет транспорта (МИИТ), Москва, Российская Федерация
[1] Russian University of Transport (MIIT), Moscow, Russian Federation
** seriozha.tchichkov@yandex.ru*

Алексеев В.М.

Баранов Л.А.

Чичков С.Н.

Резюме. **Цель.** *Рассмотреть вопросы оценки защищенности от информационных атак на интеллектуальные транспортные системы с многоуровневой системой защиты информации. С целью предотвращения атак, нацеленных на захват информации в многоуровневой системе защиты, предложено реализовать ядро локальной вычислительной сети (на всех уровнях) по полносвязной схеме. Это позволяет организовывать случайные доверенные маршруты, которые после выполнения функции по передаче информации разбираются, то есть ограничены по времени существования. Передача информации по случайно выбранным доверенным маршрутам с ограниченным временем существования затрудняет проведение внутренних атак с целью захвата объектов сети, по которым передается критически важная информация.* **Методы.** *В статье применяются методы математического анализа, теории графов и теории вероятностей.* **Результаты.** *Рассмотрена модель захвата трафика атакующим при выбранной защитником случайной стратегии формирования маршрутов в полносвязной сети. Проведена оценка модели защиты информации в многоуровневой системе защиты информации. Предложено при реализации многоуровневой системы защиты для предотвращения перехвата информационных потоков использовать динамически организуемые доверенные маршруты в условиях полносвязности.* **Заключение.** *Предложенная в статье методика позволяет оценить уменьшение вероятности захвата вершин полносвязной сети, а также оценить вероятность захвата вершин в зависимости от длительности передаваемого сообщения.*

Abstract. **Aim.** *To examine the assessment of cyber security of intelligent transportation systems with a multi-level information protection system. For the purpose of preventing attacks aimed at capturing information in a multi-level protection system, it is proposed to implement a fully connected core of the local area network (at all levels). This enables random trusted paths that are dismantled upon transmitting the information, i.e. are limited in their time of existence. Communicating information along randomly selected trusted limited-lifetime paths complicates internal attacks that aim to capture network entities involved in the communication of critical information.* **Methods.** *The paper uses methods of mathematical analysis, graph theory, and probability theory.* **Results.** *The authors examine a model of traffic capture by an attacker, whereas the defender uses random pathing in a fully connected network. A model of information protection in a multi-level information protection system was assessed. It is proposed using dynamically organised trusted paths in fully connected environments when designing a multi-level protection system to prevent interception of information flows.* **Conclusion.** *The proposed technique allows estimating the decrease in the probability of vertex capture in a fully connected network, as well assessing the probability of vertex capture depending on the duration of message transmission.*

Ключевые слова: *полносвязность, маршрут, вершина-объект, атакующий, защитник, виртуализация.*
Keywords: *full connectivity, path, vertex object, attacker, defender, virtualisation.*

Для цитирования: *Алексеев В.М., Баранов Л.А., Чичков С.Н. Оценка защищенности от информационных атак на интеллектуальные транспортные системы с многоуровневой системой защиты информации // Надежность. 2025. №4. С. 43-51. https://doi.org/10.21683/1729-2646-2025-25-4-43-51*

For citation: *Alekseev V.M., Baranov L.A., Chichkov S.N. Evaluation of cyber security of intelligent transportation systems with a multi-level information protection system. Dependability 2025;4: 43-51. https://doi.org/10.21683/1729-2646-2025-25-4-43-51*

Поступила: *02.06.2025* / **После доработки:** *11.07.2025* / **К печати:** *28.09.2025*
Received on: *02.06.2025* / **Revised on:** *11.07.2025* / **For printing:** *28.09.2025*

Введение

Защита информационных ресурсов требует совершенствования не только технических средств, но и разработки новых моделей идентификации атак, обеспечивающих защиту от внешних и внутренних угроз в локальных вычислительных сетях, а также создания принципов управления и программно-технической реализации сетевой инфраструктуры для систем различного назначения транспортного комплекса. Особенность сетей интеллектуальных транспортных систем заключается в том, что в них значительно возрастают объемы передаваемой информации с использованием маршрутизации информационных потоков, направляемых в центры обработки информации от различных источников. Центральной задачей интеллектуальных транспортных систем является обеспечение безопасной перевозки грузов и пассажиров. В этой связи обеспечение защиты сетевой инфраструктуры интеллектуальных транспортных систем (как критических объектов) является актуальной задачей.

Обеспечение защиты для критически важных объектов [1, 2, 3] предложено осуществить с использованием принципа многоуровневости. Реализация многоуровневой системы базируется на разделении функций, выполняемых на разных уровнях. Каждый из уровней нацелен на выполнение функций отражения внешних и внутренних атак путем использования анализаторов различных типов. В случае обнаружения атаки от внешних или внутренних источников анализаторы прерывают информационный поток, поскольку расположены посредине между источником и получателем. В статье предложено политику безопасности в многоуровневой

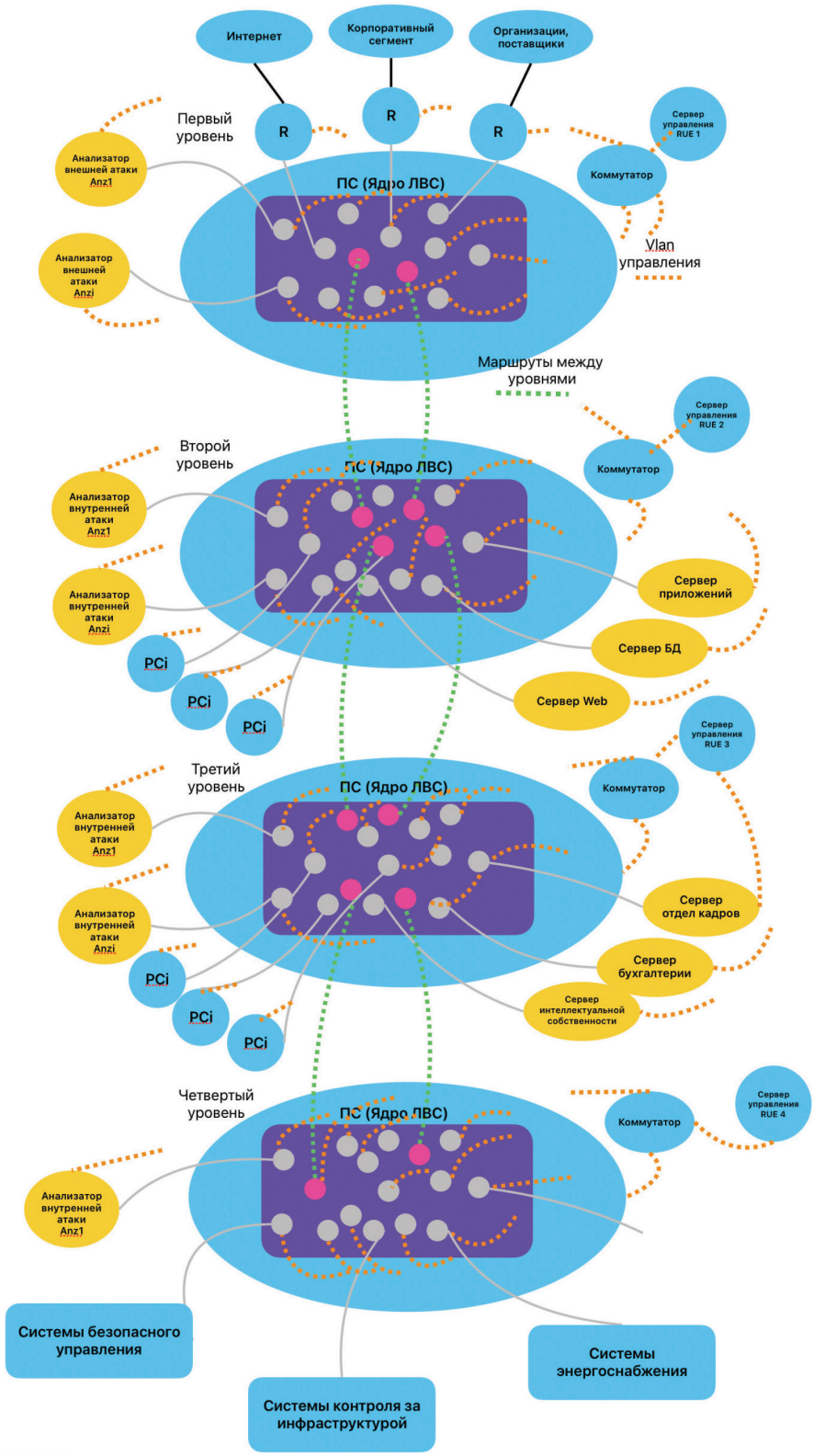


Рис. 1 Структура многоуровневой системы защиты информации

системе защиты строить на формировании случайных, динамически организуемых доверенных маршрутах, что позволяет защититься от внутренних атак перехвата информационных потоков.

Рассмотрена модель построения системы защиты информации, реализующей принцип «убегающего защитника от атакующего». Модель «убегающего защитника от атакующего» предложено реализовать на основе игры преследования на графах, где атакующий пытается получить доступ к объекту, включенному в маршрут передачи информации в текущий момент времени, а защитник формирует маршруты на графах (маршруты доставки информации в компьютерной системе). Задача атакующего (атакующих) – получить доступ к маршруту доставки информации в компьютерной системе, формируемому защитником (с целью получения конфиденциальной информации), а цель защитника – избегать захвата.

Цель исследования – оценить защиту информации в многоуровневой системе с динамически изменяемыми маршрутами. Для достижения цели необходимо решить следующие задачи:

- определить вероятность захвата вершины – объекта, включенного в случайно выбранный маршрут, по которому передается информационный поток;

- определить длительность захвата атакующим вершины – объекта, по которой передается информационный поток.

1. Функционирование многоуровневой модели защиты информации

На каждом уровне реализована полносвязная сеть (рис. 1). На первом уровне располагаются сетевые объекты локальной вычислительной сети, обеспечивающие связь с внешними корпоративными сетями, пользователями ресурсов и интернетом. С целью предотвращения возможных атак из внешних систем на первом уровне устанавливаются анализаторы *Anz*, каждый из которых нацелен на заданный тип информационной атаки *Inf*. На первом уровне нет персональных компьютеров субъектов и серверов.

Здесь происходит анализ трафика на присутствие внешних информационных атак. Сформированы признаки, на основании которых анализаторами *Anz* выявляются информационные атаки *Inf*. Передача информационных потоков из одного уровня в другой и обратно осуществляется в случае отсутствия признаков атак. На каждом уровне многоуровневой системы защиты локальная сеть реализована с использованием модели изолированной программной среды (ИПС) с использованием VLAN [4, 5, 6, 7]. Маршруты формируются сервером *RUE* [7,8]. Для реализации данной функции (формирования маршрутов *RUE*) создается отдельный *vlan–contr* управления. Сервер *RUE* формирует и отправляет конфигурационные файлы по *vlan–contr* на объекты, включаемые в маршрут (технология SDN (Software Defined Networking)) [8], где задается маршрут – vlan и политика информационного потока: порты, *vlan*, тип протокола, приоритетность, активность).

Маршруты на всех уровнях системы защиты реализуются также с помощью *vlan* с использованием серверов RUE_I, I=1,n. Объекты сети, не включенные в маршруты, неактивны. Маршрутизатор по маршруту, сформированному сервером *RUE*, направляет пакеты на *Anz* с тегом *vlan*, в котором определен протокол, приоритет и задан номер *vlan*. Передача информации из первого уровня во второй осуществляется по случайно заданным маршрутам, определяемым серверами RUE_I.

На втором уровне системы защиты располагаются субъекты с персональными компьютерами, сервера различных ресурсов (web, vks, mail, информационные базы для работы с клиентами и другие ресурсы).

На третьем уровне располагаются критически важные ресурсы, требующие усиленной защиты, такие как базы персональных данных, базы ноу-хау, бухгалтерии и другие ресурсы. Маршруты, связывающие второй уровень и третий, формируются также случайно серверами RUE_I, I=2,3.

На четвертом уровне защиты реализуются технологии, обеспечивающие функционирование систем безопасного управления на основе технологии мультисервисной передачи информации или других существующих технологий передачи информации, используемых для реализации интеллектуальных систем управления. Передача данных из третьего в четвертый уровень и наоборот также осуществляется по случайно заданным маршрутам RUE_I, I=3,4 .

На каждом уровне возможно появление внутренних атак, возникающих в результате неумышленных или злоумышленных действий субъектов. В этой связи, на каждом уровне устанавливаются анализаторы внутренних атак, основанные на использовании моделей профиля субъектов.

Рассмотрим граф $G=(V,E)$, описывающий состояние объектов локальной сети, расположенных на первом уровне, по которым передаются данные между объектами (маршрутизаторами и анализаторами *Anz*), где $V=\{v_1,v_2,\ldots,v_n\}$ – множество вершин – объектов локальной вычислительной сети, $E \subseteq V_i \times V_j; i, j = 1, n; i \neq j$ – множество ребер (обозначают связи между объектами). Объекты полносвязной сети $n_I \in n$ включены в общую сеть, где n_I – количество объектов в ядре ПС на уровне I. При этом, $n > n_I$, так как в n включаются персональные компьютеры, маршрутизаторы, собственно объекты ядра полносвязной ПС сети и другие объекты сетевой структуры.

Маршруты в ПС сети на каждом уровне I формируются специальным сервером управления RUE_I с использованием специальных протоколов (Open flow, rest api) [8, 9, 10, 11]. Маршруты $M_{k_i}^{RUE_I}$ простые и образуют множество, формируемое методом группового учета аргументов [12, 13], состоят из:

- наикратчайших маршрутов

$$M_{k_1}^{RUE_I} = V_i \times V_j; i, j = 1, n; i \neq j,$$

где k_1 – идентификатор наикратчайших маршрутов;

- маршрутов через один промежуточный объект

$$M_{k_2}^{RUE_I} = V_i \times V_k \times V_j; i, j, k = 1, n; i \neq \langle j, k \rangle; j \neq k,$$

где k_2 – идентификатор маршрутов с одним промежуточным объектом;

- маршрутов через два промежуточных объекта

$$M_{k_3}^{RUE_I} = V_i \times V_k \times V_l \times V_j; i, j, k, l = 1, n;$$
$$i \neq \langle j, k, l \rangle; j \neq \langle k, l \rangle; k \neq l,$$

где k_3 – идентификатор маршрутов с двумя промежуточными объектами;

- аналогично для маршрутов, проходящих через три и более промежуточных объектов.

Для всех маршрутов можно записать общую формулу:

$$\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I} = V_i \times V_j; \| V_i \times V_k \times V_j; \| V_i \times V_k \times V_l \times V_j;$$
$$\| \cdots_{i,j,k,l=1,n; i \neq \langle j,k,l \rangle; j \neq \langle k,l \rangle; k \neq l},$$

где n_1 – число промежуточных объектов в простых маршрутах, n_1=1,2,3,…h.

Рассмотрим формирование маршрутов передачи информации из первого во второй уровень. Информационные потоки поступают из внешней сети (корпоративный сегмент, либо интернет, либо пользователи юридические субъекты) на первый уровень многоуровневой системы защиты и маршрутизируются на анализаторы *Anz* внешних атак. Обозначим T – время существования маршрута $M_{k_i}^{RUE_I}$, которое складывается из времени формирования маршрута сервером RUE_I по команде от анализатора, пропуска трафика и далее завершения маршрута, то есть его разборки. Анализаторы на основе поступившей информации формируют признаки и принимают решение о запрете или пропуске трафика. Если *Anz* установлено, что в информационном потоке не содержится некорректной информации, *Anz* передает команду серверу RUE_I на конфигурацию маршрута. Информационный поток отправляется на второй уровень. В случае обнаружения *Anz* некорректной информации, маршрут для информационного потока запрещается. Обслуживание запросов от внешних пользователей осуществляется на втором уровне многоуровневой системы защиты, где располагаются основные ресурсы.

Трафик передается во второй уровень по маршруту, формируемому серверами RUE_1 и RUE_2 – первого и второго уровня. Индексы 1, 2 означают принадлежность к первому и второму уровням. Сервер RUE_1 назначает k_s объект, через который должен пройти маршрут передачи трафика из первого уровня во второй. Сервер RUE_1 сообщает RUE_2 об объекте k_s и под маршрут сервер RUE_2 выделяет k_s в ядре второго уровня защиты. Номер k_s выбирается из условия $k_s \neq \langle i, j, k_1 \ldots \rangle$ участвующих в организации маршрутов от маршрутизаторов к анализаторам на первом уровне. Маршрут описывается:

$$(V_i \times V_k \times V_{k_s})^{RUE_1} \times (V_{k_s} \times V_k \times V_i)^{RUE_2};$$
$$i, k_s, k = 1, n; i \neq \langle k_s, k \rangle; k_s \neq k.$$

Исходные условия задачи:

- граф содержит n вершин;
- атакующий A на каждом шаге j случайно выбирает одну вершину ядра ПС (равновероятно);
- защитник D прокладывает независимые, случайно выбранные маршруты с k_i промежуточными вершинами-объектами в ядре ПС;
- захват происходит, если хотя бы один маршрут защитника D проходит в той же вершине V_i, которую выбрал атакующий;
- движение атакующего A и защитника D происходит случайно и независимо друг от друга.

Рассмотрим внутреннюю атаку, которая может быть организована на втором, третьем или четвертом уровнях одиночным атакующим A на объекты ядра сети. (*Уязвимость CVE-2024-20399, CVE-2021-40119, оценивается на 9,8 из 10 по системе CVSS и является следствием несовершенства механизма аутентификации SSH в Cisco Policy Suite. Воспользовавшись этой уязвимостью, злоумышленник может подключиться к устройству по SSH, авторизовавшись как root)*.

Поскольку сеть полносвязная, то не все вершины-объекты активны, а только те, через которые проходят информационные потоки. Атакующий A пытается получить информацию путем овладения одной из вершин полносвязной сети, по которой проходит информационный поток, сформированный защитником D. Стратегию защитника D атакующий A не знает. Атакующий A движется равновероятно (случайное блуждание) по соседним вершинам. Состояние атакующего A обозначим $V_A(t)$ в момент времени t. Атакующий A может вставать на любую вершину – объект ПС сети с целью получить доступ к информационному потоку. Состояние защитника D в момент времени t представляется маршрутом $M_k(t) \in \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}$. Маршрут $M_k(t)$ защитника D проходит по объектам, включенным в этот маршрут сервером управления RUE_I. Обозначим t_{M_k} – время существования маршрута. Если атакующий A, встав на вершину $V_A(t) \in M_k(t) \in \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}$, по которой проходит маршрут информационного потока, овладевает им, то считаем, что атакующий A достиг цели.

Рассмотрим задачу определения вероятности захвата вершины – объекта, включенного в случайно выбранный маршрут, по которому передается информационный поток.

Решение. Защитник *D* формирует маршрут информационного потока, проходящий через вершины – объекты ядра ПС:

$$\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l} = V_i \times V_j; \left\| V_i \times V_k \times V_j; \right\| V_i \times V_k \times V_l \times V_j; \left\| \cdots_{i,j,k,l=1,n; i \neq \langle j,k,l \rangle; j \neq \langle k,l \rangle; k \neq l}. \quad (1)$$

Возможны два случая. Случай первый – маршрут информационного потока проходит через объект – вершину V_i, i=1,n принадлежащую одному из объектов, участвующих в формировании маршрута (1). *A* атакует вершину – объект V_i и получает доступ к информации в промежуток времени *T* существования информационного потока $\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$, проходящего через V_i, i=1,n , то есть $V_A(t) = \left(V_i \in M_k(t)\right) \in \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$.

Случай второй – если информационный поток не проходит через объект – вершину V_i, i=1,n, то *A* не получает доступа к информационному потоку, то есть $V_A(t) = V_i \notin \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$.

Оценку захвата вершины V_i атакующим *A* в полносвязной сети выполним с помощью параметра центральности вершины $C(V_i)$, который показывает связность (важность) вершины – объекта для формирования маршрутов передачи информационных потоков в сети и определяется:

$$C(V_i) = n_s \times \frac{P_{i,j}}{n_{sv}}, j = 1, n; n > 1, \quad (2)$$

где n_s – связи V_i вершины – объекта с соседними вершинами, равно n–1;

$P_{i,j}$ – вероятность осуществления передачи информации из вершины – объекта i к соседним вершинам – объектам, не занятым в маршруте;

n_{sv} – общее количество связей в ПС сети уровня *I*, $n_{sv}=n\times(n-1)$ (конечная вершина 0 граф n=1).

Примем вероятность перехода из вершины – объекта V_i к соседним объектам $P_{i,j}=1/(n-1)$.

Защитник *D* выбирает случайную стратегию формирования маршрута $M_{k_i}^{RUE_l}$. В этом случае, вероятность выбора вершины – объекта V_i из всех вершин – объектов, задействованных в маршрутах $\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$, определяется как $P_{V_i}^d = \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}\right)}$.

Из формулы (1) следует (подставив значения n_s, n_{sv}, $P_{i,j}$), что для полносвязного ядра (для любого из уровней *I*) параметр центральности вершины для всех одинаковый и равен

$$C(V_i) = 1/\left(n \times (n-1)\right), j = 1, n. \quad (3)$$

При выборе стратегии случайного формирования маршрутов защитником *D* вероятность захвата информационного потока на вершине V_i атакующим *A* равна

$$P_{V_i} = C(V_i) \times P_{V_i}^d. \quad (4)$$

Наличие нескольких маршрутов в ядре изменяет величину $C(V_i)$, поскольку меняются параметры n_s и $P_{i,j}$ из-за уменьшения количества вершин, с которыми возможно организовать маршрут, что вытекает из ограничения соединения с соседней вершиной – объектом, занятым в маршруте (условие простого маршрута). Причем, при формировании маршрутов с промежуточными объектами параметр принимает значение равное

$$P_{i,j} = 1/\left((n-1)-k\right), \quad (5)$$

где k – соседние объекты, задействованные в маршрутах.

Из последней формулы (5) вытекает, что вероятность захвата информационного потока атакующим *A* возрастает при наличии действующих маршрутов в ядре ПС на любом из *I*-их уровней. Преодолеть возникшую коллизию возможно с использованием модели изолированной программной среды и виртуализации сети. Использование виртуализации позволяет формировать маршруты на портах объектов (на одном порту объекта можно организовывать несколько *vlan*), что позволяет формировать простые маршруты, проходящие одновременно по разным портам на одном объекте. Это позволяет исключить из формулы (4) переменную k.

Рассчитаем вероятность захвата атакующим *A* за время *T* вершины V_i, по которой передается информационный поток. Если атакующий движется случайным образом, то вероятность того, что вершина – объекта V_i в момент времени *t* будет занята *A*, равна:

$$P_{V_i}(T) = 1 - \prod_{t=1}^{T}\left(1 - p_i\left(x_D(t) = x_A^j(t)\right)\right), \quad (6)$$

где $p_i\left(x_D(t) = x_A^j(t)\right)$ – вероятность занятия V_i в момент времени *t* атакующим *A*, j=1,m – шаги по вершинам V_i сети.

Если атакующий движется равновероятно (случайное блуждание) по соседним вершинам:

$$p\left(x_A(t) = V_i\right) = \frac{1}{n}, \text{ где } V_i \in V_n. \quad (7)$$

Подставляем (7) в (6). Тогда вероятность захвата вершины V_i за время *T* равна:

$$P_c(T) = 1 - \left(1 - \frac{1}{n}\right)^T.$$

Найдем вероятность необнаружения маршрута за один шаг j=1. В момент времени *t*, если:

- защитник *D* с маршрутом k_i в случайной вершине $V_i \in V$;

- атакующий занимают случайную вершину-объект V_i, через которую проходит один из k_i маршрутов *D*.

Тогда вероятность, что атакующий A не попал на маршрут защитника в этот момент:

$$P_{\text{нет захвата маршрута за шаг j=1}} = 1 - \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}, \quad (8)$$

то есть атакующий на шаге j=1 в одной из вершин; с вероятностью p, что она совпадет с любой из случайных в сформированных маршрутах

$$p = \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}.$$

Вероятность непопадания на объект – вершину, включенную в маршрут, за j шагов определяется при независимом движении A и D на каждом шаге:

$$P_{\text{нет захвата маршрута за j шаг}} = \left(1 - \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}\right)^{j}. \quad (9)$$

Вероятность попадания на объект – вершину, включенную в маршрут, за j шагов – это противоположное событие. Тогда:

$$P(j) = 1 - \left(1 - \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}\right)^{j}. \quad (10)$$

Интерпретация уравнения (10):

- при j=0 : $P(j$=0)=0;
- при $j \to \infty$: $P(j) \to 1$ (атакующий обнаружит действующий маршрут);
- при большом количестве маршрутов k_i вероятность захвата любого маршрута атакующим A растет быстрее.

На рис. 2 показано как вероятность захвата (время захвата T=j) маршрута защитника $P(j)$ возрастает с увеличением числа шагов j для различных соотношений k_i/n – числа маршрутов k_i и числа вершин n ПС сети:

- чем больше k_i маршрутов прокладывается по сети, тем быстрее происходит захват;
- при меньшем n (граф меньшего размера) вероятность захвата выше при тех же k_i.

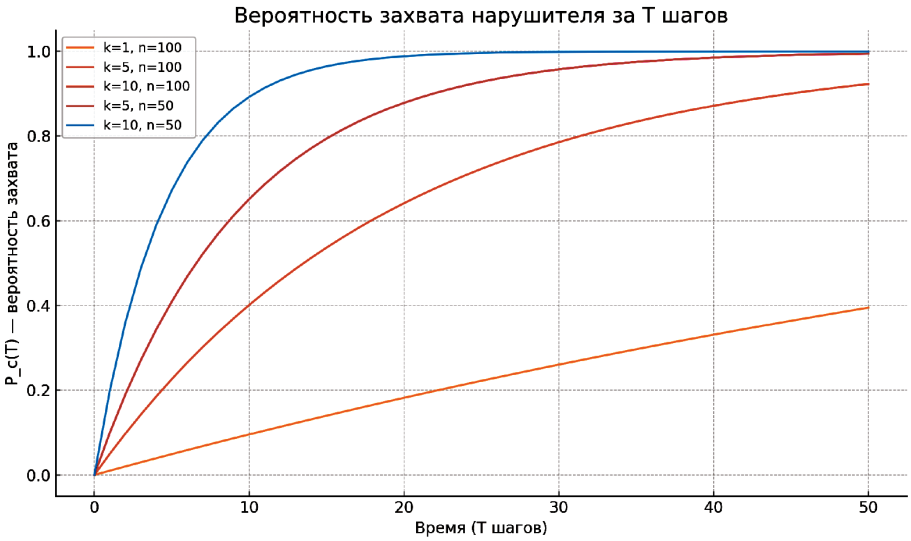


Рис. 2. Вероятность захвата маршрута защитника за j шагов, j=T

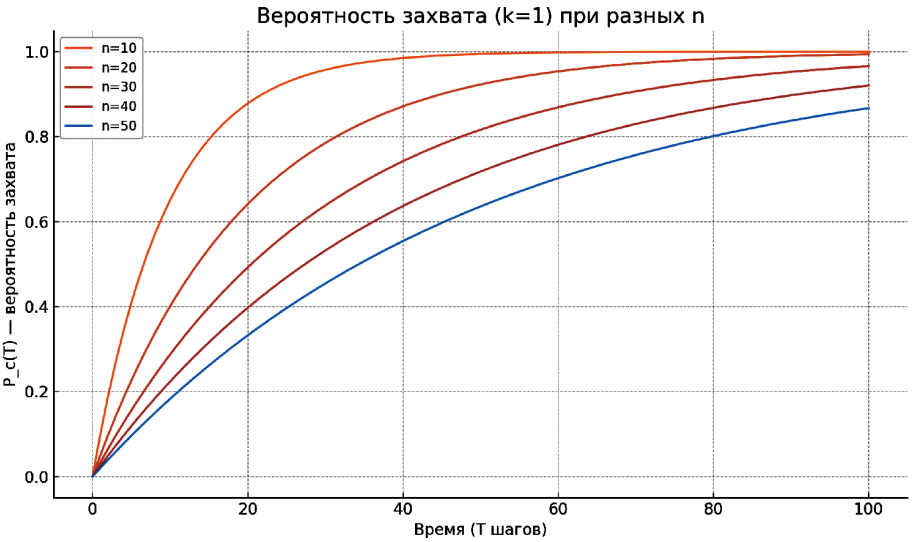


Рис. 3 Вероятность захвата маршрута при одном атакующем и одном маршруте (k = 1) и различных размерах графа n = 10, 20, 30, 40, 50

На рис. 3 показаны зависимости вероятности захвата маршрута при одном атакующем и одном маршруте для различных размеров графа. Из рис. 3 следует:

- чем меньше граф (n), тем быстрее вероятность захвата растет;
- при n = 10 захват вероятен уже за ~20 шагов;
- при n = 50 требуется гораздо больше шагов, чтобы достичь высокой вероятности (например, 80–90%).

На рис. 4 показано, как увеличение числа маршрутов k_i при фиксированном числе вершин n=30 влияет на скорость захвата:

- при k_i=1 вероятность растет медленно, нужно ~30–40 шагов для высокой вероятности;
- при k=5 уже за ~15 шагов вероятность захвата достигает ~80%;
- при k=10 вероятность захвата достигает 90% примерно за 10 шагов;
- при k=20 захват почти гарантирован за первые 5–6 шагов.

Таким образом, на основании полученных данных можно сделать следующий вывод: увеличение числа вершин n ядра ПС сети при постоянно заданном

количестве маршрутов k снижает вероятность захвата вершины в сформированных маршрутах.

Рассмотрим решение задачи определения времени захвата атакующим *A* вершины V_i за j шагов, по которой передается информационный поток, за время его существования t_{M_k}.

Решение. Оценку времени захвата атакующим вершины случайного маршрута проведем с использованием геометрического распределения [16]. Условия, применения геометрического распределения:

- каждый шаг j – независим;
- защитник и атакующий независимо и случайно выбирают вершины на каждом шаге;
- вероятность захвата постоянна на каждом шаге;
- на каждом шаге вероятность того, что защитник и атакующий окажутся в одной вершине, определяется из (8) и равно

$$p = \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}\right)}.$$

Геометрическое распределение описывает число шагов до первого успеха в последовательности независимых испытаний, где в каждом испытании вероятность успеха равна p. Формула геометрического распределения:

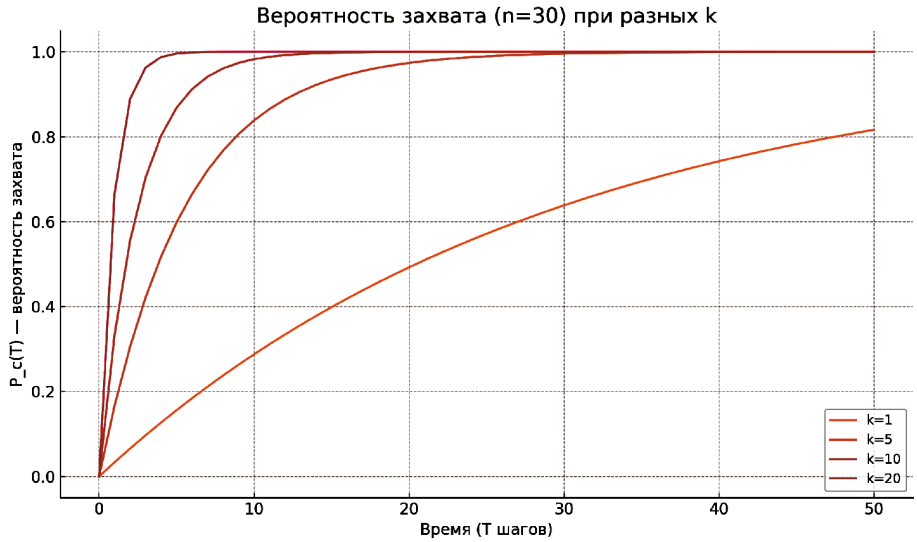


Рис. 4 Вероятность захвата при k_i и постоянном числе вершин

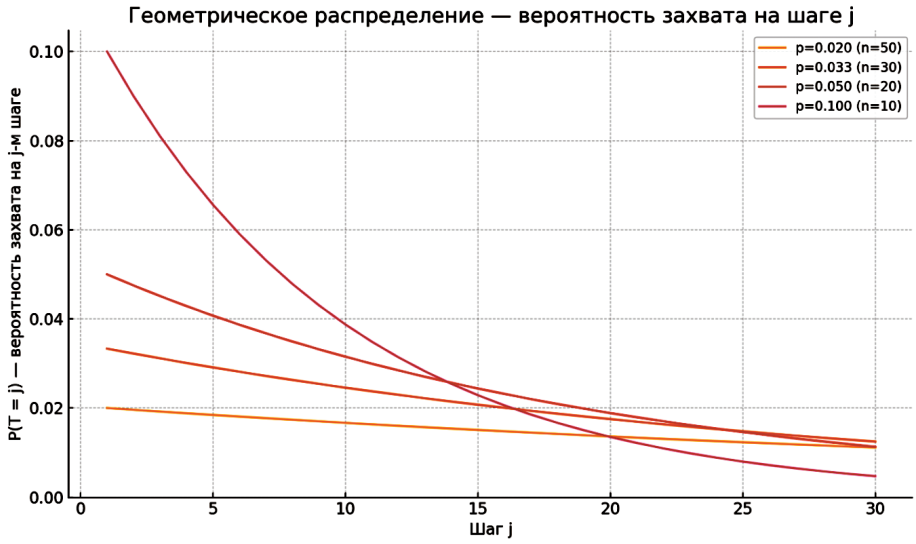


Рис. 5 Вероятность захвата вершины от времени t=J

$$\mathbb{P}[J = t] = (1-p)^{t-1} \cdot p, \qquad (11)$$

где J – количество шагов до первого успеха;

p – вероятность успеха на каждом шаге в момент времени t–1;

$(1–p)^{t-1}$ – ни одного успеха в первых t–1 шагах;

p – и успех на t-м шаге.

Захват возможен только в одном месте. Если в текущем шаге не произошло захвата, идем к следующему шагу, и процесс повторяется с той же вероятностью. Поскольку каждый шаг – одно испытание, захват – это успех и каждое испытание независимо, то мы имеем классическую ситуацию геометрического распределения времени до первого успеха. Распределение времени (10) захвата за j шагов:

$$\mathrm{Geom}(p) -> P[J \le j] = (1-p)^{j-1} \cdot p. \qquad (12)$$

Ожидаемое (среднее) время захвата: $\mathbb{P}[J] = \frac{1}{p} = \frac{n}{k_i}$.

На рис. 5 приведены значения времени t=j геометрического распределения Geom(p) с осью шагов j. Он показывает, как меняется вероятность захвата на каждом шаге при разных значениях p=k_i/n. J определяет время проходящее от начала процесса захвата до его завершения. Длительность существования информационного потока определяется объемом передаваемой информации и обычно составляет t_{M_k}=3–5 с. Время захвата вершины – объекта атакующим лежит в пределах 15–20 с. Исходя из этого, можно сделать вывод, что для осуществления перехвата трафика атакующий должен завладеть как можно большим количеством вершин-объектов, через которые передаются информационные потоки.

Заключение

Рассмотрена модель построения системы защиты информации, реализующей принцип «защитника от атакующего». Получена оценка вероятности захвата атакующим вершины графа, через которую проходит маршрут.

Предложено, при реализации многоуровневой системы защиты для предотвращения перехвата информационных потоков использовать динамически организуемые доверенные маршруты в условиях полносвязности.

Предложенная методика позволяет оценить уменьшение вероятности захвата вершин полносвязной сети. Предложенная методика позволяет оценить вероятность захвата вершин полносвязной сети в зависимости от длительности передаваемого сообщения.

Благодарность. Работа выполнена за счет бюджетного финансирования в рамках государственного задания от 20.03.2025 № 103-00001-25-02.

Список литературы

1. Попов П.А., Розенберг Е.Н., Сабанов А.Г. и др. Комплексная безопасность АСУ ТП объектов КИИ железнодорожного транспорта // Надежность. 2024. Том: 24 №: 4. С. 48-57. DOI: 10.21683/1729-2646-2024-24-4-48-57

2. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утв. приказом ФСТЭК России от 02.06.2020 г. № 76.

3. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утв. приказом ФСТЭК России от 25.12.2017 г. № 239.

4. Сайт Oxidized: Система управления конфигурациями сетевого оборудования // Oxidized [электронный ресурс]. URL: https://bubnovd.net/post/blogger/система-управления-конфигурациями-oxidized/ (дата обращения: 14.04.2025).

5. Дмитриева Ю.С. Сравнительный анализ методов управления сетевыми ресурсами в сетях SDN // Труды учебных заведений связи. 2022. № 8. С. 73-83.

6. Волков А.С., Баскаков А.Е. Разработка алгоритма многопутевой маршрутизации в программно-конфигурируемых сетях связи // T-Comm – Телекоммуникации и Транспорт. 2021. № 5. С. 17-23.

7. Черников А.С., Паус А.С. Многопоточная маршрутизация в программно-конфигурируемых сетях // Радиооптика. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 06. С. 35-46. DOI: 10.7463/rdopt.0616.0850725

8. Eiman Alotaibi. A tutorial on software-defined networks emulation // Journal of Engineering Research. DOI:10.1016/j.jer.2023.12.005

9. Mohammad Nowsin Amin Sheikh, I-Shyan Hwang, Muhammad Saibtain Raza. A Qualitative and Comparative Performance Assessment of Logically Centralized SDN Controllers via Mininet Emulator // Computers. 2024. Vol. 13(4). P. 85. DOI: 10.3390/computers13040085

10. Программно-определяемые сети SDN // Cloud Networks [электронный реурс]. URL: https://cloudnetworks.ru/inf-tehnologii/programmno-opredelyaemye-seti-sdn/ (дата обращения: 14.04.2025).

11. Mudassar Hussain Nadir Shah, Rashid Amin. Software-Defined Networking: Categories, Analysis, and Future Directions // Sensors. 2022. Vol. 22(15). P. 5551. DOI: 10.3390/s22155551

12. Ivakhnenko A.G. Longterm forecasting and management of complex systems. Kiev: Technics, 1975. 310 p.

13. Алексеев В.М., Чичков С.Н. Защита информации в интеллектуальных транспортных системах управления городским транспортом // Надежность. 2022. Том 22. № 3. С. 62-68.

14. Вахний Т.В., Tyu A.K. Матрично-игровая программа с выбором критерия для определения оптимального набора средств защиты компьютерной системы // Математические структуры и моделирование. 2016. № 2(38). С. 103-115.

15. Савченко С.О., Капчук Н.В. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр // Динамика систем, механизмов и машин. 2017. Том 5. № 4. DOI: 10.25206/2310-9793-2017-5-4-84-90

16. Колчин В.Ф. Геометрическое распределение. В кн.: Большая российская энциклопедия : [в 35 т.] / гл. ред. Ю. С. Осипов. М.: Большая российская энциклопедия, 2004-2017.

References

1. Popov P.A., Rozenberg E.N., Sabanov A.G., Shubinsky I.B. Integrated Safety of ACS of Railway CII Facilities. *Dependability* 2024;24(4):48-57. (in Russ.) DOI: 10.21683/1729-2646-2024-24-4-48-57

2. [Information security requirements that define the levels of trust to the information security and information technology protection tools. Approved by the order of the FSTEC of Russia dated 06.02.2020 No. 76]. (in Russ.)

3. [Safety requirements for significant facilities of critical information infrastructure of the Russian Federation. Approved by the order of the FSTEC of Russia dated 12.25.2017 No. 239]. (in Russ.)

4. [Oxidized: Network equipment configuration management system]. (accessed 14.04.2025). Available at: https://bubnovd.net/post/blogger/система-управления-конфигурациями-oxidized/

5. Dmitrieva J. Comparative Analysis of Network Resource Management Methods in SDN. *Proc. Of Telecom. Universities* 2022;8(1):73-83. (in Russ.)

6. Volkov A.S., Baskakov A.E. Development of a multipath routing algorithm in software-defined communication networks. *T-Comm* 2021;15(9):17-23. (in Russ.)

7. Chernikov A.S., Paus A.S. Multi-threaded Routing in Software-defined Networking. *Radiooptics of the Bauman MSTU* 2016;6:35-46. DOI: 10.7463/rdopt.0616.0850725

8. Alotaibi E. A tutorial on software-defined networks emulation. *Journal of Engineering Research*. DOI:10.1016/j.jer.2023.12.005

9. Mohammad Nowsin Amin Sheikh, I-Shyan Hwang, Muhammad Saibtain Raza. A Qualitative and Comparative Performance Assessment of Logically Centralized SDN Controllers via Mininet Emulator. *Computers* 2024;13(4):85. DOI: 10.3390/computers13040085

10. Cloud Networks. (accessed 14.04.2025). Available at: https://cloudnetworks.ru/inf-tehnologii/programmno-opredelyaemye-seti-sdn/

11. Mudassar Hussain Nadir Shah, Rashid Amin. Software-Defined Networking: Categories, Analysis, and Future Directions. *Sensors* 2022;22(15):5551. DOI: 10.3390/s22155551

12. Ivakhnenko A.G. Longterm forecasting and management of complex systems. Kiev: Technics; 1975. (in Russ.)

13. Alekseev V.M., Chichkov S.N. Information security in intelligent mass transit management systems. *Dependability* 2022;22(3):62-68. (in Russ.)

14. Vahniy T.V., Guts A.K., Novikov N.Y. Matrix-game program with selection criterion for determination of optimal tool set for computer system protection. *Mathematical Structures and Modeling* 2016:2(38):103-115. (in Russ.)

15. Savchenko S.O., Kapchuk N.V. Algorithm of creation of model of the violator in the information security system with application of game theory. *Dynamics of Systems Mechanisms and Machines* 2017;5(4):84-89. (in Russ.) DOI:10.25206/2310-9793-2017-5-4-84-89

16. Kolchin V.F. Geometric distribution. In: Osipov Yu.S., chief editor. The Great Russian Encyclopaedia: [in 35 volumes]. Moscow: The Great Russian Encyclopaedia; 2004-2017. (in Russ.)

Сведения об авторах

Алексеев Виктор Михайлович – доктор технических наук, профессор, профессор кафедры «Управление и защита информации», Российский университет транспорта (МИИТ), Москва, Российская Федерация, e-mail: alekseevvm@rambler.ru.

Баранов Леонид Аврамович – доктор технических наук, профессор, заведующий кафедрой «Управление и защита информации», Российский университет транспорта (МИИТ), Москва, Российская Федерация.

Чичков Сергей Николаевич – аспирант кафедры «Управление и защита информации», старший преподаватель кафедры «Высшая математика», Российский университет транспорта (МИИТ), Москва, Российская Федерация, e-mail: seriozha.tchichkov@yandex.ru.

About the authors

Victor V. Alekseev, Doctor of Engineering, Professor, Professor of the Department of Management and Protection of Information, Russian University of Transport (MIIT), Moscow, Russian Federation, e-mail: alekseevvm@rambler.ru.

Leonid A. Baranov, Doctor of Engineering, Professor, Head of the Department of Management and Protection of Information, Russian University of Transport (MIIT), Moscow, Russian Federation.

Sergey N. Chichkov, post-graduate student, Department of Management and Protection of Information, Senior Teacher, Department of Higher Mathematics, Russian University of Transport (MIIT), Moscow, Russian Federation, e-mail: seriozha.tchichkov@yandex.ru.

Вклад авторов в статью

Алексеев В.М. Разработка и оценка моделей.

Баранов Л.А. Разработка и оценка моделей.

Чичков С.Н. Выполнение расчетов, оформление результатов.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Надежность, том 25, №4, 2025 / Dependability 4, 2025
Методы и системы защиты информации.
Информационная безопасность

УДК 519.81:004.056:007.51
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-52-60

Применимость метода ELECTRE I при многокритериальном выборе страхуемых автоматизированных систем и приоритете киберзащищенности и критерий трехзначной мажоритарной логики

The applicability of ELECTRE I as part of multi-criteria selection of insurable automated systems and the priority of cyber security and the criterion of three-valued majority logic

Шептунов М.В.
Sheptunov M.V.

Московский Государственный лингвистический университет (ФГБОУ ВО «МГЛУ»),
Московский Гуманитарный университет (АНО ВО «МосГУ»), Москва, Российская Федерация
Moscow State Linguistic University,
Moscow University for the Humanities, Moscow, Russia
triumf403@yandex.ru

Шептунов М.В.

Резюме. Цель. *Выяснить и показать применимость подхода разработки индексов попарного сравнения альтернатив (РИПСА) на примере одного из методов ELECTRE – для выбора автоматизированных информационных систем (АИС) с учетом критериев, относящихся к киберзащищенности АИС и страхованию киберрисков.* **Методы.** *Из группы методов ELECTRE в качестве ее представителя в статье использован метод ELECTRE I, подробно изложенный в известных книгах. Данная группа методов относится к подходу РИПСА, одним из отечественных первопроходцев которого, направленного на сопоставление многокритериальных альтернатив, был акад. РАН Ларичев О.И. В целях вводимого критерия, названного «трехзначный мажоритарный критерий киберзащищенности АИС с учетом страхования» применены элементы трехзначной мажоритарной логики.* **Результаты.** *Показана применимость подхода РИПСА в виде метода ELECTRE I для выбора АИС в ракурсе рассмотренных критериев, относящихся к киберзащищенности АИС, с учетом страхования киберрисков. Разработан модифицированный, новый в плане киберзащищенности при страховании киберрисков критерий, основанный на трехзначной мажоритарной логике – а именно позволивший выразить и учесть в логико-математическом виде: некоторые особенности страховой защиты АИС в связи с присущими им киберрисками, а также способность АИС противостоять собственными средствами классифицируемым по трем категориям кибератакам на подобные организационно-технические системы.* **Выводы.** *Критерий качества технико-экономического характера на основе трехзначной мажоритарной логики может использоваться не только в ракурсе технических и организационно-технических параметров либо характеристик киберзащищенности АИС, но и в ракурсе финансово-экономических параметров либо характеристик защищенности страхуемых АИС. Методы группы ELECTRE подхода разработки индексов попарного сравнения альтернатив применимы: как в ракурсе анализа и организационно-технических мер по снижению различных связанных с АИС киберрисков, так и в ракурсе страховой защиты от них. Как показано в статье, возможно обойтись в методах ELECTRE на две единицы меньшим количеством критериев за счет разработанного интегрального критерия, а именно трехзначной мажоритарной логики для многокритериальных альтернатив.*

Abstract. Aim. *To use the case of one of the ELECTRE methods to identify and demonstrate the applicability of the development of indexes for pairwise comparison of alternatives (RIPSA) for selecting automated information systems (AIS) taking into account criteria associated with AIS cybersecurity and cyber risk insurance.* **Methods.** *The paper uses the ELECTRE I method that is well-described in well-known publications. The ELECTRE group of methods belongs to the RIPSA approach that aims to compare multi-criteria alternatives. One of the Russian pioneers of this approach was the RAS member Larichev O.I. The introduced criterion called the "three-digit majority criterion of AIS cybersecurity taking into account insurance" uses elements of three-digit majority logic.* **Results.** *The paper shows the applicability of the RIPSA approach, ELECTRE I specifically, for selecting AIS as regards the examined criteria associated with AIS cybersecurity, taking into account cyber risk insurance. A modified criterion has been developed that is new as regards cyber security in the context of cyber liability insurance*

and is based on a three-digit majority logic. Specifically, it allows expressing and taking into account in a logical and mathematical form some features of AIS insurance protection given the inherent cyber risks, as well as the ability of AIS to independently withstand the three categories of cyber attacks. **Conclusion.** *The three-digit majority logic-based technical and economic quality criterion is applicable to not only technological and organisational parameters or characteristics of AIS cyber security, but the financial and economic parameters or security characteristics of insured AIS as well. The ELECTRE methods of developing pairwise alternative comparison indexes are applicable both in the analysis, organisational and technological measures to reduce various AIS-related cyber risks, and in associated insurance protection. The paper shows that the developed integral criterion, namely the three-digit majority logic for multi-criteria alternatives, allows using the ELECTRE methods with two criteria less.*

Ключевые слова: *принятие решений, сравнение альтернатив, управление доступом, показатель, многокритериальный выбор, франшиза, перестрахование.*
Keywords: *decision-making, comparison of alternatives, access control, indicator, multi-criteria choice, franchise, reinsurance.*

Для цитирования: *Шептунов М.В. Применимость метода ELECTRE I при многокритериальном выборе страхуемых автоматизированных систем и приоритете киберзащищенности и критерий трехзначной мажоритарной логики // Надежность. 2025. №4. С. 52-60. https://doi.org/10.21683/1729-2646-2025-25-4-52-60*
For citation: *Sheptunov M.V. The applicability of ELECTRE I as part of multi-criteria selection of insurable automated systems and the priority of cyber security and the criterion of three-valued majority logic. Dependability 2025;4: 52-60. https://doi.org/10.21683/1729-2646-2025-25-4-52-60*

Поступила: *16.05.2024* / **После доработки:** *25.05.2025* / **К печати:** *28.09.2025*
Received on: *16.05.2024* / **Revised on:** *25.05.2025* / **For printing:** *28.09.2025*

Введение

В настоящее время весьма актуален именно многокритериальный выбор автоматизированных информационных систем (АИС) гражданского назначения в ракурсе их киберзащищенности со страхованием киберрисков. Критерии для таких АИС нередко разнонаправлены, противоречивы и вполне могут представлять самостоятельный интерес. Все больший интерес вызывают и смежные вопросы о страховании киберрисков, для которых вследствие практической невозможности абсолютной комплексной защиты систем (даже при больших финансовых вложениях) – в условиях расширяющегося спектра киберугроз и из-за растущих возможностей компьютерных сетей – следует предусматривать страхование. Сказанное актуально для каждого предприятия – объекта экономики и одновременно информатизации, стремящегося защитить свои АИС и соответствующие электронные ресурсы.

Этим обусловлена уместность использования для ставящейся здесь проблемы данной теоретико-прикладной сферы т.н. (в основном в российской научной и образовательной литературе) подхода РИПСА (разработки индексов попарного сравнения альтернатив), направленного на сопоставление многокритериальных альтернатив. В СССР и РФ одним из первопроходцев этой проблематики был акад. РАН Ларичев О.И. [1]. Однако в переводе с французского заложенные профессором Руа Б. [2] методы группы ELECTRE (Elimination Et Choix Traduisantla Realite), относящиеся к упомянутому подходу, фигурируют как «исключение и выбор, отражающие реальность», однако нередко и как «исключение и выбор в условиях реальности».

Реальность такова, что для АИС, их выбора зачастую не только критериев более 2-х–3-х, но и альтернатив для ЛПР (лиц, принимающих решения) нередко не меньше трех или даже больше. Тем более, принимая в расчет страхование киберрисков, нуждающееся в предпочтительнее специализированном, обособленном критерии (и в то же время системно связанном с другими имеющимися и разработанными критериями для АИС, наиболее приоритетными здесь в ракурсе киберзащищенности). Среди таковых может быть, например (*в качестве лишь одного из множества возможных примеров для АИС в гражданской сфере*) [3]: среднее время проникновения нарушителя в автоматизированную систему защищенной обработки информации (далее АСЗОИ).

Известно, например, из [4], что при выборе между дорогостоящими проектами заказчику следует проводить собственные оценки технологий, обращаться к экспертам для осуществления независимого анализа проектов – сказанное относится и к проектируемым и модернизируемым АИС. Тем более, к альтернативам пока еще не апробированных технологий безопасности, предполагающих возможность доработки благодаря техническим решениям в процессе модификаций.

Исходя из известных книг[1], видятся вполне возможными для применения и такие критерии (показатели), здесь именно в рамках подхода РИПСА, причем по своей сущности относящиеся к киберзащищенности:

[1] Как, например: Хетагуров Я.А. Проектирование автоматизированных систем обработки информации и управления (АСОИУ): учебник. Москва: БИНОМ. Лаборатория знаний; 2015. 240 с.

I) коэффициент защиты системы обработки информации с N каналами

$$K_{\text{I}} \equiv K_{\text{з}} = \sum_{i=1}^{N_{\text{з}}} \frac{K_{\text{з}i}}{N}, \quad (1)$$

где $N_{\text{з}}$ – количество охваченных защитой каналов системы;

II) показатель сложности защиты системы

$$K_{\text{II}} \equiv \tilde{R} = \frac{\Delta R}{R} = \frac{\left[(R+\Delta R)-R\right]}{R}, \quad (2)$$

характеризующий относительные затраты дополнительных ресурсов ΔR на защиту основных ресурсов R (причем годовые эксплуатационные расходы из-за введения защиты увеличиваются не более чем на 13–60%);

III) величина остаточного (коммерчески ценного информационного) ресурса через время t при сокращении его хищения в процессе защиты

$$K_{\text{III}} \equiv S_{tx} = S_0(1+r)^t - (S_x - S_y)(1+r)^t = \\ = S_0(1+r)^t - \left(S_x - \frac{a_1 y_c}{1+b_1 y_c}\right)(1+r)^t, \quad (3)$$

где S_0 – величина (стоимость) исходного ресурса;

r – процентная банковская ставка;

t – анализируемый интервал времени;

S_x – величина похищенного ресурса;

$S_y = \frac{a_1 y_c}{1+b_1 y_c}$ – величина сокращения хищения, определяемая затратами y_c на средства защиты (обычно в виде подсистемы защиты);

$(S_x – S_y)$ – разность между величиной похищенного ресурса и величиной сокращения хищения;

a_1, b_1 – коэффициенты, определяемые методом экспертных оценок либо из выражений

$$a_1 = \frac{S_{y1}S_{y2}(y_{c1}-y_{c2})}{y_{c1}y_{c2}(S_{y1}-S_{y2})},\ b_1 = \frac{S_{y2}y_{c1}-S_{y1}y_{c2}}{y_{c1}y_{c2}(S_{y1}-S_{y2})},$$

вытекающих из уравнений для двух близких – к входящим во множество альтернатив – вариантов АИС, у которых определены соответствующие воздействия S_y и y_c:

$$S_{y1} = \frac{a_1 y_{c1}}{1+b_1 y_{c1}},\ S_{y2} = \frac{a_1 y_{c2}}{1+b_1 y_{c2}}.$$

Здесь и далее в статье под *киберзащищенностью* будем понимать, по аналогии, например, с [5], способность АИС успешно выполнять предусмотренные задачи при сохранении безопасного состояния в условиях кибератак, направленных на нанесение ущерба критически важным или потенциально опасным объектам, или объектам, представляющим повышенную опасность для жизни и здоровья граждан, имущества физических или юридических лиц, экономики, окружающей среды. Причем полагая, что первая зависит как от возможностей несанкционированного доступа к системе (НСД) вероятного нарушителя, так и от недекларированных возможностей (НДВ) программных и аппаратных средств АИС.

Разумеется, не только вышеуказанные критерии (1) и (2) могут быть использованы (и, как предполагается, определены наряду с их значениями и их весов, в т.ч., методом экспертных оценок) – в нашем случае в ракурсе подхода РИПСА, методов ELECTRE. Не считая страховой защиты АИС, не исключено, что можно было бы ограничиться иногда и этими двумя. Учитывая, что они достаточно универсальны в плане киберзащищённости АИС и информации (как хранящейся в АИС, так и обрабатываемой с их помощью) – что видится из известных книг – однако и ряд других реалистично и уместно использовать с вышеприведённым набором критериев в целях: настоящей статьи и большей объективности выбора. Далее ввиду того, что область их применения далеко не ограничивается каким-либо одним направлением, а подходит к выбору самых различных АИС в упомянутом разрезе, дополним (1), (2) и (3) таковыми:

IV) среднее время проникновения нарушителя в АИС $K_{\text{IV}} \equiv \bar{t}_{\text{пр}}$;

V) стоимость создания или модернизации подсистемы защиты информации $K_{\text{V}} \equiv S$.

Кроме того, при выборе АИС должен учитываться и функционал системы. Поэтому дополним предыдущие 5 критериев I) – V) еще и таким:

VI) интегральный показатель (функциональной) эффективности АИС

$$K_{\text{VI}} \equiv A = \sum_{i=1}^{N} A_i = \sum_{i=1}^{N} \frac{V_i}{T_i} = \sum_{i=1}^{N} \frac{\left(\sum_{j=1}^{m}\theta_j + \sum_{k=1}^{\xi}\delta_k\right)_i}{\left(\sum_{k=1}^{\xi} t_k - \sum_{j=1}^{m}\tau_j\right)_i}, \quad (4)$$

где V_i – суммарный объем информации, подготовленный i-м блоком АИС за определенный период времени и представленный в каких-либо универсальных единицах измерения информации;

T_i – интервал времени, характеризующий длительность подготовки i-м блоком АИС суммарного объема информации;

N – число блоков АИС, задействованных в реализуемом в АИС информационном процессе;

θ_j – объем информации, поступившей на i-й блок АИС от j-го источника информации;

m – число источников информации;

δ_k – случайного либо неслучайного характера объем выданной информации i-м блоком АИС на информационную шину, удовлетворяющей требованию k;

ξ – общее число требований k;

t_k – момент времени, соответствующий выдаче подготовленной информации (отвечающей требованию k) i-м блоком на информационную шину АИС;

τ_j – момент времени, соответствующий поступлению информации на i-й блок АИС от j-го источника информации,

причем на знаменатель формулы (4) накладывается ограничение в виде

$$T_i = \left(\sum_{k=1}^{\xi} t_k - \sum_{j=1}^{m}\tau_j\right) \le T_{0i} \quad (5)$$

на длительность каждого T_i по отношению к его предельно допустимому верхнему значению T_{0i}.

Примечание. Величина δ_k способна иметь случайный характер вследствие того, что часть поступившей информации может не удовлетворять отдельному требованию k среди ξ таких требований.

Добавление интегрального показателя V) – критерия (4)–(5) – сообразно еще и потому, что, в т.ч., от функциональной конкретной структуры зависит (функциональная) эффективность АИС. Данный показатель был предложен в статье [6], причем – как в ней утверждается – в качестве универсального показателя для оценки технико-эксплуатационных, технологических, прагматических, экономических и др. качеств АИС. Этот интегральный показатель эффективности A, как отмечается в [6], является функциональной характеристикой, которую можно повышать, совершенствуя техническую базу АИС и используя труд квалифицированных сотрудников. Приведенный показатель – указывающий и на то, что обесценение информации суть равнозначный результат недостаточно полного ее объема и ее запаздывания – отображает в равной мере временные и количественные (в разрезе количественных мер информации) факторы. Несмотря на невозможность учесть и этим одним показателем изменяющиеся (в самом процессе принятия решений) предпочтения ЛПР, как и все проблемы киберзащищенности, отметим следующее. При наличии в той или иной альтернативной АИС, например, всего N=6 функциональных блоков (подсистем) – отбора информации, преобразования информации, передачи информации, обработки информации, хранения информации, поиска информации – такого рода перечень структурных элементов системы является открытым. Он во многом зависит от круга задач, стоящих перед АИС и вполне способен повлечь изменение ее конфигурации и состава – в т.ч., при необходимости ее модернизации.

Практически значимы и затраты времени проникновения нарушителя в системы – пусть хотя бы в среднем, и затраты в абсолютном стоимостном выражении не только на создание, но и модернизацию соответствующей подсистемы АИС. Тем не менее, поскольку ни одна даже очень дорогостоящая АИС, АСОИУ (автоматизированная система обработки информации и управления), АСЗОИ не дает гарантии полной абсолютной защиты от НСД и НДВ – влекущих киберугрозы и кибератаки, в дополнение к организационно-техническим, программным и/или т.п. имеющимся мерам защиты следует учесть и страховую защиту.

Имеет смысл принять во внимание и следующее: например, из [4] известно, что для одинакового ущерба простой технической системе достаточно нанести меньше вреда, чем интеллектуальной – в силу наличия у последней запаса безопасности.

Страховая защита должна служить для АИС вспомогательным, но немаловажным рубежом, когда предшествующие уже пройдены нарушителем. Этот уровень защиты нередко игнорируется, что лишь отчасти связано с не очень большой распространенностью страхования подобных рисков. Хотя даже при наличии т.н. франшизы (как вариант, условной, т.е. когда по условиям страхового договора предусмотрено освобождение страховой компании от возмещения ее клиенту убытков, не превышающих определенного размера [7]), пренебрегать им вряд ли следует, полагаясь на идеальность прочих видов защиты.

Как справедливо отмечается в [8], сложность оценки количественных преимуществ киберстрахования может усугубляться: во-первых, широко распространенным отсутствием понимания того, какие события может покрывать киберстрахование и – как следствие – ошибочным мнением, что прочие виды страхования покроют убытки от киберинцидента; во-вторых – тем, что для многих юридических лиц характерна неосознанность того, насколько они уязвимы для кибератак, приводящая к принципиально неверному организационно-управленческому и т.п. решению о ненужности для них киберстрахования.

Чаще всего объектами киберстрахования по корпоративным программам, как известно, например, из [9], являются имущественные интересы клиента. Они могут быть связаны с такими рисками, как: наступления ответственности за причинение ущерба имуществу физических и (или) юридических лиц; несения непредвиденных расходов; наступления убытков от перерывов в производстве. В то время как отдельная страховка рисков кибератак в РФ является более редкой. Известные российские страховщики, в т.ч., этой разновидности: «АльфаСтрахование», «СбербанкСтрахование», «Согаз», «Альянс» и др. Для базовой программы страхования характерны охватываемые ею риски: утраты и искажения информации и обрабатывающего ее ПО, нарушения конфиденциальности, целостности и (или) доступности персональных данных, расследования и диагностики кибератак, хищения интеллектуальной собственности, вымогательства, ущерба деловой репутации и т.д.

Например, автор [10] выделяет как в отдельную группу риски, связанные с: реагированием на киберинциденты, ликвидацией последствий, финансовыми и иными расследованиями, аудитом безопасности и судебным урегулированием.

В любом случае, как отмечается, например, в [11], для большинства страховщиков киберрисков важнейшую роль играет сетевая компьютерная безопасность. Что вполне естественно, учитывая, что с бурным развитием вычислительных сетей существенно повышаются и шансы успешных кибератак через них.

Следует отметить, что стоимость программы страхования зависит не только от количества и набора покрываемых рисков, величин страхового покрытия и франшизы (при ее наличии), но и сфер(ы) деятельности клиента и др. факторов. Например [12], европейскими страховщиками принимаются во внимание при киберстраховании:

а) стоимость объекта страховой защиты (и чем она выше, тем страховая ставка ниже);

б) наличие средств (подсистемы) защиты информации, в т.ч., антивирусных программ (и чем более положительно себя зарекомендовали используемые средства

и подсистема защиты информации и чем большей они стойкости к атакам, тем ниже страховой тариф);

в) количество атак на страхователя, а также на др. компании той же либо схожей отрасли за тот же значимый период.

Для учета также страховой защиты видится уместным дополнительный разносторонний критерий, который, впрочем, может несложным и даже интуитивно понятным образом строиться на основе трехзначной мажоритарной логики – в ракурсе как нефинансовых особенностей, вариантов систем, так и финансовых, вводимых в следующем п. 1 операцией (6).

Однако даже в случае, если учитывать величины страховых взносов в самом критерии (показателе) I) в составе его величины ΔR, имело бы смысл такие нюансы, как наличие франшизы, наличие перестрахования (особенно для крупных информационных рисков больших, распределенных АИС) и т.п. учесть обособленным критерием (показателем).

Кроме того, отнюдь не следует «сбрасывать со счетов» и то обстоятельство, что процесс принятия решения (хотя и необязательно) одним ЛПР – пусть и в присутствии консультанта, усложняется и/или замедляется из-за изменений предпочтений ЛПР в самом процессе принятия решения. Эти изменения часто могут быть неоднократными, постепенными. Сказанным вновь подчеркнута уместность и востребованность в нашем случае именно методов группы ELECTRE: с учетом различных защитных мер и параметров при иных подходах весьма сложно в принципе принять решение в задачах многокритериального выбора АИС. В то время как проблемные вопросы, связанные с ацикличностью отношений между альтернативами – в случае появления такого цикла, включающего последние – как известно из [1] – несложным образом решаются при объявлении входящих в цикл альтернатив эквивалентными.

Цель исследования: выяснить и показать применимость подхода РИПСА на примере одного из методов ELECTRE – для выбора автоматизированных информационных систем при полагаемых приоритетными критериях, относящихся к киберзащищенности АИС с учетом страхования киберрисков.

Задачи исследования:

- выяснить и показать возможность применения метода ELECTRE I как одного из способов обоснования выбора наиболее защищенных АИС с учетом страхования киберрисков;

- разработать и/или модифицировать критерий, основанный на трехзначной мажоритарной логике, позволяющий выразить (учесть) в логико-математическом виде те или иные – хотя бы некоторые либо основные – особенности страховой защиты АИС в связи с присущими им киберрисками, а также способность АИС противостоять собственными средствами тем или иным кибератакам на подобные системы;

- посредством решения предыдущих задач исследования выяснить и показать более широкую применимость критерия (критериальной базы) на основе трехзначной мажоритарной логики, чем: а) только в ракурсе технических и/или организационно-технических параметров либо характеристик киберзащищенности АИС и б) только в ракурсе финансово-экономических или финансовых параметров либо характеристик киберзащищенности страхуемых АИС.

1. Методы

Вполне подходящим из известной и вышеупомянутой группы методов ELECTRE является метод ELECTRE I, подробно изложенный в известных книгах[1]. С учетом вышесказанного во Введении, опишем его на примере (с достаточной степенью детализации для решения поставленных задач), как и упомянутые для этого критерии. Прежде проясним формирование и смысловые особенности обоих логико-математических критериев а), б), указанных во Введении.

Как известно из [13–14], может быть построен трехстабильный мажоритарный элемент с 3 входами и одним выходом, причем при значениях входных сигналов –1, 0 или 1 выходной сигнал такого элемента принимает одно из 3-х вышеуказанных значений -1, 0 или 1 в зависимости от алгебраической суммы входных сигналов. Имея выходным сигналом y, а входными x_1, x_2, x_3, получаем трехместную операцию (3-значную мажоритарную функцию):

$$y = sign_3\left(x_1 + x_2 + x_3\right) = \begin{cases} 1, \ если \ \ x_1 + x_2 + x_3 \geq 1, \\ 0, \ если \ \ x_1 + x_2 + x_3 = 0, \\ -1, если \, x_1 + x_2 + x_3 \leq -1. \end{cases} \quad (6)$$

Назовем обозначаемый через y логико-математический критерий VII) на основе операции (6), добавляемый к I)–VI): «*трехзначный мажоритарный критерий киберзащищенности АИС с учетом страхования*». Тогда пусть его смысловыми составляющими будут следующие, соответственно обозначенные: x_1=1 – «противостояние АИС всем известным кибератакам и киберугрозам»; x_1=0 – «противостояние АИС получившим известность кибератакам и киберугрозам, представляющим существенную опасность»; x_1=–1 – «противостояние АИС только самым известным кибератакам и киберугрозам»; x_2=1 – «сильная способность АИС самообучения при кибератаках»; x_2=0 – «слабая способность АИС самообучения при кибератаках»; x_2=–1 – «нет способности АИС самообучения при кибератаках»; x_3=1 – «нет франшизы при наличии перестрахования»; x_3=0 – «есть франшиза и/или нет перестрахования»; x_3=–1 – «страхования нет вовсе».

Естественно, что страховые компании обычно не страхуют риски, включая и такие, как киберриски, связанные с весьма вероятными или почти достовер-

[1] Как, например: Ларичев О.И. Теория и методы принятия решений, а также Хроника событий в Волшебных странах: Учебник (Гриф Министерства образования РФ). Изд. третье, перераб. и доп. Москва: Университетская книга, Логос; 2006. 392 с.

ными страховыми событиями – что и было принято здесь во внимание в ракурсе интегрального критерия *y* трехзначной мажоритарной логики. Т.е. позволившего (быть может, несколько своеобразно) объединить в рамках такового практически неизбежно соотносящиеся между собой показатели x_1, x_2, x_3, как и их значения. Тем более, т.к. видится важным учитывать нынешнюю распространенность искусственного интеллекта (ИИ) с самообучением систем. Здесь, например, значения x_2=1 и x_2=0 символизируют и характеризуют наличие соответственно «сильного» и «слабого» ИИ у более сложных «интеллектуальных» АИС, что может проявляться при защите от кибератак; нижнее значение x_2=–1 соответствует наиболее простым АИС вообще без ИИ.

Что же касается франшизы, которая, как ясно, например, из [6], может быть как безусловной, так и условной, то она не во всем выгодна клиенту-страхователю. Это связано с тем, что при безусловной франшизе при наступлении страхового случая страховое возмещение будет меньше, а при условной франшизе при малых ущербах (до определенного в договоре порогового уровня) у страховых компаний обычно нет обязательств по его выплате.

Относительно перестрахования рисков отметим, что оно – как видно, например, из [7] и [15] тем более актуально – и соответственно имеет место при тем большем количестве перестрахователей и перестраховщиков для повышения уровня страховых гарантий, чем более крупные риски страхуются прямым страховщиком (т.е. непосредственно связанной договором с клиентом страховой компанией). Ныне не вызывает сомнений важность обеспечения стабильной страховой защиты, которая для киберрисков при их страховании влечет если не обязательность, то предпочтительность перестрахования хотя бы одним перестраховщиком (по сравнению с его отсутствием).

На рис. 1 указан граф процесса многокритериального выбора АИС на основе метода ELECTRE I в достаточно общем случае с учетом, в т.ч., киберзащищенности и страхования, охватывающий и частный случай данного примера. Причем вершины (этапы, подпроцессы) с номерами 1–11 на этом графе означают следующее:

1 – формирование множества всего *N* критериев многокритериального выбора АИС, учитывающих, в т.ч., киберзащищенность и страхование АИС при использовании критерия на основе 3х-значной мажоритарной логики;

2 – формирование множества альтернатив для выбора наилучшей АИС;

3 – назначение весов критериям либо консультантом-экспертом, либо опросом нескольких экспертов, либо по числу голосов членов экспертного жюри, поданного за важность каждого критерия;

4 – разбиение множества критериев на 3 подмножества:

I^+ – подмножество критериев, по которым альтернатива A_i предпочтительнее, чем A_j;

$I^=$ – подмножество критериев, по которым альтернативы A_i и A_j равноценны;

I^- – подмножество критериев, по которым альтернатива A_j предпочтительнее, чем A_i;

5 – подсчет индексов согласия $C_{A_iA_j}$ о превосходстве гипотезы A_i над A_j;

6 – подсчет индексов несогласия $d_{A_iA_j}$ о превосходстве гипотезы A_i над A_j;

7 – задание уровней (коэффициентов) согласия α_q ЛПР с участием консультанта (где $q \geq 1$ – номер действующего уровня (коэффициента) по его хронологическому порядку);

8 – задание уровней (коэффициентов) несогласия γ_q ЛПР с участием консультанта (где $q \geq 1$ – номер действующего уровня (коэффициента) по его хронологическому порядку);

9 – проверка выполнения нестрогого неравенства для каждого из индексов согласия $C_{A_iA_j}$ по отношению к заданному уровню (коэффициенту) согласия α_q, т.е. $C_{A_iA_j} \geq \alpha_q$;

10 – проверка выполнения нестрогого неравенства для каждого из индексов несогласия $d_{A_iA_j}$ по отношению к заданному уровню (коэффициенту) несогласия γ_q, т.е. $d_{A_iA_j} \leq \gamma_q$;

11 – выбор наилучшей альтернативы (АИС) при соблюдении предъявляемых условий.

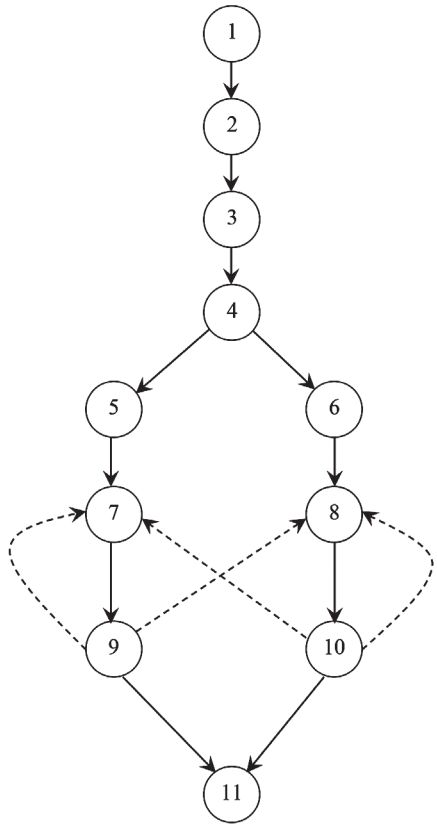


Рис. 1. Граф процесса многокритериального выбора АИС на основе метода ELECTRE I с учетом, в т.ч., киберзащищённости и страхования

Примечание. При успешном отыскании наилучшей альтернативы (АИС) указанные на рис. пунктиром переходы выполнять необязательно, хотя возможно в исследовательских, аналитических и т.п. целях.

Пример. Пусть дана группа из n=3 альтернатив A_i и N = 5 критериев, предназначенных для оценки этих A_i. При этом каждая из A_i характеризуется оценкой по каждому из 5-ти критериев, полученной от экспертов. Требуется в процессе выбора одной из АИС (A, B, D): выделить лучшую альтернативу A_i, построив для этого (на основе принципов конкорданса и дискорданса) один либо более таких индексов попарного сравнения альтернатив, что им отводится роль решающих правил.

Допустим, что альтернативы таковы: A(0,9; 0,15; 50 тыс.евро; 2 мес.; 3 тыс.евро; 90 Мбайт/час; –1); B(1; 0,3; 97 тыс.евро; 4 мес.; 5 тыс.евро; 450 Мбайт/час; 0); D(0,8; 0,4; 65 тыс.евро; 3 мес.; 4 тыс.евро; 120 Мбайт/час; +1), а (тоже экспертно оцененные) веса критериев соответственно: w_1=7, w_2=6, w_3=5, w_4=4, w_5=3, w_6=2, w_7=1, разброс оценок по критериям исчерпывается данными в табл. 1.

Табл.1. Разброс оценок вариантов АИС

Обозначения критериев	Наихудшее значение критерия	Наилучшее значение критерия
$K_{\text{I}} \equiv K_{\text{з}}$	0 (или 0 %)	1 (или 100 %)
$K_{\text{II}} \equiv \tilde{R}$	0,6 (или 60 %)	0 (или 0 %)
$K_{\text{III}} \equiv S_{\text{тх}}$	2 (тыс. евро)	98 (тыс. евро)
$K_{\text{IV}} \equiv \bar{t}_{\text{пр}}$	1 (мес.)	18 (мес.)
$K_{\text{V}} \equiv S$	6 (тыс. евро)	2 (тыс. евро)
$K_{\text{VI}} \equiv A$	80 (Мбайт/час)	560 (Мбайт/час)
$K_{\text{VII}} \equiv y$	-1	+1

Руководствуясь табл. 1, получаем такие длины шкал L_z (при $z = \overline{1,7}$):

L_1=1–0=1 или L_1=100–0=100 (%), L_2=0,6–0=0,6 или L_2=60–0=60 (%),

L_3=98–2=96 (тыс. евро), L_4=18–1=17 (мес.), L_5=6–3=3 (тыс. евро),

L_6=560–80=480 (Мбайт/час), L_7=1–(–1)=1+1=2.

Используя известные (общие для метода ELECTRE I) формулы, задействованные и в [3], определим сначала индексы согласия (конкорданса) – с гипотезой о превосходстве альтернативы A над альтернативой B и соответственно B над A. Т.к. A превосходит B по двум критериям K_{II} и K_{V}, в то время как B превосходит A по пяти K_{I}, K_{III}, K_{IV}, K_{VI} и K_{VII}, то получаем формулы примера:

$$C_{AB} = \frac{w_2 + w_5}{w_1 + w_2 + w_3 + w_4 + w_5 + w_6 + w_7},$$

$$C_{BA} = \frac{w_1 + w_3 + w_4 + w_6 + w_7}{w_1 + w_2 + w_3 + w_4 + w_5 + w_6 + w_7}.$$

Фигурирующие в тех же источниках (общие для метода ELECTREI) формулы позволяют определить соответствующие индексы несогласия (дискорданса), причем обычно для всех индексов: $0 \le C_{A_iA_j} \le 1, 0 \le d_{A_iA_j} \le 1$.

Результаты вычислений всех индексов согласия/несогласия сведены в табл. 2 в следующем п. 2, там же сделан обоснованный вывод о выбранной наилучшей альтернативе – при выдвинутых ЛПР уровнях согласия α_1=0,6 и несогласия γ_1=0,7 для данного примера (учитывая, что обычно $0<\alpha<1$, $0<\gamma<1$).

2. Результаты и обсуждение

Итак, как видно из результатов табл. 2, при выполнении характерных для метода ELECTRE I условий типа нестрогих неравенств $C_{A_iA_j} \ge \alpha_1$ и $d_{A_iA_j} \le \gamma_1$ (где выдвинутые ЛПР при помощи эксперта-консультанта значения α_1=0,6, γ_1=0,7), им обоим соответствует только альтернатива B. Две другие, а именно A и D, уступают ей; в ракурсе рассмотренного примера при заданных значениях единственная B превосходит эти остальные. Поэтому альтернатива B – наилучшая.

Табл. 2. Индексы согласия/несогласия для примера

Альтернатива	A		B		D	
A	*		0,321	0,75	0,571	1
B	***0,678***	***0,5***	*		***0,857***	***0,5***
D	0,428	0,417	0,143	0,688	*	

Особенно принимая во внимание, в т.ч., фигурирующее в ней наивысшее из возможных значение критерия $K_{\text{I}} \equiv K_{\text{з}} = 1$. Учитывая его наибольший среди всех вес w_1=7, такой результат видится естественным, хотя выбранная здесь АИС и дороже других. Однако вес стоимостного критерия $K_{\text{V}} \equiv S$ экспертно оценен ниже первых четырех большего приоритета, что также сыграло важную роль в пользу выбора альтернативы B.

Критериев могло быть больше на две единицы в случае попытки заменить предложенный критерий трехзначной логики, а именно тремя его раздельными критериальными составляющими без использования таковой. Однако с увеличением количества критериев на 2 ситуация с принятием решения стала бы гораздо более труднообозримой, тем самым только усложняя его процесс (в случае повышения изначального количества 7-ми критериев до 9-ти оно было бы более чем на 25%).

Видится также, что страхование киберрисков могло бы сыграть одну из ведущих ролей, но при куда более высоких экспертных оценках веса относящегося к нему критерия $K_{\text{VII}} \equiv y$. К этому следовало бы стремиться, в т.ч., всесторонне активизируя познавательную и просветительскую деятельность в сфере страхования, его возможностей и смежных вопросов. В перспективе развивая его сферу как таковую.

Заключение

Итак, цель статьи достигнута, а ее задачи выполнены. *Научная новизна* статьи заключается в следующем:

- выяснена применимость подхода РИПСА в виде метода ELECTRE I для выбора автоматизированных информационных систем в ракурсе рассмотренных – и небезосновательно полагаемых среди приоритетных –

критериев, относящихся к киберзащищенности АИС с учетом страхования киберрисков;

- разработан модифицированный, новый в плане киберзащищенности при страховании киберрисков критерий качества технико-экономического характера, основанный на 3-хзначной мажоритарной логике – а именно позволивший выразить и учесть в логико-математическом виде: некоторые особенности страховой защиты АИС в связи с присущими им киберрисками, а также способность АИС противостоять собственными средствами классифицируемым по трем категориям кибератакам на подобные организационно-технические системы.

Практическая ценность статьи состоит в:

- применимости критерия (критериальной базы) на основе трехзначной мажоритарной логики не только в ракурсе технических и организационно-технических параметров либо характеристик киберзащищенности АИС, но и в ракурсе финансово-экономических параметров либо характеристик защищенности страхуемых АИС;

- применимости метода группы ELECTRE подхода разработки индексов попарного сравнения альтернатив, причем как в ракурсе анализа и организационно-технических мер по снижению различных связанных с АИС киберрисков, так и в ракурсе страховой защиты от них – на случаи преодоления первичных иных рубежей защиты;

- возможности обойтись на 2 единицы меньшим количеством критериев (в рассмотренном на примере случае всего 7 критериев вместо 9 критериев) за счет разработанного (дополнительного) интегрального критерия трехзначной мажоритарной логики для многокритериальных альтернатив (по сравнению с неиспользованием такого критерия);

- при практическом применении результатов и материалов статьи – в улучшении условий управленческого труда лиц, принимающих организационно-управленческие, организационные и т.п. решения с многокритериальным выбором АИС путем его рационализации, а именно: повышении системности трудового процесса принятия решений и его обоснованности, объективности и достоверности наряду с его упрощением и адаптацией условий труда ЛПР, с учетом индивидуальных особенностей в виде предпочтений при участии консультанта.

Отметим, что для удобства расчетов и выбора – при нескольких критериях и числах, существенно превышающих рассмотренные в примере – имеет смысл использовать табличные, стандартные возможности MS Excel (чаще всего имеющегося практически на каждой ЭВМ).

Одно из возможных направлений дальнейших исследований – вопросы, связанные с применением предложенного критерия (критериальной базы) на основе трехзначной мажоритарной логики в ракурсе метода ELECTRE II и/или III.

Благодарности

Автор признателен своим прежним и нынешним вузам-работодателям: Финансовому университету при Правительстве РФ, где была начата данная работа после аттестации в должности доц., и продолжена в указанной должности в Российском Государственном гуманитарном университете, Московском Государственном лингвистическом университете и Московском гуманитарном университете за материальное стимулирование, периодическое премирование научной деятельности.

Список литературы

1. Анич И., Ларичев О.И. Метод ЭЛЕКТРА и проблема ацикличности отношений альтернатив // Автоматика и телемеханика. 1996. № 8. С. 108-118.

2. Roy B. Multicriteria Methodology for Decision Aiding. Dordrecht: Kluwer Academic Publisher, 1996. 303 p.

3. Шептунов М.В. Применимость метода ELECTRE I для оценки многокритериальных альтернатив в задачах выбора принципа управления доступом к музейным цифровым копиям // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 4. С. 62-71. DOI: 10.28995/2686-679X-2020-4-62-71

4. Лобач Д.И. О некоторых случаях количественной оценки ущерба технической системе // Надежность. 2024. Т. 24. № 4. С. 58-64. DOI: 10.21683/1729-2646-2024-24-4-58-64

5. Гапанович В.А., Розенберг Е.Н., Шубинский И.Б. Некоторые положения отказобезопасности и киберзащищенности систем управления // Надежность. 2014. № 2. С. 88-100. DOI: 10.21683/1729-2646-2014-0-2-88-100

6. Яшин В.Н. Оценка эффективности автоматизированных информационных систем // Вестник Самарского Государственного технического университета. Сер. Технические науки. 2017. № 3(55). С. 43–49.

7. Страхование от *А* до *Я* / Под ред. Л.И. Корчевской, К.Е. Турбиной. М.: ИНФРА-М, 1996. 624 с.

8. Бутакова Н.А. Стимулы обеспечения кибербезопасности и роль киберстрахования // Пермский юридический альманах. Научный журнал. М.: Статут, 2025. С. 211–221.

9. Просветова А.А., Дубкова Е.В. Кибер-страхование как способ обеспечения информационной безопасности // Международный журнал гуманитарных и естественных наук. 2020. № 4-3(43). С. 138–141. DOI: 10.24411/2500-1000-2020-10411

10. Крупенко Ю.В. Киберриски и теоретические основы киберстрахования // Проблемы современной экономики: глобальный, национальный и региональный контекст: сб. науч. ст. / ГрГУ им. Янки Купалы; редкол.: М.Е. Карпицкая (гл. ред.) [и др.]. Гродно: ГрГУ, 2022. С. 249-257.

11. Борисов Н.М., Адамчук Н.Г. Киберстрахование как инструмент обеспечения кибербезопасности // Страховое дело. 2020. № 4. С. 21–25.

12. Волкова Т.А., Суслякова О.Н. Страхование информационных рисков (киберстрахование) // Инновационная экономика: перспективы развития и совершенствования. 2018. № 7(33). Т.1. С. 117–122.

13. Варшавский В.И. Трехзначная мажоритарная логика // Автоматика и телемеханика. 1964. № 25(5). С. 673-684.

14. Овсиевич Б.Л. Некоторые свойства симметрических функций трехзначной логики // Проблемы передачи информации. 1965. № 1(1). С. 57-64.

15. Шептунов М.В. Страхование и новое научное направление: методы оперативного рационального перестрахования особо серьезного риска на базе эволюционных алгоритмов // Сборник работ победителей национального конкурса научных и инновационных работ по теоретической и прикладной экономике. СПб.: Первый класс, 2012. 156–167 с.

References

1. Anich I., Larichev O.I. [ELECTRA method and the problem of acyclicity of relations of alternatives]. *Automation and Remote Control*. 1996;57(8):1154–1162.

2. Roy B. Multicriteria Methodology for Decision Aiding. – Dordrecht: Kluwer Academic Publisher; 1996. 303 p.

3. Sheptunov M.V. [Applicability of the ELECTRE I method for evaluating multi-criterional alternatives in problems of choosing of a principle of access control to museum digital copies]. *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*. 2020;4:62–71. (in Russ.)

4. Lobach D.J. On some cases of quantitative estimation of damage to a technological system. *Dependability*. 2024;24(4):58–64. DOI: 10.21683/1729-2646-2024-24-4-58-64. (in Russ.)

5. Gapanovich V.A., Rozenberg E.N., Shubinsky I.B. Some concepts of fail-safety and cyber protection of control systems. *Dependability*. 2014;(2):88–100. DOI: 10.21683/1729-2646-2014-0-2-88-100. (in Russ.)

6. Yashin V.N. Evaluation of efficiency of automated information systems . *Vestnik of Samara State Technical University. Technical Sciences*. 2017;3(55):43–49. (in Russ.)

7. Insurance from *A* to *Z*. Korchevskaja L.I., Turbina K.E., ed. Moscow: INFRA-M, 1996. 624 p. (in Russ.)

8. Butakova N.A. Cybersecurity incentives and the role of cyber insurance. *Perm Legal Almanac*. – Moscow: Statute; 2025: 211–221. (in Russ.)

9. Prosvetova A.A., Dubkova E.V. Cyber insurance as method for ensuring information security. *International Journal of Humanities and Natural Sciences.* 2020; 4-3(43):138–141. DOI: 10.24411/2500-1000-2020-10411 (in Russ.)

10. Krupenko Y.N. Cyberrisks and theoretical foundations of cyberinsurance. *Problems of Modern Economy: Global, National and Regional Context: a collection of scientific articles / GrSU im. Janki Kupaly; ed. by M.E. Karpitskaya (chief ed.) et al. – Grodno: GrSU;* 2022; 249–257. (in Russ.)

11. Borisov N.M., Adamchuk N.G. The Ability of Insurers in the Cybersecurity Business. *Insurance business*. 2020; 4:21–25. (in Russ.)

12. Volkova T.A., Suslyakova O.N. Insurance of information risks (cyber insurance). *Innovative economy: prospects for development and improvement*. 2018;7(33):1:117–122. (in Russ.)

13. Varshavsky V.I. [Ternary majority logic]. *Automation and Remote Control*. 1964;25(5):673–684. (in Russ.)

14. Ovsievich B.L. [Certain properties of symmetric functions in three-valued logic]. *Problems of Information Transmission*. 1965;1(1):57–64. (in Russ.)

15. Sheptunov M.V. [Insurance and the new scientific direction: methods of operational rational reinsurance of extra-severe risks on the base of the evolutionary algorithms]. *Collection of works by the winners of the national competition of the scientific and innovative works in theoretical and applied economics*. Saint-Petersburg: Pervyi klass. Publ., 2012:156–167. (in Russ.)

Сведения об авторе

Шептунов Максим Валерьевич – кандидат технических наук, доцент; доцент кафедры Международной информационной безопасности и член Ученого совета Института информационных наук МГЛУ (ИИН ФГБОУ ВО «Московский Государственный лингвистический университет»); доцент кафедры Прикладной информатики и статистики факультета Экономики, управления и международных отношений МосГУ (Московского гуманитарного университета); Москва, Российская Федерация; e-mail: triumf403@yandex.ru.

About the author

Maxim V. Sheptunov, Candidate of Engineering, Associate Professor; Associate Professor, Department of International Information Security, Member of the Academic Council, Institute of Information Science, MSLU (Moscow State Linguistic University); Associate Professor, Department of Applied Computer Science and Statistics, Faculty of Economics, Management and International Relations, MosUH (Moscow University for the Humanities); Moscow, Russian Federation; e-mail: triumf403@yandex.ru.

Вклад автора в статью

Шептунов М.В. Выяснена применимость подхода РИПСА в виде метода ELECTRE I для выбора АИС в ракурсе рассмотренных критериев, относящихся к киберзащищенности АИС, с учетом страхования киберрисков. Разработан модифицированный, новый в плане киберзащищенности при страховании киберрисков критерий, основанный на трехзначной мажоритарной логике. Сделаны выводы относительно разработанного критерия качества технико-экономического характера, причем имеющего не только самостоятельное значение, но и при его применении в методах группы ELECTRE подхода разработки индексов попарного сравнения альтернатив.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

УДК 004.052
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-61-68

Выявление системных неисправностей в программно-аппаратных комплексах на основе интеллектуальных технологий

Detecting system faults in hardware and software systems using intelligent solutions

Панков И.А.[1]*, Аверченко А.П.[1], Панков Д.А.[2]*
Pankov I.A.[1]*, Averchenko A.P.[1], Pankov D.A.[2]*

[1] *Омский государственный технический университет, Омск, Российская Федерация*
[2] *ООО «ЛАНИТ-ТЕРКОМ», Санкт-Петербург, Российская Федерация*
[1] *Omsk State Technical University, Omsk, Russian Federation*
[2] *LANIT-TERKOM LLC, Saint Petersburg, Russian Federation*
* *E-mail: pankovDDD@yandex.ru, pankov99ai@yandex.ru*

Панков И.А.

Аверченко А.П.

Панков Д.А.

Резюме. *Представлена система выявления неисправностей в распределенных программно-аппаратных комплексах, основанная на наборе интеллектуальных технологий. Подход объединяет динамическое тестирование (фаззинг), корректируемое большими языковыми моделями, а также анализ шаблонов уязвимостей известных баз знаний MITRE и OWASP для выявления программных ошибок, способствующих проведению потенциальных атак. Предложенная архитектура оперативно диагностирует отказы и сбои, локализует их причину и автоматически эскалирует инцидент системному администратору. Практическая значимость решения подтверждена экспериментально по таким параметрам, как среднее время обнаружения ошибок, охват кода, количество обнаруженных дефектов.*

Abstract. *The paper presents a system for detecting faults in distributed software and hardware systems that is based on a set of intelligent technologies. The method combines dynamic testing (fuzzing) enhanced with large language models, as well as analysis of vulnerability patterns of the well-known MITRE and OWASP knowledge bases to identify software errors that enable potential attacks. The proposed architecture promptly diagnoses failures and faults, localizes their causes and automatically escalates the incident to the system administrator. The practical significance of the solution is confirmed experimentally in terms of such parameters as the average error detection time, code coverage, and the number of detected defects.*

Ключевые слова: *обнаружение неисправностей, распределенные комплексы, отказы и сбои, фаззинг, большие языковые модели.*
Keywords: *fault detection, distributed systems, failures and faults, fuzzing, large language models.*

Для цитирования: *Панков И.А., Аверченко А.П., Панков Д.А. Выявление системных неисправностей в программно-аппаратных комплексах на основе интеллектуальных технологий // Надежность. 2025. №4. С. 61-68. https://doi.org/10.21683/1729-2646-2025-25-4-61-68*
For citation: *Pankov I.A, Averchenko A.P., Pankov D.A. Detecting system faults in hardware and software systems using intelligent solutions. Dependability 2025;4: 61-68. https://doi.org/10.21683/1729-2646-2025-25-4-61-68*

Поступила: *27.08.2025* / **После доработки:** *11.09.2025* / **К печати:** *28.09.2025*
Received on: *27.08.2025* / **Revised on:** *11.09.2025* / **For printing:** *28.09.2025*

Введение

Современные распределенные программно-аппаратные комплексы управления и связи представляют собой сложные системы, функционирование которых зависит от различных внутренних и внешних факторов. Система содержит несколько интерфейсов связи, таких как локальные сети, радиосвязь, беспроводные протоколы; также она состоит из центра управления и нескольких связных узлов (подсистем), которые географически распределены (рис. 1). Контроль устойчивости программно-аппаратного комплекса (ПАК) к отказам и сбоям в реальном масштабе времени является важной задачей для выполнения требований, заложенных в техническое задание на проектирование. Цель статьи – повысить эффективность поиска неисправностей и потенциальных уязвимостей в программах для ПАК за счет внедрения комплекса интеллектуальных технологий. В распределенном ПАК есть специальная программа, которая имитирует сбои и отказы, которая делает это не для одного устройства, а сразу для подсистем. В процессе разработки и эксплуатации ПАК для проверки его устойчивости применяют три основных метода: имитация неисправностей на программном уровне, сканирование аппаратного состояния устройств, акустический мониторинг (как дополнительный способ контроля техногенных событий). Эти методы позволяют собирать и анализировать комплексную информацию обо всех устройствах в подсистеме. Инъекторы неисправностей объединены в единую локальную сеть, что дает возможность централизованно управлять тестированием и передавать данные в модуль анализа и детектор атак. Традиционные методы диагностики часто недостаточно эффективны для оперативного определения причин отказов.

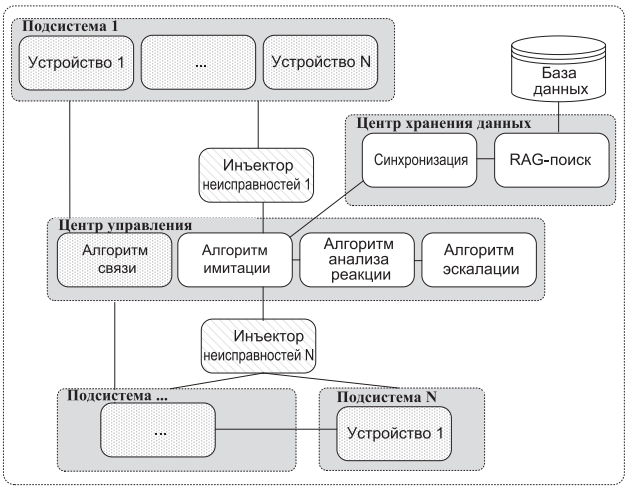
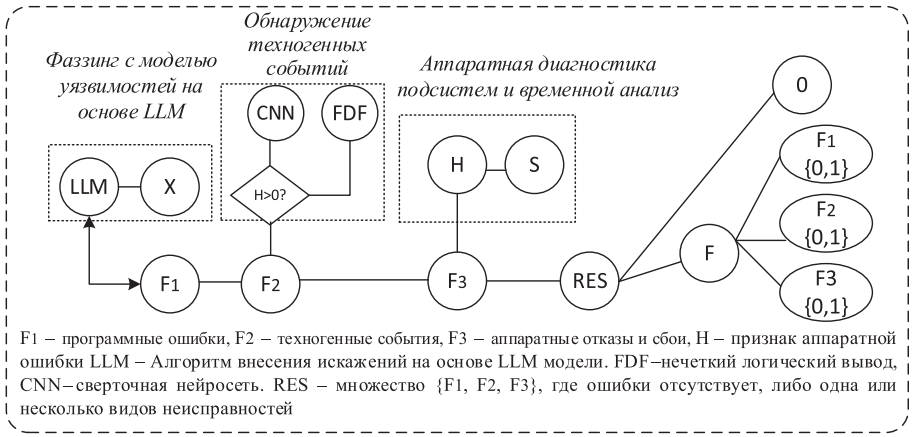


Рис. 1. Структурная схема ПАК

Проверка устойчивости к отказам и сбоям необходима ПАК не только в процессе разработки, но и во время эксплуатации. Это связано с двумя основными проблемами: структура распределенной системы постоянно меняется, когда добавляются или исключаются устройства, что требует непрерывного мониторинга и диагностики. Также стандартных средств диагностики в ряде случаев недостаточно, чтобы четко разделить программные и аппаратные отказы из-за высокой взаимосвязи компонентов. В данной статье наиболее подробно рассмотрен вопрос эффективного поиска неисправностей, которые вызваны программными дефектами. Для поиска программных ошибок комплекса используется фаззинг, которому для получения наилучших результатов охвата алгоритмов работы устройств необходимы входные данные. Часто получение таких данных затруднено в связи с особенностью тестирования или сложной структурой протоколов обмена [2] (рис. 2). Для генерации входных данных эффективно использовать алгоритмы больших языковых моделей (Large Language Models, LLM).

Предложенная система имитации позволяет детализировать причины отказов за счет анализа подсистем ПАК, которые возникают в процессе работы оборудования. Контроль осуществляется алгоритмом анализа реакции на имитируемые неисправности с помощью фаззинга. Алгоритм обрабатывает и интерпретирует данные на основе работы нейросети, а также методов нечеткого логического вывода, что обеспечивает более точное локализации дефекта (рис. 3).

Поскольку генерация данных применяет алгоритмы LLM, то следует уточнить, что подготовка структуры



F1 – программные ошибки, F2 – техногенные события, F3 – аппаратные отказы и сбои, H – признак аппаратной ошибки LLM – Алгоритм внесения искажений на основе LLM модели. FDF–нечеткий логический вывод, CNN–сверточная нейросеть. RES – множество {F1, F2, F3}, где ошибки отсутствует, либо одна или несколько видов неисправностей

Рис. 2. Схема фаззинга ПАК

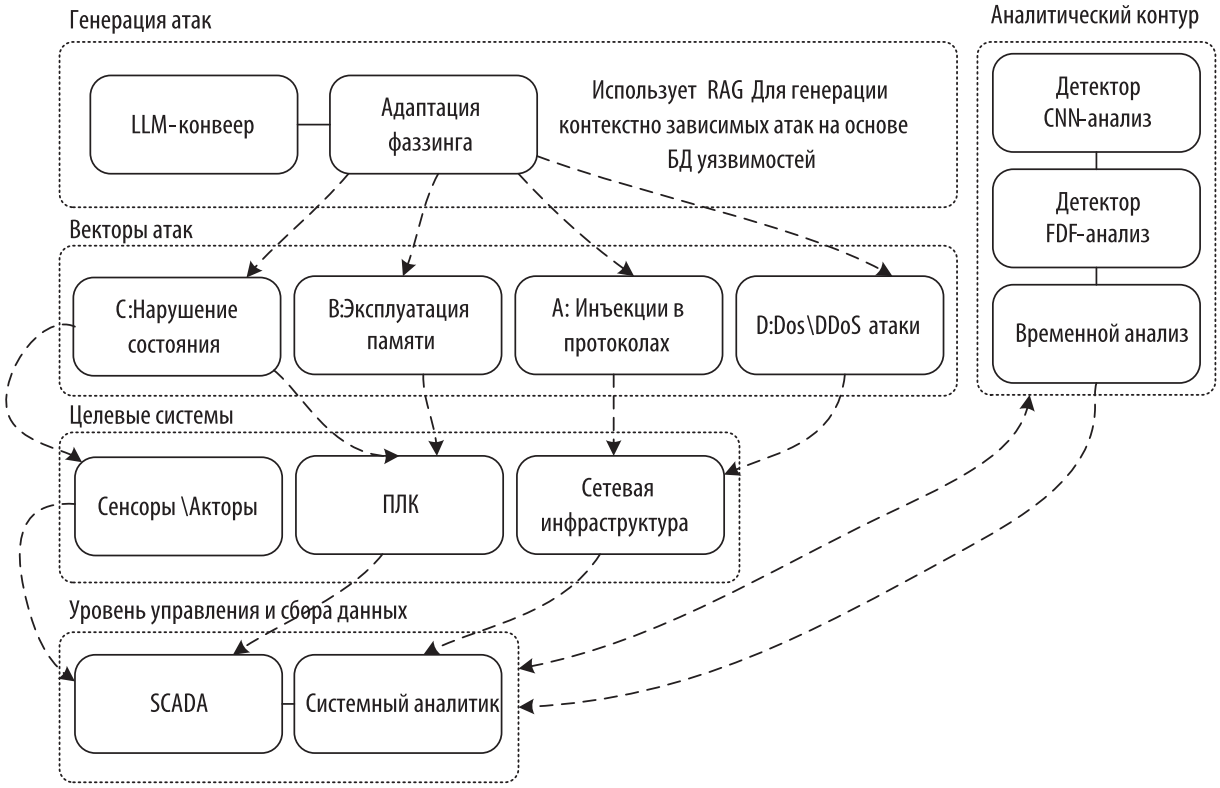


Рис. 3. Схема формирования векторов атак для подсистем ПАК с использованием базы знаний CVE

данных на вход алгоритмов фаззинга происходит с помощью алгоритма генерации, дополненного поиском – Retrieval Augmented Generation или RAG [2].

RAG-подход является формирование так называемого «вектора атаки», представляющего собой конкретное тестовое воздействие, нацеленное на проверку устойчивости системы к угрозам из баз знаний уязвимостей информационной безопасности CVE. Для этого RAG выбирает известные уязвимости из базы знаний для используемых в ПАК программных средствах и аппаратных модулях. С помощью семантического поиска, основанного на преобразовании текстовых запросов в векторные представления, осуществляется сопоставление с фрагментами информации из базы знаний по принципу семантической близости. В результате извлекаются наиболее релевантные описания уязвимостей, эксплойтов (программных модулей для эксплуатации уязвимостей) и атакующих шаблонов.

Применение заданной модели эффективно как для имитации неисправностей в памяти устройств, так и для искажения данных протоколов обмена между устройствами. Такой контекст является специфичным для текущей цели тестирования и существенно расширяет возможности LLM по генерации точных и применимых в конкретной ситуации тестовых данных. Генерация перестает быть абстрактной: модель синтезирует конкретные команды, сетевые пакеты, входные данные для фаззинга (направленного случайного тестирования) или сценарии эксплуатации, ориентированные на выявленные уязвимости.

1. Архитектура конвейера программного поиска дефектов

Поиск дефектов программ в ПАК реализован в виде конвейера, включающего обработку и генерацию данных, проведение фаззинга и анализ результатов с контролем выполнения по метрикам объема тестирования. Фаззинг представляет собой метод динамического тестирования программного обеспечения, при котором в систему подаются случайно сгенерированные или модифицированные входные данные с целью вызвать сбои, переполнения буфера, ошибки обработки или другое аномальное поведение программы [3]. В контексте распределенных систем этот подход позволяет проверять как отдельные компоненты, так и взаимодействие между ними, включая сетевые протоколы, интерфейсы, форматы обмена данными и аппаратные драйверы [3, 4]. Общий алгоритм включает подготовку данных с определением режимов испытания устройства согласно шаблону спецификации (*шаблон 1*), внесение отказов и сбоев в конечное устройство с изученным программным кодом с помощью техники фаззинга (*шаблон 2*). После чего осуществляется определение тестовых испытаний по имитации неисправностей на основе нечеткого логического вывода. Тестирование устройства производится путем искусственного внесения ошибок в программное и аппаратное обеспечение проверяемых устройств на основе тестовой документации и статистики ошибок, которые были обнаружены в период тестирования.

Для программно-аппаратных систем существует ряд ограничений по приросту объема тестирования в

процентах протестированного кода, который сложно обойти без применения дополнительных инструментов. Фаззинг используется совместно с алгоритмом LLM для улучшения процесса имитации неисправностей, что позволяет увеличить скорость и объем тестируемого кода. Алгоритм LLM формирует данные на вход работы алгоритма фаззинга, а также выходные данные фаззинга, которые поступают на вход работы алгоритма LLM для генерации новых шаблонов, которые позволяют проверить как устойчивость к обычных ошибкам программного обеспечения, так и для проверки устойчивости к модификации известных шаблонов атак [5, 6]. Приведем формальное описание процесса поиска ошибок программ ниже.

$\sum_x b_x \to \max$, где b_x – кумулятивный набор дефектов за счет применения тестовых наборов в распределенной программно-аппаратной системе для набора атакующих запросов на основе уязвимостей и дефектов устройств.

Для $c_{i,j}$ – i-й сбой или отказ при выполнении j-го искажения данных;

$A_{m(t)} = \{a_{q1}, a_{q2}, ..., a_{|a_{q|O|}}\}$ – набора атакующих запросов на основе уязвимостей и дефектов устройств;

$R_{m(t)} = \{r_{q1}, r_{q2}, ..., r_{|a_{q|O|}}\}$ – наборов реализованных дефектов с помощью объединения оригинальных шаблонов (O) и модифицированных;

$P = \{o_1, o_2, ..., o_{|O|}\} \cup \{g_1, ..., g_n\}$ – множество тестов программы для устройства ПАК.

Особенность подхода заключается также в способности к генерации сложных, многоэтапных сценариев атак, имитирующих реальные тактики, техники и процедуры, применяемые злоумышленниками. Такие сценарии трудно воспроизвести с помощью классических методов случайного фаззинга. Важным преимуществом является и высокая адаптивность RAG: по мере получения обратной связи от системы, например, через сигналы от сверточных нейронных сетей (Convolutional Neural Networks, CNN), временной анализ или методы нечеткой логики, происходит динамическое обновление контекста и формулировка новых запросов. Это позволяет уточнять и углублять исследование потенциальных векторов атак.

Процесс тестирования с использованием RAG включает несколько последовательно выполняемых этапов. Сначала, на основе полученного контекста, LLM генерирует конкретные тестовые воздействия [7, 8]. Эти воздействия затем автоматически применяются к тестируемой системе. Цикл тестирования обеспечивает улучшение качества воздействия и повышение вероятности выявления уязвимостей.

Для проведения исследования с помощью техники фаззинга представим в виде конвейера обработки для создаваемого ПАК (рис. 4).

Интеграция RAG осуществляется на этапе активного тестирования системы, где он взаимодействует с адаптивным фаззингом, управляемым LLM, а также инструментами временного анализа. Таким образом, обеспечивается интеллектуальное, контекстно-зависимое наполнение процесса генерации тестовых воздействий. Это напрямую способствует повышению точности классификации инцидентов информационной безопасности, снижению времени обнаружения целевых атак и увеличению охвата потенциальных уязвимостей.

Следует подчеркнуть, что целью использования RAG в данной архитектуре является не извлечение готовых ответов, а именно генерация интеллектуальных тестовых воздействий, синтезируемых на основе специализированного контекста, извлеченного из базы знаний. Вектор атаки представляет собой конкретную команду, пакет данных или скрипт, сгенерированный языковой моделью на основе актуальных сведений об уязвимостях. Автоматизированный цикл RAG совместно с LLM обеспечивает высокий уровень покрытия атакующих сценариев для исследуемых систем.

2. Применение алгоритмов LLM для улучшающих объема найденных ошибок с помощью фаззинга

Работа LLM в сочетании с фаззингом строится следующим образом. Сначала проводится сбор и предварительная обработка данных – собираются образцы входных сообщений, логи работы системы, специфи-

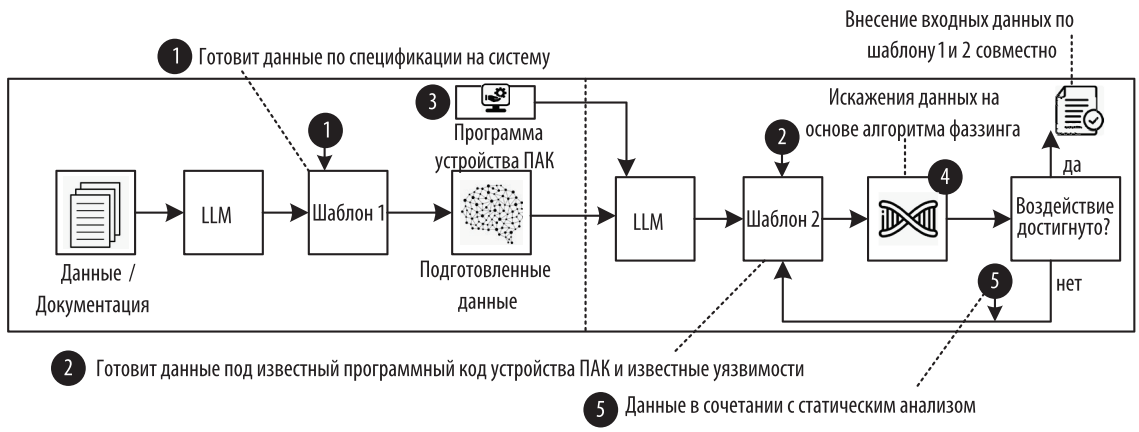


Рис. 4. Структурная схема конвейера генерации данных для устройств ПАК с использованием алгоритма LLM

кации протоколов и API. Эти данные используются для дообучения или тонкой настройки языковой модели, чтобы адаптировать ее под конкретную предметную область [9, 10]. Затем модель интегрируется в фаззинг-систему, которая вместо случайной генерации использует выход работы алгоритма LLM для создания более реалистичных и содержательных тестовых данных. Ключевое нововведение – LLM L определяет условную вероятность $P_L(i \mid C)$ для генерации нового входа i при наличии контекста C. Новый вход (i_{new}): Данные, которые будут поданы в программу P. Контекст C**:** информация, доступная модели для принятия решения. Контекст может включать:

• Исходный код программы P (полностью или частично).

• Начальный набор валидных входов (corpus S).

• Историю предыдущих сгенерированных входов $\{i_1, i_2, ..., i_{t-1}\}$.

• Информацию обратной связи: покрытие кода, отчеты о сбоях.

Таким образом, на каждом шаге t фаззинга LLM генерирует новый вход: $i_t \sim P_L(i \mid C_t)$

$$\max_{\theta} \mathrm{E}\left[\sum_{t=1}^{T} O(i_t)\right],$$

θ – это параметры LLM (или параметры запроса), для которого проводится оптимизация;

i_t – вход, сгенерированный на шаге t согласно $P_L(i \mid C_t; \theta)$;

$O(i_t)$ – результат проверки входа решающим алгоритмом;

E – математическое ожидание, которое учитывает вероятностный характер генерации входов.

Модель обучается на примерах корректных сообщений, передаваемых между компонентами системы, после чего генерирует тестовые данные, которые не только соответствуют синтаксису протокола, но и учитывают его семантические особенности. На этапе выполнения фаззинга система запускает тестовые случаи, сгенерированные моделью, после чего отслеживает реакцию программно-аппаратного комплекса. При этом используется обратная связь от мониторинговых и аналитических модулей, которые фиксируют покрытие кода, возникшие ошибки и нештатное поведение системы (рис. 5).

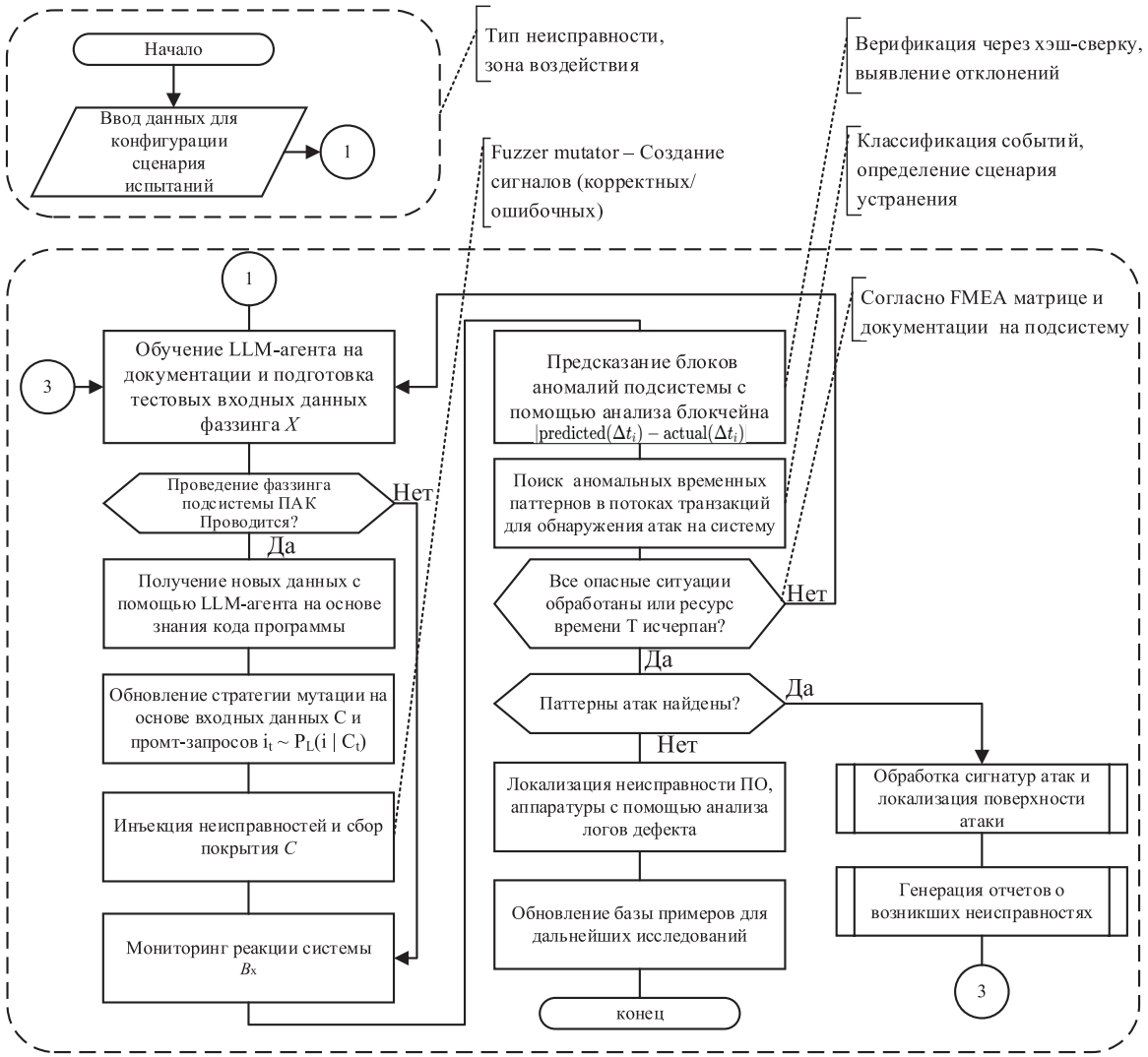


Рис. 5. Алгоритм имитации неисправностей на основе фаззинга с LLM коррекцией вектора атаки

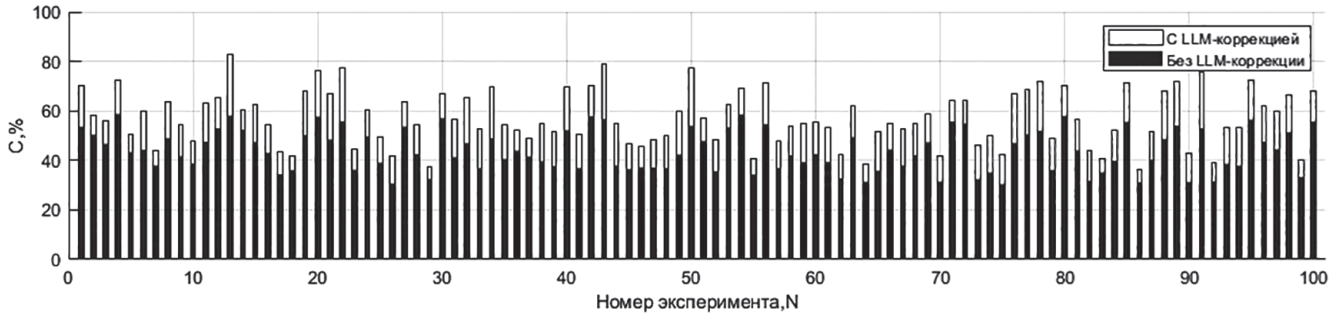


Рис. 6. Сравнение результатов покрытия кода *C*, %, алгоритмом фаззинга с LLM-коррекцией с алгоритмом фаззинга без LLM-коррекции.

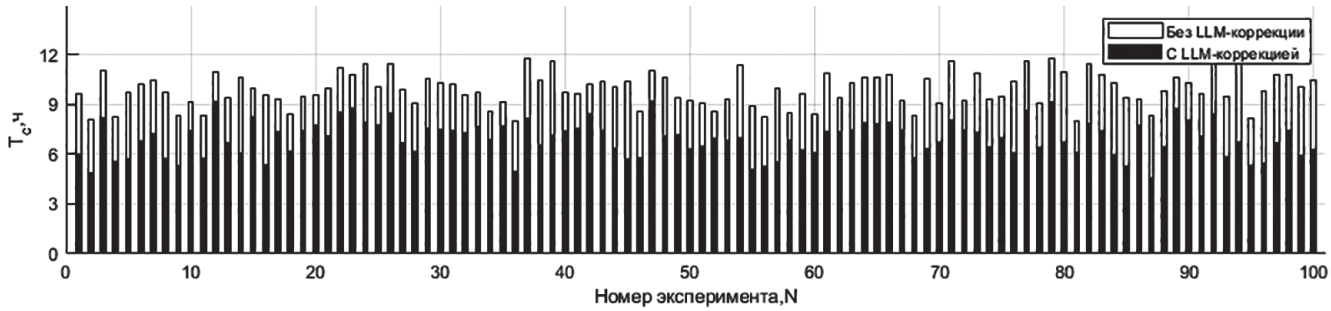


Рис. 7. Сравнение времени выполнения T_C, %, алгоритмом фаззинга с LLM-коррекцией с алгоритмом фаззинга без LLM-коррекции.

Эта информация поступает обратно к LLM, которая корректирует свои дальнейшие генерации, стремясь достигнуть максимального атакующего воздействия на исследуемую систему в виде количества отказов, сбоев и выявленных ошибок при минимальном количестве тестовых запусков. Кроме того, LLM используется для анализа результатов фаззинга. Модель способна интерпретировать логи, классифицировать типы найденных ошибок, выделять повторяющиеся паттерны и предлагать возможные пути исправления уязвимостей. Это особенно ценно в распределенных системах, где количество потенциальных точек отказа велико, а диагностика проблем требует глубокого понимания контекста.

Еще одной важной стороной использования LLM в фаззинге является возможность моделирования атаки на систему [11, 12]. Языковая модель может генерировать не просто одиночные атаки, а такие последовательности, которые имитируют цепочки вредоносных сценариев – например, попытки внедрения кода, перехвата управления, изменения состояния системы с захватом управления.

Такой подход усиливает фаззинг за счет привлечения знаний о современных методах эксплуатации уязвимостей и позволяет заранее находить и устранять потенциально опасные функции в системе [13].

Таким образом, интеграция языковых моделей в процесс фаззинга значительно повышает его практическую значимость, позволяя проводить тестирование более направлено и адаптивно (рис. 6 и 7) для тестирования подсистемы ПАК с тремя устройствами в условиях реальной эксплуатации. Сочетание RAG для интеллектуального доступа к данным, базы знаний MITRE для анализа угроз и базы знаний OWASP для обеспечения безопасности приложений, позволяет создать комплексную систему управления ПАК, которая не только автоматизирует рутинные задачи, но и обеспечивает понимание структуры данных и поведения системы в условиях постоянно меняющихся киберугроз [14, 15].

Заключение

Предложенная в работе система выявления неисправностей для распределенных ПАК основана на использовании фаззинга совместно с подготовкой данных тестирования с применением алгоритмов больших языковых моделей, что позволило повысить устойчивость распределенного ПАК к отказам и сбоям за счет увеличения количества обнаруженных дефектов за заданное время тестирования и последующее устранение найденных программных дефектов. Формализованный процесс фаззинга, валидированный с помощью метрик времени тестирования и объема проверенного кода соответствует международным и отечественным стандартам качества и надежности для электронных устройств. Сравнительный анализ с классическими методами имитации неисправностей показал, что фаззинг совместно с интеллектуальными технологиями, обеспечивает проверку на наличие уязвимостей из баз знаний MITRE и OWASP, что позволяет сокращает временные и ресурсные затраты на устранение дефектов и время работы служб информационной безопасности.

Возможность сигнализации об полученных ошибках администратору системы обеспечивает обратную связь для разработчиков ПАК в процессе эксплуатации. Экспериментальные исследования подтвердили практическую значимость разработанного решения. Было достигнуто увеличение скорости обнаружения ошибок до двух раз и увеличение покрытия кода до 20%, что способствует снижению числа уязвимостей, включая «уязвимости нулевого дня».

Использование представленных интеллектуальных технологий совместно с другими видами анализа, таких как аппаратная диагностика и акустический анализ, будет рассмотрено подробнее в следующих работах и позволит выполнять выявление дефектов более эффективно за счет всестороннего анализа подсистем ПАК.

Список литературы

1. Meng Ruijie, Mirchev Martin, Böhme Marcel et al. Large Language Model guided Protocol Fuzzing. 2024. DOI: 10.14722/ndss.2024.24556

2. Elnaggar R., Delgado B., Fung J. M. RAG-Based Fuzzing of Cross-Architecture Compilers. URL: https://arxiv.org/abs/2504.08967 (дата обращения: 13.07.2025).

3. Панков И.А., Панков Д.А., Денисова Л.А. Автоматизация разработки и тестирования цифровых систем связи с многоуровневой архитектурой // Автоматизация в промышленности. 2023. № 1. С. 31–35.

4. Панков И.А., Панков А.П., Панков Д.А. и др. Перспективы использования FMEA-анализов для высокоответственных технических систем // Известия Тульского государственного университета. Технические науки. 2024. № 3. С. 26–31.

5. Панков И.А. Выявление дефектов при тестировании алгоритмов цифровых устройств на базе ПЛИС // Известия Тульского государственного университета. Технические науки. 2023. № 11. С. 277–280.

6. Панков И.А., Панков Д.А. Обнаружение системных дефектов цифровых устройств при имитации неисправностей с применением // Надежность. 2023. Т. 23. № 4. С. 51–58.

7. Chunqiu Steven Xia, Matteo Paltenghi, Jia Le Tian et al. Fuzz4All: Universal Fuzzing with Large Language Models. 2024. URL: https://arxiv.org/abs/2308.04748 (дата обращения: 29.09.2025).

8. Zafar A., Wajid B., Akram B. A hybrid fault diagnosis architecture for Wireless Sensor Networks // ICOSST. 2015. DOI: 10.1109/ICOSST.2015.7396395

9. Heracleous C., Keliris C., Panayiotou C. et al. Fault diagnosis for a class of nonlinear uncertain hybrid systems // Nonlinear Analysis: Hybrid Systems. 2022. Vol. 44. P. 101137. DOI: 10.1016/j.nahs.2021.101137

10. Pan Z., Fu Y., Guo H. et al. Analysis of Covert Attacks Using False Data against Network Control Systems: Three Case Studies // Syst Sci Complex. 2023. Vol. 36. Pp. 1407–1422.

11. Reber A., Cha S.K. Optimizing Fuzzing Seed Selection // Proceedings of the 23rd USENIX Security Symposium. San Diego, CA, 2014. Pp. 861–875.

12. Fibich C., Tauner S., Rössler P. et al. FIJI: Fault InJection Instrumenter // EURASIP Journal on Embedded Systems. 2019. DOI: 10.1186/s13639-019-0088-7

13. Trippel T., Shin K.G. Fuzzing Hardware as Software // USENIX: [сайт]. 2022. URL: https://www.usenix.org/system/files/sec22-trippel.pdf (дата обращения: 13.07.2025).

14. Панков Д.А., Денисова Л.А. Контроль и диагностика отказов программно-аппаратных комплексов // Омский научный вестник. 2018. № 2. С. 128–130.

15. Панков Д.А., Денисова Л.А. Проектирование аппаратно-программного комплекса: определение объема тестовых испытаний микропроцессорных устройств // Автоматизация в промышленности. 2020. № 12. С. 23–29.

References

1. Meng R., Mirchev M., Böhme M. et al. Large Language Model guided Protocol Fuzzing. Network and Distributed System Security (NDSS) Symposium 2024; San Diego (CA, USA). DOI: 10.14722/ndss.2024.24556

2. Elnaggar R., Delgado B., Fung J. M. RAG-Based Fuzzing of Cross-Architecture Compilers. (accessed 13.07.2025). Available at: https://arxiv.org/abs/2504.08967.

3. Pankov I.A., Pankov D.A., Denisova L.A. [Automation of development and testing of digital communication systems with multilevel architecture]. *Avtomatizatsiya v promyshlennosti* 2023;1:31-35. (in Russ.)

4. Pankov I.A., Pankov A.P., Pankov D.A. et al. Prospects for the use of FMEA analyzes for highly critical technical systems. *Izvestiya Tula State University* 2024;3:26-31. (in Russ.)

5. Pankov I.A. Detecting defects when testing algorithms digital devices based on FPGA. *Izvestiya Tula State University* 2023;11:277-280. (in Russ.)

6. Pankov D.A., Pankov I.A. Detecting system defects of digital devices in the course of malfunction imitation using fuzzing. *Dependability* 2023;23(4):51-58. (in Russ.)

7. Chunqiu Steven Xia, Matteo Paltenghi, Jia Le Tian et al. Fuzz4All: Universal Fuzzing with Large Language Models. 2024. (accessed 29.09.2025). Available at: https://arxiv.org/abs/2308.04748.

8. Zafar A., Wajid B., Akram B. A hybrid fault diagnosis architecture for Wireless Sensor Networks. ICOSST; 2015. DOI: 10.1109/ICOSST.2015.7396395

9. Heracleous C., Keliris C., Panayiotou C. et al. Fault diagnosis for a class of nonlinear uncertain hybrid systems. *Nonlinear Analysis: Hybrid Systems* 2022;44:101137. DOI: 10.1016/j.nahs.2021.101137

10. Pan Z., Fu Y., Guo H. et al. Analysis of Covert Attacks Using False Data against Network Control Systems: Three Case Studies. *Syst Sci Complex* 2023;36:1407-1422.

11. Reber A., Cha S.K. Optimizing Fuzzing Seed Selection. Proceedings of the 23rd USENIX Security Symposium. San Diego (CA, USA); 2014. Pp. 861-875.

12. Fibich C., Tauner S., Rössler P. et al. FIJI: Fault InJection Instrumenter. EURASIP Journal on Embedded Systems 2019. DOI: 10.1186/s13639-019-0088-7

13. Trippel T., Shin K.G. Fuzzing Hardware as Software. (accessed 13.07.2025). Available at: https://www.usenix.org/system/files/sec22-trippel.pdf

14. Pankov D.A., Denisova L.A. Control and diagnostics of faults in hardware-software complex. *Omsk Scientific Bulletin* 2018;2(158):128-133. (in Russ.) DOI:https://doi.org/10.25206/1813-8225-2018-158-128-133.

15. Pankov D.A., Denisova L.A. [Designing a software and Hardware system: defining the scope of testing of computer-based devices]. *Avtomatrizatsiya v promyshlennosti* 2020;12:23-29. (in Russ.)

Сведения об авторах

Панков Илья Анатольевич – аспирант ОмГТУ, pankov99ai@yandex.ru.

Аверченко Артем Павлович – аспирант ОмГТУ, руководитель СКБ «Цифровая обработка сигналов на ПЛИС» ОмГТУ.

Панков Денис Анатольевич – руководитель проектов и системный аналитик ООО «ЛАНИТ-ТЕРКОМ», участник программного комитета по стандартизации информационных технологий, канд. техн. наук. pankovDDD@yandex.ru.

About the authors

Ilia A. Pankov, postgraduate student, OmSTU, pankov99ai@yandex.ru.

Artem P. Averchenko, postgraduate student, OmSTU, head of the Digital Signal Processing using FPGA SDB, OmSTU.

Denis A. Pankov, Project Manager and System Analyst, LANIT-TERKOM LLC, Member of the Program Committee for Information Technology Standardisation, Candidate of Engineering, pankovDDD@yandex.ru.

Вклад авторов

Панков Илья Анатольевич провел экспериментальные исследования с применением фаззинга и нечеткой логики для выявления ошибок ПО и техногенных событий.

Аверченко Артем Павлович предложил идеи по имитации неисправностей для программно-аппаратных модулей на ПЛИС.

Панков Денис Анатольевич разработал архитектуру системы имитации неисправностей и предложил комбинацию техники фаззинга совместно с большими языковыми моделями для улучшения объема найденных ошибок ПО и уязвимостей.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

УДК 004.056:004.058 + 620.169.2
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-69-76

Об оценивании устойчивости функционирования объектов критической информационной инфраструктуры, подверженных воздействию угроз нарушения их информационной безопасности

On assessing the operational stability of critical information infrastructure facilities affected by information security threats

Воеводин В.А.[1]*, Третьяков С.М.[2]
Voevodin V.A.[1]*, Tretyakov S.M.[2]

[1] Национальный исследовательский университет «Московский институт электронной техники», Зеленоград, Российская Федерация
[2] Военная академия связи, Санкт-Петербург, Российская Федерация
[1] National Research University of Electronic Technology, Zelenograd, Russian Federation
[2] Military Academy of the Signal Corps, Saint Petersburg, Russian Federation
** vva541@mai.ru*

Воеводин В.А.

Третьяков С.М.

Резюме. Цель. *Формализовать научную задачу количественного оценивания устойчивости функционирования объектов критической информационной инфраструктуры, подверженных воздействию угроз нарушения их информационной безопасности.* **Методы**. *Познавательные методы: системного анализа, индуктивно-дедуктивный, анализ научной задачи, формализации научных знаний, построения гипотез. Операционные методы: абстрагирование, конкретизация, сравнение, обобщение, аналогия, моделирования, методы экспертного оценивания.* **Результаты.** *Обоснована актуальность, сформулирована вербальная и формальная постановки научной задачи количественного оценивания устойчивости функционирования объектов критической информационной инфраструктуры, предложены показатели для оценивания исходных данных и получаемого результата.* **Заключение**. *Осуществлен системный анализ проблемной ситуации, что позволило выявить объективные основания актуальности решения научной задачи, осуществить ее формальную постановку, обосновать выбор управляемых и неуправляемых факторов для оценивания устойчивости, сформулировать ограничения, предложить способ учета динамики критической информационной инфраструктуры в результате воздействия угроз нарушения ее информационной безопасности.*

Abstract. Aim. *To formalise the scientific problem of quantifying the operational stability of critical information infrastructure facilities exposed to information security threats.* **Methods**. *Cognitive methods: systems analysis, induction and deduction, analysis of a scientific problem, formalisation of scientific knowledge, construction of hypotheses. Operational methods: abstraction, specification, comparison, generalisation, analogy, simulation, expert evaluation.* **Results.** *The paper substantiates the relevance, defines – both verbally and formally – the scientific problem of quantifying the operational stability of critical information infrastructure facilities, suggests indicators for assessing the input data and the result.* **Conclusions**. *The authors systematically analysed the problem, which allowed substantiating the relevance of a potential solution, formalising it, substantiating the choice of the controllable and uncontrollable factors for assessing stability, defining the restrictions, suggesting the method for taking into account the dynamics of critical information infrastructure exposed to information security threats.*

Ключевые слова: *критическая информационная инфраструктура, угрозы нарушения информационной безопасности, устойчивость функционирования, система восстановления функциональности.*
Keywords: *critical information infrastructure, information security threats, operational stability, functionality restoration system.*

Для цитирования: *Воеводин В.А., Третьяков С.М. Об оценивании устойчивости функционирования объектов критической информационной инфраструктуры, подверженных воздействию угроз нарушения их информационной безопасности // Надежность. 2025. №4. С. 69-76. https://doi.org/10.21683/1729-2646-2025-25-4-69-76*

For citation: *Voevodin V.A., Tretyakov S.M. On assessing the operational stability of critical information infrastructure facilities affected by information security threats. Dependability 2025;4: 69-76. https://doi.org/10.21683/1729-2646-2025-25-4-69-76*

Поступила: *13.09.2024* / **После доработки:** *16.03.2025* / **К печати:** *28.09.2025*
Received on: *13.09.2024* / **Revised on:** *16.03.2025* / **For printing:** *28.09.2025*

Введение

Информационная инфраструктура создается для удовлетворения потребностей субъектов информационных отношений (обладателей информации и операторов информационных систем) и служит активным средством в их целенаправленной деятельности. Противник с целью нарушить функциональность объектов критической информационной инфраструктуры (КИИ) наносит поражающие воздействия по их элементам.

В результате поражения отдельных элементов может быть нарушена их функциональность или они могут быть уничтожены, что может привести к нарушению функциональности КИИ в целом.

Для обеспечения устойчивости функционирования КИИ выделяется соответствующий ресурс, который необходимо эффективно распределить по задачам и времени. Под ресурсом понимаются выделяемые для обеспечения устойчивости объектов КИИ силы, средства и материальный ресурс. Если силы и средства могут применяться неоднократно, такой ресурс позиционируется как возобновляемый. Материальный ресурс расходуется безвозвратно и позиционируется как невозобновляемый ресурс. Для принятия решения по обеспечению устойчивости КИИ, органам управления требуется инструмент для количественного оценивания устойчивости функционирования КИИ, чтобы сравнить альтернативные варианты управленческих решений и обосновать выбор рационального.

Для успешного решения задач по обеспечению безопасности КИИ современные методические потребности органов управления в оценивании устойчивости КИИ и возможности существующего научно-методического аппарата должны находится в *гармонии*.

В результате исследований сформулированы вербальная и формальная постановки научной задачи количественного оценивания устойчивости КИИ, предложены подходы к формированию исходных данных и интерпретации получаемого результата. Новизна результатов заключается в том, что был осуществлен системный анализ проблемной ситуации, результаты которого позволили: а) выявить актуальность задачи обеспечения устойчивости КИИ, находящейся в условиях воздействия угроз; б) выявить ограниченность существующих методов поддержки принимаемых решений; в) осуществить формальную постановку задачи.

При постановке задачи обоснован выбор управляемых и неуправляемых параметров, сформулированы ограничения, предложен способ учета динамики КИИ в результате изменения обстановки.

Анализ существующих нормативных правовых актов, методических документов, приказов исполнительных органов власти (Регуляторов) и национальных стандартов позволяет утверждать, что они в совокупности и по отдельности не содержат общепринятых методических рекомендаций по количественному оцениванию устойчивости КИИ применительно к условиям воздействия угроз.

Существующий инструментарий оценивания устойчивости КИИ ориентирован на *штатные условия, зафиксированные в эксплуатационной документации,* и базируется на положениях теории надежности. Методы теории надежности, основанные на анализе экспериментальных данных, постоянно развиваются. Результаты фундаментальных исследований теории надежности технических систем отражены достаточно полно и глубоко в публикациях Б.В. Гнеденко [1], И.А. Ушакова [2], А.М. Половко и С.В. Гурова [3], В.А. Каштанова [4], И.Б. Шубинского [5, 6] и других признанных ученых.

Однако для условий воздействия угроз применение методов теории надежности для оценивания устойчивости КИИ не всегда оправдано. Такое ограничение связано с редкостью событий воздействия угроз, ограниченностью интервала времени их наблюдения, изменчивостью обстановки, поведенческой неопределенностью. Ограниченность методов теории надежности при исследовании живучести, безопасности, защищенности сложных систем и надежности программного обеспечения отмечалась И.А. Ушаковым в докладе «Надежность: прошлое, настоящее, будущее» [7].

Результаты исследования особенностей количественного оценивания эффективности информационных систем и технологий применительно к *штатным* условиям функционирования как сервисных систем приводятся Р.М. Юсуповым и А.А. Мусаевым [8]. Авторы предлагают в основу оценивания положить вероятностный подход, что для условий воздействия угроз не всегда приемлемо.

Отсутствие методического аппарата для количественного оценивания устойчивости КИИ при воздействии угроз сдерживает развитие отношений, которые возникают при обеспечении безопасности КИИ.

1. Анализ возможностей существующего методического аппарата

Особенностями существующего подхода к управлению информационной безопасностью (ИБ) является то, что для его осуществления характерны и являются преобладающими императивные нормы права. Деятельность, которая регулируется преимущественно

силой закона и подзаконных актов, позиционируется как административная и относится к репродуктивной. К существующей инерционности директивного подхода необходимо объективно добавить и то, что требования Регулятора известны противнику (источнику угроз), который может использовать эти знания и целенаправленно планировать эффективное воздействие угрозами в обход требуемых мер защиты.

Вместе с тем, опять же силой закона, обладателям информации и операторам информационных систем предписано: а) обеспечить защиту информации; б) не допускать воздействий на технические средства обработки информации, в результате которого нарушается их функционирование; в) осуществлять постоянный контроль за обеспечением уровня защищенности информации. При исполнении этих предписаний действуют диспозитивные нормы права, в соответствии с которыми обладателям информации и операторам информационных систем предоставляется право самостоятельно регулировать эти отношения. Для самостоятельного регулирования таких отношений требуется инструмент, позволяющий решить задачу количественного оценивания устойчивости функционирования соответствующих объектов информатизации.

В настоящее время известен ряд подходов к решению задачи оценивания и повышения устойчивости функционирования объектов информатизации, функционирующих в условиях воздействия дестабилизирующих факторов различной физической природы. Некоторые из таких подходов, представляющих интерес для оценивания устойчивости КИИ, приведены в трудах Д.П. Зегжды [9], И.В. Котенко, И.Б. Саенко, М.А. Кациняка, О.С. Лауты [10], А.А. Шелупанова и Р.В. Мещерякова [11, 12], С.А. Коноваленко [13], С.И. Макаренко [14, 15], Ю.И. Стародубцева, П.В. Закалкина [16], Ю.К. Язова [17], Г.Е. Черкесова, А.О. Недосекина и В.В. Виноградова [18, 19], И.А. Рябинина [20].

Основные усилия были направлены на развитие подходов к оцениванию устойчивости структурно-сложных технических систем на основе парадигмы структурной и функциональной устойчивости, когда критерий отказа системы и/или элемента является бинарным.

Вопросы обеспечения устойчивости функционирования сложных систем рассматривались и в смежных областях. Так, критерии, методы анализа и синтеза технических и информационных систем, методы обеспечения и повышения надежности, эксплуатации исследовались А.М. Половко совместно с С.В. Гуровым и приведены в [3]. В качестве предмета исследования были рассмотрены невосстанавливаемые и восстанавливаемые, нерезервированные и резервированные системы длительного и кратковременного времени существования.

Обобщая результаты ретроспективного анализа, можно утверждать, что для условий воздействия целенаправленных угроз существуют лишь отельные публикации, которые не объединены в единый методический аппарат, что в совокупности переводит поставленную задачу в статус научной проблемы. Также следует отметить, что отсутствует общепринятое официальное определение понятия «устойчивость функционирования КИИ» и место в понятийном поле термина «живучесть КИИ», поэтому приводится авторское видение этой терминологии, которое опубликовано в [21].

2. Вербальная постановка задачи

При оценивании устойчивости КИИ можно выделить отдельные группы факторов: а) устойчивость элементов (узлов и ребер), входящих в состав схемы устойчивости объекта КИИ; б) условия функционирования КИИ (сценарии воздействия угроз); в) способы применения сил и средств восстановления функциональности элементов КИИ.

Для формальной постановки задачи факторы, определяющие условия функционирования КИИ, подразделяются на две группы: а) факторы, которые могут *контролироваться* лицом, принимающим решение (ЛПР); б) факторы, которые не могут быть контролируемы ЛПР по различным причинам.

Каждый элемент оцениваемого объекта на периоде воздействия угроз может принимать три различных состояния: а) функционален – способен выполнять требуемые функции; б) поврежден – восстановление функциональности возможно через определенный промежуток времени восстановления, не превышающий момента окончания воздействия угроз; в) поражен – восстановление функциональности не целесообразно или невозможно из-за ограниченности ресурса, в том числе и временного. Последовательный переход из одного состояния в другое позиционируется как процесс функционирования элемента и объекта КИИ в целом.

3. Формальная постановка задачи

1) Управляемые факторы

Пусть задана структура информационной-телекоммуникационной сети[1] (объект критической инфраструктуры) в момент времени t_0, соответствующий началу периода воздействия угроз $(0, T]$

$$S(t_0) = \{A(t_0), L(t_0)\},$$

где $A(t_0) = \{a_i(t_0)\}$ – семейство *узлов связи* (узлов), $a_i(t_0)$ – индикатор состояния i-го узла (если узел $a_i(t_0)$ функционален, то $a_i(t_0) = 1$ или 0 в противном случае), $i = 1, 2, \ldots, N_A$; N_A – мощность семейства $A(t_0)$; $L(t_0) = \{l_{i,j}(t_0)\}$ – семейство *линий связи* (ребер), $l_{i,j}(t_0)$ – индикатор состояния i,j-й линии связи (если линия связи $l_{i,j}(t_0)$ функциональна, то $l_{i,j}(t_0) = 1$ или 0 в противном случае), $i,j = 1, 2, \ldots, N_L$; $N_L = (N_A)^2$ – мощность семейства $L(t_0)$.

[1] Концепция структурной схемы устойчивости в данном случае применяется по аналогии с ГОСТ Р МЭК 61078-2021 Надежность в технике. Структурная схема надежности.

Определено исходное семейство *элементов* объекта КИИ в момент времени t_0

$$E(t_0)=\{e_k(t_0)\}=A(t_0)\cup L(t_0)=\{\{a_i(t_0)\}\cup\{l_{i,j}(t_0)\}\},$$

где $k=1, 2, \ldots, N_E$; N_E – мощность исходного семейства элементов $E(t_0)$, $e_k(t_0)\in E(t_0)$.

Процесс функционирования подверженного воздействию угроз объекта КИИ характеризуется сменой состояний его элементов $e_k(t)\in E(t_0)$; если k-й элемент на момент времени t сохранил функциональность, то $e_k(t)=1$, если k-й элемент был поврежден, то $e_k(t)=\tau_k(t)$ где $\tau_k(t)$ – время до окончания восстановления функциональности k-го элемента на момент времени t; если k-й элемент был поражен в результате воздействия угрозы, то его идентификатору безвозвратно присваивается значение $e_k(t)=0$.

Пусть известны количественные оценки факторов, которые оказывают непосредственное влияние на устойчивость объекта КИИ:

- семейство актуальных угроз

$$U=\{u_m\},$$

где u_m – идентификатор актуальной угрозы с индексом m, $m=1, 2, \ldots, N_U$, N_U – мощность семейства актуальных угроз;

- семейство стационарных коэффициентов оперативной готовности элементов объекта КИИ

$$K_{\text{Or}}(t_0, t_0+t)\underset{\substack{t\in(0,T],\\ k=1,2,\ldots,N_E}}{=}\{\hat{k}_{\text{Or}k}(t_0, t_0+t)\},$$

где $\hat{k}_{\text{Or}k}$ – стационарный коэффициент оперативной готовности k-го элемента на интервале $t\in(0, T]$. Физически $\hat{k}_{\text{Or}k}$ отражает вероятность того, что элемент a_k проработает безотказно в течение заданного периода времени T, начиная с момента времени t_0.

Защищенность элементов объекта КИИ от воздействия угроз U

$$P(u)\underset{\substack{k=1,2,\ldots N_E,\\ m=1,2,\ldots N_U}}{=}\{p_{k,m^*}, \underset{\sim}{p}_{k,m^*}, \widehat{p}_{k,m^*}\},$$

где $p_{k,m}$ – оценка вероятности сохранения функциональности элементом с индексом $e_k(t_0)\in E(t_0)$ при воздействии угрозы с индексом $u_m\in U$. Если угроза u_m для элемента $e_k(t_0)$ является не актуальной, то $p_{k,m}=1$. Из всех актуальных угроз U для оценивания защищенности элемента с индексом e_k выбирается угроза с индексом u_{m^*}, при которой

$$p_{k,m^*}=\min_{\substack{k=1,2,\ldots N_E,\\ m=1,2,\ldots N_U}} p_{k,m},$$

где $\underset{\sim}{p}_{k,m^*}$ – вероятность *повреждения* k-го элемента при воздействии угрозы u_{m^*}; $\widehat{p}_{k,m^*}$ – вероятность *поражения* k-го элемента при воздействии угрозы u_{m^*}, при этом

$$\widehat{p}_{k,m^*}=1-\left(p_{k,m^*}+\underset{\sim}{p}_{k,m^*}\right).$$

Учитывая, что элемент может находится только в одном из трех состояний следует, что

$$p_{k,m^*}+\widehat{p}_{k,m^*}+\underset{\sim}{p}_{k,m^*}=1.$$

Оценка *требуемых* производительных *возможностей* для восстановления функциональности объекта КИИ после воздействия угроз $u\in U$

$$\mathrm{T}(u)\underset{\substack{k=1,2,\ldots,N_E,\\ m=1,\ldots,N_U}}{=}\{\tau_{k,m}\}\underset{\substack{k=1,2,\ldots,N_E,\\ m=1,\ldots,N_U}}{=}\{\underset{\sim}{\tau}_{k,m}, \widehat{\tau}_{k,m}\},$$

где $\underset{\sim}{\tau}_{k,m}$ – нижняя оценка *требуемого времени* восстановления функциональности элемента e_k, из всех актуальных угроз U выбирается угроза с индексом u_{m^*} при которой

$$\underset{\sim}{\tau}_k=\underset{\sim}{\tau}_{k,m^*}=\max_{m=1,2,\ldots,N_U}\underset{\sim}{\tau}_{k,m},$$

где $\widehat{\tau}_{k,m}$ – верхняя оценка *требуемого* времени восстановления функциональности элемента e_k, из всех актуальных угроз U выбирается угроза с индексом u_{m^*} при которой

$$\widehat{\tau}_k=\widehat{\tau}_{k,m^*}=\max_{m=1,2,\ldots,N_U}\widehat{\tau}_{k,m}.$$

Ресурсные возможности системы восстановления функциональности субъекта КИИ, выделенные для восстановления функциональности объекта КИИ в условиях воздействия угроз

$$\Theta\underset{\substack{i=1,2,\ldots,N_D,\\ j=1,2,\ldots,N_R}}{=}\{d_i, r_j\},$$

где d_i – число единиц d_i-го *возобновляемого* ресурса, d_i – классификатор i-го *возобновляемого* ресурса, $i=1, 2, \ldots, N_D$, N_D – количество классификаторов возобновляемого ресурса; r_j – число единиц r_j-го *невозобновляемого* ресурса, r_j – классификатор j-го *невозобновляемого* ресурса, $j=1, 2, \ldots, N_R$, N_R – количество классификаторов (артикулов) невозобновляемого ресурса.

2) Неуправляемые факторы

Параметры воздействия угроз по семейству элементов объекта КИИ

$$\mathrm{H}(u)=\{\underset{\sim}{\eta}_{m,k,n}, \widehat{\eta}_{m,k,n}\},$$

где $\underset{\sim}{\eta}_{m,k,n}$ – нижняя граница времени до n-го воздействия угрозы $u_m\in U$ по элементу a_k. Из всех актуальных угроз U для каждого воздействия n выбирается угроза с индексом $u_{m^*}\in U$, для которой

$$\underset{\sim}{\eta}_{m^*,k,n}=\min_{\substack{m=1,2,\ldots,N_U,\\ n=1,\ldots,N}}\underset{\sim}{\eta}_{m,k,n},$$

где $m=1, \ldots, N_U$, N_U – число актуальных угроз; $k=1, \ldots, N_E$; $k=1, 2, \ldots, N_E$, N_E – число элементов СОФ; $n=1, \ldots, N_U$, N – прогнозируемое число воздействий угроз; $\widehat{\eta}_{m,k,n}$ – верхняя граница времени до k-го воздействия

угрозы $u_m \in U$ по элементу a_k при воздействии угрозы n. Из всех актуальных угроз U для каждого воздействия n выбирается угроза с индексом $u_{m^*} \in U$, для которой

$$\hat{\eta}_{m^*,k,n} = \max_{\substack{m=1,2,\ldots,N_U,\\ n=1,\ldots,N}} \hat{\eta}_{m,k,n},$$

где m=1, …, N_U, N_U – число актуальных угроз; k=1, …, N_E; k=1, 2, …, N_E, N_E – число элементов СОФ; n=1, …, N_U, N – прогнозируемое число воздействий угроз.

Оценка требуемых ресурсов для восстановления функциональности объекта КИИ, подверженного воздействию угроз (формируется в результате технической разведки)

$$\hat{\Theta} = \left\{\hat{d}_{k,m,i}, \hat{r}_{k,m,j}\right\},$$

где $\hat{d}_{k,m,i}$ – требуемый *возобновляемый* ресурс i-го типа для восстановления функциональности поврежденного элемента e_k при воздействии угрозы $u_m \in U$, i=1, 2, …, N_D, N_D – число типов (классификаторов) *возобновляемого* ресурса. Из всех комбинаций индексов элементов k и угроз m $\langle k, m\rangle$ выбирается комбинация $\langle k^*, m^*\rangle$ при которой *возобновляемый* ресурс с индексом i имел бы максимальное число единиц учета

$$\hat{d}_i\langle k^*, m^*\rangle = \max_{\substack{k=1,2,\ldots,N_E,\\ m=1,2,\ldots,N_U}} \hat{d}_i\langle k, m\rangle,$$

$\hat{r}_{k,m,j}$ – требуемый *невозобновляемый* ресурс j-го типа для восстановления функциональности поврежденного элемента e_k при воздействии угрозы $u_m \in U$, j=1, 2, …, N_R, N_R – число типов (классификаторов) *невозобновляемого* ресурса. Из всех комбинаций индексов элементов k и угроз m $\langle k, m\rangle$ выбирается комбинация $\langle k^*, m^*\rangle$ при которой *невозобновляемый* ресурс с индексом j имел бы максимальное число единиц учета

$$\hat{r}_j\langle k^*, m^*\rangle = \max_{\substack{k=1,2,\ldots,N_E,\\ m=1,2,\ldots,N_U}} \hat{r}_j\langle k, m\rangle.$$

3) Ограничения

Соответствие конфиденциальности информации требованиям на всем периоде воздействия угроз $t \in (0, T]$

$$\mathrm{К}(t) \underset{t\in(0,T]}{\in} \mathrm{К}_{\mathrm{Тр}},$$

где К(t) – совокупность требований по обеспечению конфиденциальности реализованных в момент времени $t \in (0, T]$;

$\mathrm{К}_{\mathrm{Тр}}$ – совокупность требований по обеспечению конфиденциальности.

Соответствие целостности информации требованиям на всем периоде воздействия угроз $t \in (0, T]$

$$\mathrm{Ц}(t) \in \mathrm{Ц}_{\mathrm{Тр}},$$

где Ц(t) – совокупность требований по обеспечению целостности информации реализованных в мент времени $t \in (0, T]$;

$\mathrm{Ц}_{\mathrm{Тр}}$ – совокупность требований по обеспечению целостности.

Требуется, с учетом принятых ограничений, разработать:

Семейство методов теоретической обработки исходных данных (оператор) – $\mathcal{M}$, позволяющих получать количественные оценки показателей, характеризующих устойчивость функционирования элементов объекта КИИ, находящегося под воздействием угроз $u \in U$

$$\left\{\varphi_k(u,t)\right\} \underset{\substack{t\in(0,T]\\ u\in U\\ \mathrm{К}(t)\in\mathrm{К}_{\mathrm{Тр}}\\ \mathrm{Ц}(t)\in\mathrm{Ц}_{\mathrm{Тр}}}}{=} \mathcal{M}\left\{\begin{matrix} E(t_0), U, K_{\mathrm{Ог}}, P(u),\\ \mathrm{T}(u,t), \Theta(t), \mathrm{H}(u), \hat{\Theta}\end{matrix}\right\},$$

где $\{\varphi_k(u,t)\}$ – семейство функций устойчивости, характеризующих устойчивость функционирования элементов объекта КИИ, находящегося под воздействием угроз $u \in U$, $\varphi_k(u,t)$ – частная функция устойчивости k-го элемента.

2. Семейство методов теоретической обработки исходных данных (оператор) – $\mathcal{B}$, характеризующих семейство функций устойчивости отдельных элементов объекта КИИ $\varphi_k(u,t)$ и его структуру $S(t)$, позволяющих получать количественную оценку, характеризующую устойчивость функционирования объекта КИИ в целом, находящегося под воздействием угроз $u \in U$

$$\Phi(t) = \mathcal{B}\left\{\varphi_k(u,t), S(t), \hat{\Theta}\right\} =$$

$$= \mathcal{B}\left\{\mathcal{M}\left\{\begin{matrix} E(t_0), U, K_{\mathrm{Ог}}, P(u),\\ \mathrm{T}(u,t), \Theta(t), \mathrm{H}(u,t)\end{matrix}\right\}, S(t), \hat{\Theta}\right\},$$

где $\Phi(t)$ – функция устойчивости объекта КИИ, находящегося под воздействием угроз, $\mathcal{B}$ – оператор, позволяющий отобразить семейство частных функций устойчивости элементов объекта КИИ в функцию устойчивости объекта КИИ в целом.

Новизна полученных результатов заключается: а) в усовершенствовании онтологии предметной области, позволяющей стоить адекватные вербальные модели предмета исследования; б) в оригинальной постановке научной задачи, позволяющей оценить устойчивость объекта КИИ для условий воздействия угроз, когда методы математической статистики и теории вероятностей, которые нашли широкое применение для штатных условий, не могут быть применимы без грубых допущений; в) в использовании для представления исходных данных и результатов оценивания не усредненных вероятностных характеристик, как это принято для штатных условий, а функций, отражающих зависимость параметров исходных данных и получаемого результата от времени, что позволяет снять ограничение на стационарность и эргодичность исследуемого случайного процесса; г) применение для оценивания устойчивости отдельных элементов методов теории управляемых полумарковских процессов с *тремя* возможными состояниями, что позволяет связать частные характеристики

защищенности и восстанавливаемости элементов, подверженных угрозам, с частными оценками устойчивости их функционирования; д) в приложении методов управляемых полумарковских процессов для оценивания устойчивости объекта КИИ в целом на основе частных оценок функций устойчивости элементов; е) в приложении разработанной методологии для количественного оценивания эффективности планов восстановления функциональности объекта КИИ, элементы которого получили повреждения в результате воздействия угроз; ж) в приложении разработанных методов оценивания устойчивости для обоснования распределения затрат между мероприятиями по обеспечению защищенности и восстанавливаемости элементов.

Заключение

Таким образом, предлагаемая постановка научной задачи позволяет обобщить методы теории надежности, теории случайных функций, теории информационной безопасности на случаи, когда при оценивании устойчивости КИИ не представляется возможным принять допущения: а) о массовости случайных явлений; б) о неограниченности времени наблюдения за оцениваемым объектом; в) о стационарности сопутствующей обстановки; г) об отсутствии поведенческой неопределенности. Разработаны соответствующие методы и математические модели, которые приведены в [22-24].

При поддержке Фонда Потанина

Список литературы

1. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. М.: Наука, 1965. 524 с.

2. Ушаков И.А. Обобщенные показатели при исследовании сложных систем / И.А. Ушаков, Е.И. Литвак. М.: Знание, 1985. 128 с.

3. Половко А.М., Гуров С.В. Основы теории надежности. СПб.: БХВ-Петербург, 2006. 704 с.

4. Каштанов В.А., Медведев А.И. Теория надежности сложных систем: 2-е изд., перераб. М.: ФИЗМАТЛИТ, 2010. 608 с.

5. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.

6. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 296 с.

7. Ушаков И.А. Надежность: прошлое, настоящее, будущее: пленарный доклад на открытии конференции «Математические методы в надежности» (MMR–2000), Бордо, Франция, 2000 // Надежность: Вопросы теории и практики: сетевой журн. 2016. № 1(1). С. 17-27.

8. Юсупов Р.М. Особенности оценивания эффективности информационных систем и технологий / Р.М. Юсупов, А.А. Мусаев // Труды СПИИРАН. 2017. Вып. № 2 (51). С. 5–34.

9. Зегжда Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / под ред. Д.П. Зегжды. М.: Горячая линия – Телеком, 2022. 560 с.

10. Котенко И.В. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей / И.В. Котенко, И.Б. Саенко, М.А. Коцыняк, О.С. Лаута // Труды СПИИРАН. 2017. № 6(55). С. 160-184. DOI: 10.15622/sp.55.7

11. Шелупанов А.А. Безопасность комплексных гетерогенных систем и сетей. Теория и практика: монография // С.Ю. Исхаков, А.А. Шелупанов, Р.В. Мещеряков. Томск: Изд-во Томского государственного университета систем управления и радиоэлектроники, 2015. 119 с.

12. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем: монография / Р.В. Мещеряков, А.А. Шелупанов. Томск: Издательство В–спектр, 2007. 278 с.

13. Коноваленко С.А. Методика оценивания функциональной устойчивости гетерогенной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Системы управления, связи и безопасности. 2023. № 4. С. 157-195. DOI: 10.24412/2410-9916-2023-4-157-195

14. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки : [монография]. СПб.: Наукоемкие технологии, 2020. 337 с.

15. Макаренко С.И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть III: Управление системой связи в условиях конфликта // Техника радиосвязи. 2021. № 1(48). С. 103-116. DOI: 10.33286/2075-8693-2021-48-103-116

16. Стародубцев Ю.И., Закалкин П.В. Структурно-функциональный анализ конфликтной ситуации между государственной системой обеспечения информационной безопасности и иностранной системой деструктивных воздействий // Вопросы кибербезопасности. 2024. № 4(62). С. 82-91. DOI: 10.21681/2311-3456-2024-4-82-91

17. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах : [монография] / Ю.К. Язов; Федеральное гос. науч. учреждение «Северо-Кавказский науч. центр высш. шк.». Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. 270 с.

18. Черкесов Г.Н., Недосекин А.О., Виноградов В.В. Анализ функциональной живучести структурно-сложных технических систем // Надежность. 2018. Том 18. № 2. С. 17-24. DOI: 10.21683/1729-2646-2018-18-2-17-24

19. Черкесов Г.Н. Описание подхода к оценке живучести сложных структур при многоразовых воздействиях высокой точности / Г.Н. Черкесов, А.О. Недосекин // Надежность. 2016. Том 16. № 2(57). С. 3–15.

20. Рябинин И.А. Надежность и безопасность структурно-сложных систем. Спб.: Политехника, 2000. 248 с.

21. Воеводин В.А. Генезис понятия структурной устойчивости информационной инфраструктуры автоматизированной системы управления производственными процессами к воздействию целенаправленных угроз информационной безопасности // Вестник Воронежского института ФСИН России. 2023. № 2, апрель–июнь. С. 30-41.

22. Воеводин В.А. Модель оценки функциональной устойчивости информационной инфраструктуры для условий воздействия множества компьютерных атак // Информатика и автоматизация. 2023. № 22(3). С. 691-715. DOI: 10.15622/ia.22.3.8

23. Воеводин В.А. Частная полумарковская модель как инструмент снижения сложности задачи оценивания устойчивости функционирования элементов информационной инфраструктуры, подверженной воздействию угроз // Информатика и автоматизация. 2024. № 23(3). С. 611-642. DOI: 10.15622/ia.23.3.1

24. Воеводин В.А., Крахотин Н.А. Методы оценивания связности неориентированного двухполюсного помеченного графа с учетом деструктивного воздействия внешних угроз на его вершины // Вестник Дагестанского государственного технического университета. Технические науки. 2024. № 51(1). С. 46-60. DOI:10.21822/2073-6185-2024-51-1-46-60

References

1. Gnedenko B.V., Beliaev Yu.K., Soloviev A.D. [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965. (in Russ.)

2. Ushakov I.A., Litvak E.I. [Generalised indicators in the study of complex systems]. Moscow: Znanie; 1985. (in Russ.)

3. Polovko A.M., Gurov S.V. [Fundamentals of the dependability theory]. St. Petersburg: BHV-Peterburgl; 2006. (in Russ.)

4. Kashtanov V.A., Medvedev A.I. [Dependability theory of complex systems: 2nd edition, revised]. Moscow: Fizmatlit; 2010. (in Russ.)

5. Shubinsky I.B. [Structural dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012. (in Russ.)

6. Shubinsky I.B. [Functional dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012. (in Russ.)

7. Ushakov I.A. [Dependability: past, present, future: keynote speech of the opening of Mathematical Methods in Reliability (MMR-2000) conference, Bordeau, France, 2000]. *Reliability: Theory & Applications* 2016;1(1):17-27. (in Russ.)

8. Yusupov R.M., Musaev A.A. Efficiency of Information Systems and Technologies: Features of Estimation. *SPIIRAS Proceedings* 2017;2(51):5-34. (in Russ.)

9. Zegzhda D.P. [Cybersecurity of the digital industry. Theory and practice of functional resistance to cyber attacks]. Moscow: Goriachya liniya – Telekom; 2022. (in Russ.)

10. Kotenko I., Saenko I., Kotsynyak M., Lauta O. Assessment of Cyber-Resilience of Computer Networks based on Simulation of Cyber Attacks by the Stochastic Networks Conversion Method. *SPIIRAS Proceedings* 2017;6(55):160-184. DOI: 10.15622/sp.55.7

11. Shelupanov A.A., Iskhakov S.Yu., Shelupanov A.A., Meshcheryakov R.V. [Security of complex heterogeneous systems and networks. Theory and practice: a monograph]. Tomsk: Tomsk State University of Control Systems and Radioelectronics Publishing; 2015. (in Russ.)

12. Meshcheryakov R.V., Shelupanov A.A. [Comprehensive information security of automated systems: a monograph]. Tomsk: V–spektr Publishing; 2007. (in Russ.)

13. Konovalenko S. A. Methodology for assessing the functional stability of a heterogeneous system for detecting, preventing and eliminating the consequences of computer attacks. *Systems of Control, Communication and Security* 2023;4:157-195. (in Russ.). DOI: 10.24412/2410-9916-2023-4-157-195

14. Makarenko S.I. [Models of a communication system exposed to deliberate destabilising effects and intelligence: a monograph]. St. Petersburg: Naukoemkie tekhnologii; 2020. (in Russ.)

15. Makarenko S. I. Information conflict between a communication system and a system of destabilizing influences. Part III: Controlling of a communication system in conflict situation. *Radio communication technology* 2021;1(48):103-16. DOI: 10.33286/2075-8693-2021-48-103-116

16. Starodubtsev Yu.I., Zakalkin P.V. Sructural and functional analysis of the conflict situation between the state information security system and a foreign system of destructive influences. *Cybersecurity issues* 2024;4(62):82-91. DOI: 10.21681/2311-3456-2024-4-82-91

17. Yazov Yu.K. [Fundamentals of the methodology for quantifying the effectiveness of information protection in computer systems: a monograph]. Federal State Scientific Institution North Caucasus Scientific Centre of Higher Education. Rostov-on-Don: NCSCHE Publishing; 2006. (in Russ.)

18. Cherkesov G.N., Nedosekin A.O., Vinogradov V.V. Functional survivability analysis of structurally complex technical systems. *Dependability* 2018;18(2):17-24. DOI: 10.21683/1729-2646-2018-18-2-17-24

19. Cherkesov G.N., Nedosekin AO. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy. *Dependability* 2016;16(2):3-15. DOI:10.21683/1729-2646-2016-16-2-3-15

20. Ryabinin I.A. Reliability and safety of structurally complex systems. St. Petersburg: Polytekhnica; 2000. (in Russ.)

21. Voevodin V.A. [The genesis of the concept of structural resilience of the information infrastructure of an automated production process management system to the effects of targeted information security threats]. *Vestnik*

of Voronezh Institute of the Russian Federal Penitentiary Service 2023;2:30-41. (in Russ.)

22. Voevodin V. A Model for Assessing the Functional Stability of Information Infrastructure Elements for Conditions of Exposure to Multiple Computer Attacks. *Informatics and Automation* 2023;22(3):691-715. DOI: 10.15622/ia.22.3.8

23. Voevodin, V. A. On the formulation of the task of assessing the stability of the functioning of critical information infrastructure facilities. *Cybersecurity issues* 2025;1(65): 41-49. DOI: 10.21681/2311-3456-2025-1-41-49.

24. Voevodin V.A., Krahotin N.A. Methods for assessing the connectivity of an undirected bipolar labeled graph taking into account the destructive impact of external threats on its vertices. *Herald of Dagestan State Technical University. Technical Sciences* 2024;51(1):46-60. (in Russ.) DOI:10.21822/2073-6185-2024-51-1-46-60

Сведения об авторах

Воеводин Владислав Александрович – 124575, Зеленоград, корп. 901, кв. 160, Россия, НИУ «Московский институт электронной техники», доцент кафедры «Информационная безопасность», кандидат технических наук, доцент, почетный радист России; vva541@mail.ru; Известия вузов Электроника: 2024, Т.29. №3, 2024, Т.29. №2; Информатика и автоматизация 2023, Т. 22, № 3, 2024 Т 23 №3; Вестник Дагестанского государственного технического университета. Технические науки: 2024 Т 51 №1, 2023 Т50 №23, 2023 Т50 №1, 2022 Т49 №3; Вестник Воронежского института ФСИН России, 2023, № 2; Информационные технологии: 2024 Т30 №1; International Journal of Open Information Technologies: 2023. Т. 11, № 9; Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика: 2022. № 2; Системы управления, связи и безопасности. 2021. № 2.

Третьяков Сергей Михайлович – 194064, г. Санкт-Петербург, К-64, Тихорецкий проспект, д.3, Военная академия связи, доцент кафедры технического обеспечения связи и автоматизации, кандидат технических наук, доцент; smt2k@mail.ru.

About the authors

Vladislav A. Voevodin, 901, app. 160, Zelenograd, 124575, Russia, National Research University of Electronic Technology, Senior Lecturer, Department of Information Security, Candidate of Engineering, Associate Professor, Honorary Radio Operator of Russia; vva541@mail.ru; Proceedings of Universities Electronics: 2024;29(3), 2024;29(2); Computer Science and Automation 2023;22(3), 2024;23(3); Herald of Daghestan State Technical University. Technical Sciences 2024;51(1), 2023;50(23), 2023;50(1), 2022;49(3); Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service 2023;2; Information technologies 2024;30(1); International Journal of Open Information Technologies 2023; 11(9); Vestnik of Astrakhan State Technical University Series: Management, computer science and informatics 2022;2; Systems of Control, Communication and Security 2021;2.

Sergey M. Tretyakov, 3, K-64 Tikhoretsky Prospekt, 194064, St. Petersburg, Russia, Military Academy of the Signal Corps, Senior Lecturer, Department of Technical Support of Communications and Automation, Candidate of Engineering, Associate Professor; smt2k@mail.ru.

Вклад авторов в статью

Воеводин В.А.: Вербальная и формальная постановки задачи.

Третьяков С.М.: Введение, анализ литературы по теме, исследование актуальности научной задачи, анализ возможностей существующего методического аппарата.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

УДК 656.2.078.5:656.25
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-77-81

25 лет: Центр обучения АО «НИИАС» как интегратор поля компетенций технологического суверенитета

Twenty-five years: The JSC “NIIAS” Training Center as an Integrator of Technological Sovereignty Competencies

Капитонов К.С.[1]
Kapitonov K.S.[1]

[1] *Акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС»), Российская Федерация, Москва*
[1] *JSC “Scientific Research and Design and Survey Institute of Informatization, Automation and Communication on Railway Transport” (JSC “NIIAS”), Russian Federation, Moscow*
k.kapitonov@vniias.ru

Капитонов К.С.

Резюме. Цель. *Анализ эволюции и роли Центра обучения АО «НИИАС» в контексте цифровой трансформации железнодорожной отрасли, преодоления «компетентностного вакуума» и формирования кадрового потенциала для обеспечения технологического суверенитета. Определение методологических основ и перспективных направлений деятельности Центра как интегратора передовых компетенций.* **Методы.** *В исследовании применяются историко-логический анализ этапов развития Центра обучения, системный подход к рассмотрению его роли в отраслевой экосистеме «РЖД – НИИАС – ВУЗы», а также методология проблемно-ориентированного обучения, основанная на принципе «учить понимать океан, а не давать рыбу». Использованы методы каскадной передачи знаний и моделирования интеграционных процессов в образовательной среде.* **Результаты.** *Выявлены и охарактеризованы ключевые этапы трансформации миссии Центра обучения: от ликвидации системных пробелов в знаниях персонала к проактивному формированию единого поля компетенций и созданию профессий будущего. Раскрыта уникальная методология «живого» обучения, позволяющая минимизировать разрыв между образовательными программами и реальными требованиями к внедрению инноваций, таких как «виртуальная сцепка» и роботизированные комплексы. Разработана и представлена каскадная модель интеграции, обеспечивающая синхронизацию знаний между разработчиками технологий (АО «НИИАС»), заказчиком (ОАО «РЖД») и образовательными учреждениями. Анонсированы новые программы профессиональной переподготовки по роботизации, запуск которых запланирован на 2026 год: «Бизнес-аналитик по роботизации процессов на железнодорожном транспорте» и «Аудитор по роботизации производственных процессов на транспорте».* **Выводы.** *Деятельность Центра обучения АО «НИИАС» эволюционировала в направлении создания системы опережающей подготовки кадров, что позволяет не только реагировать на текущие вызовы, но и проактивно формировать будущее железнодорожного транспорта. Центр позиционируется как ключевой элемент интеллектуальной защиты критической инфраструктуры, чья методология и интеграционная модель способствуют преодолению «компетентностного вакуума», повышению безопасности движения и обеспечению технологического суверенитета отрасли. Перспективным направлением развития признано создание единой цифровой образовательно-производственной экосистемы («Цифровой контур подготовки кадров РЖД»).*

Abstract. Objective. *Analysis of the evolution and role of the JSC “NIIAS” Training Center in the context of the digital transformation of the railway industry, overcoming the “competence vacuum” and forming personnel potential for ensuring technological sovereignty. Definition of methodological foundations and promising directions of the Center’s activity as an integrator of advanced competencies.* **Methods.** *The study uses historical and logical analysis of the Training Center’s development stages, a systematic approach to considering its role in the industry ecosystem “RZD – NIIAS – Universities”, as well as the methodology of problem-oriented learning based on the principle of “teaching to understand the ocean rather than giving fish”. Methods of cascade knowledge transfer and modeling of integration processes in the educational environment are used.* **Results.** *The key stages of the transformation of the Training Center’s mission have been identified and characterized: from eliminating systemic knowledge gaps of personnel to proactively forming a unified field of competencies and creating professions of the future. The unique methodology of “live” learning is revealed, which minimizes the gap between educational programs and the real requirements for the implementation of innovations, such as “virtual coupling” and robotic complexes. A cascade integration model has been developed and presented, ensuring knowledge synchronization*

between technology developers (JSC "NIIAS"), the customer (JSC "RZD") and educational institutions. New professional retraining programs in robotization, scheduled for launch in 2026, are announced: "Business Analyst for Robotization of Processes in Railway Transport" and "Auditor for Robotization of Production Processes in Transport". **Conclusion.** *The activity of the JSC "NIIAS" Training Center has evolved towards creating a system of advanced personnel training, which allows not only to respond to current challenges but also to proactively shape the future of railway transport. The Center is positioned as a key element of the intellectual protection of critical infrastructure, whose methodology and integration model contribute to overcoming the "competence vacuum", improving traffic safety and ensuring the technological sovereignty of the industry. The creation of a unified digital educational and production ecosystem ("Digital Contour of RZD Personnel Training") is recognized as a promising direction for development.*

Ключевые слова: *НИИАС, цифровая трансформация, дополнительное профессиональное образование, технологический суверенитет, безопасность движения, человеческий фактор, компетентностный вакуум, единое поле компетенций.*
Keywords: *NIIAS, digital transformation, additional professional education, technological sovereignty, traffic safety, human factor, competency vacuum, unified field of competencies.*

Для цитирования: *Капитонов К.С. 25 лет: Центр обучения АО «НИИАС» как интегратор поля компетенций технологического суверенитета. Надежность. 2025;25(4):77-81. https://doi.org/10.21683/1729-2646-2025-25-4-77-81*
For citation: *Kapitonov K.S. Twenty-five years: The JSC "NIIAS" Training Center as an Integrator of Technological Sovereignty Competencies. Dependability. 2025;25(3):77-81. (In Russ.) https://doi.org/10.21683/1729-2646-2025-25-4-77-81*

Поступила: 21.08.2025 / **После доработки:** 21.10.2025 / **К печати:** 07.11.2025
Received on: 21.08.2025 / **Revised on:** 21.10.2025 / **For printing:** 07.11.2025

Введение

В 2025 году Центру обучения АО «НИИАС» исполнилось 25 лет. Этот юбилей является знаковым событием, позволяющим зафиксировать достигнутую зрелость функции дополнительного профессионального образования как стратегического актива, синхронного технологической эволюции Института и запросам отрасли на цифровую трансформацию. Актуальность темы статьи обусловлена нарастающими темпами технологических изменений на железнодорожном транспорте, которые опережают традиционные циклы обновления знаний, создавая тем самым «компетентностный вакуум» – системную угрозу безопасности движения и операционной устойчивости.

Центр обучения был создан в соответствии с Постановлением расширенного заседания Коллегии Министерства путей сообщения Российской Федерации от 15 февраля 2000 года №4 как ответ на системный вызов, обнаживший глубинные проблемы в подготовке кадров для железнодорожного транспорта: устаревшие знания эксплуатационного персонала и отсутствие единых стандартов формирования компетенций в области актуальных инноваций, внедряемых на транспорте. Создание Центра обучения на базе ВНИИАС МПС России стало стратегическим ответом на этот вызов – не на человеческую халатность, а на системный провал в компетенциях. Центр обучения должен был стать «интегратором знаний», обеспечивая соответствие компетенций специалистов железнодорожного транспорта современным технологиям и повышая операционную устойчивость.

Сегодня, четверть века спустя, железнодорожный транспорт столкнулся с новым классом вызовов. Цифровая трансформация, внедрение прорывных технологий интервального регулирования движения поездов «виртуальная сцепка» и «подвижный блок-участок» [1], роботизированных комплексов [2] и создание «Цифровой железнодорожной станции» происходят со скоростью, опережающей традиционные циклы обновления знаний. В свою очередь, это создает «компетентностный вакуум» как среди действующего персонала предприятий железнодорожного транспорта, так и в стенах учебных заведений транспорта.

Важно понимать, что этот «компетентностный вакуум» является прямой угрозой безопасности движения, так как действующий работник железной дороги или выпускник транспортного ВУЗа/колледжа с устаревшими знаниями – это не «нулевой» специалист, а специалист с отрицательной производительностью, который своими действиями способен создать аварийные ситуации.

1. Эволюция миссии: от ликвидации последствий к формированию будущего

Стратегически важным для АО «НИИАС» является активное участие в подготовке кадров, способных ответить на технологические вызовы современности и обеспечить технологический суверенитет железнодорожного транспорта. Эта задача решается через формирование Центром обучения АО «НИИАС» единого поля компетенций в сфере актуальных инноваций и

своевременную адаптацию образовательных программ в соответствии с меняющимися технологическими реалиями.

За 25 лет миссия Центра обучения АО «НИИАС» претерпела качественную трансформацию: от исправления системных ошибок к проактивному формированию кадрового капитала для технологического суверенитета железнодорожной отрасли.

За это время Центр прошел путь от традиционного обучения до интегратора передовых компетенций и организатора комплексного обучения для ВУЗов и предприятий транспорта, а в настоящее время становится центром компетенций, сопровождающим процесс внедрения современных решений в области цифровизации, автоматизации и роботизации железнодорожного транспорта. Важно подчеркнуть, что каждый этап развития не только отвечал на запросы отрасли, но и формировал кадровую базу для будущих технологических прорывов.

Сегодня Центр обучения АО «НИИАС» содействует распространению и достижению максимального синергетического эффекта от практического внедрения передовых технологий разработки АО «НИИАС» – путём популяризации знаний, разработки и реализации специализированных образовательных программ. Вместе с этим, через периодическое системное и структурированное обучение персонала компаний, внедряющих инновационные технологические решения АО «НИИАС», Центр обучения минимизирует для партнёров АО «НИИАС» ошибки, связанные с потенциальными рисками человеческого фактора. Это особенно важно на железнодорожном транспорте, где безопасность напрямую зависит от квалификации и бдительности персонала.

Ключевым положительным изменением образовательной парадигмы Центра стал отход от статичного представления нормативной базы. Слушатели образовательных программ Центра получают самую актуальную нормативную базу для учебных и практических занятий. При этом в своих программах Центр принципиально не «обеспечивает нормативной базой» в её статичном, архивном виде: в образовательном процессе слушатели программ повышения квалификации Центра погружаются в живую, действующую систему принятия решений, где документ – не догма, а инструмент. В дополнение к этому Центр обеспечивает постобразовательную поддержку через сессии «вопросов-ответов» с экспертами-разработчиками АО «НИИАС».

2. Методология «живого» обучения: философия понимания океана

Сегодня всё чаще на страницах профессиональных изданий эксперты заявляют о разрыве между образованием и практикой [3] и о том, что учебные программы транспортных вузов и колледжей зачастую отстают от требований работодателей. Существующие публикации, однако, недостаточно освещают роль корпоративных учебных центров, в частности, центров обучения при научно-исследовательских институтах – разработчиках передовых технологий, в качестве интеграторов компетенций и методологических хабов, способных нивелировать данный разрыв. Данная статья призвана восполнить этот пробел.

Следует пояснить, что проблема классического образования – несоответствие практикоориентированных компетенций выпускников ожиданиям работодателей – заключается в том, что студент получает «застывшую» выдержку из отраслевого приказа пятилетней давности. В реальности, при реализации перспективных проектов вроде «Высокоскоростная железнодорожная магистраль Москва – Санкт-Петербург» (ВСМ-1) или «Цифровая железнодорожная станция», технологии меняются быстрее, чем успевает обновиться официальный регламент. Это особенно актуально в условиях, когда технологии на Восточном полигоне [4] меняются быстрее, чем успевают обновиться официальные регламенты.

Контекст – главный инструмент Центра обучения АО «НИИАС». Подход, реализуемый в Центре обучения, – это обучение через контекст и принцип, который можно озвучить как «Мы не даём рыбу, мы учим понимать океан, в котором плавают эти рыбы». Эта методология реализуется через проблемно-ориентированное обучение на реальных инженерных задачах. Только так можно подготовить специалистов к реалиям, которые только появляются на транспорте, а не закрепить их в устаревших стандартах.

Например, изучение передовых технологий интервального регулирования движения поездов разработки АО «НИИАС» начинается не с положений приказов, а с постановки перед слушателями программы повышения квалификации инженерной задачи: «Как увеличить пропускную способность участка на 15% без изменения инфраструктуры?». Вместе со слушателями мы приходим к необходимости нового способа интервального регулирования. Лишь после совместного поиска решения слушатели знакомятся с реальными актуальными организационно-распорядительными документами, закрепляющими успешное решение, и детально разбирают с экспертами АО «НИИАС», почему каждый пункт в нормативных документах написан именно так, объясняя суть изменений в технологических регламентах. Такой подход противодействует «компетентностному вакууму» и обеспечивает «каскадное обновление знаний» – когда каждый выпускник программ повышения квалификации Центра прошел глубокий брифинг, изучил суть изменений и способен достигать максимального синергетического эффекта при практической реализации этой инновации.

При этом следует отметить, что на рынке образовательных услуг Центр обучения АО «НИИАС» является единственным центром компетенций, реализующим программы повышения квалификации по технологиям интервального регулирования движения поездов с использованием автоблокировки с подвижными блок-участками и гибридной технологии «виртуальная сцепка».

Вместе с этим, АО «НИИАС» имеет патенты на изобретения и свидетельства о государственной регистрации программ для ЭВМ, которые обеспечивают юридическую защиту интеллектуальной собственности и авторских прав по всему спектру компетенций АО «НИИАС», подтверждают статус единственного поставщика услуг, уникальность и эксклюзивность обучения в Центре обучения АО «НИИАС».

3. Единое поле передовых компетенций

Формирование единого поля компетенций является критическим фактором успешной цифровой трансформации железнодорожного транспорта России. Для своевременной подготовки компетентных кадров важно выстраивать тесное сотрудничество между заказчиками технологий, разработчиками новых технологий, компаниями-пользователями этих технологий и ведущими отраслевыми вузами.

Главный барьер для преподавателей ВУЗов на пути интеграции реальных документов ОАО «РЖД» в учебный процесс – не правовой, а методологический: отсутствие единого «поля компетенций» между заказчиком (РЖД), разработчиками инноваций (НИИАС) и ВУЗами.

Преподаватель зачастую не знает, как и зачем применять конкретный приказ в учебном процессе. Он видит не инструмент, а бюрократическую бумагу. Ему не хватает методической «обвязки» – практических ситуаций (кейсов), разборов, симуляторов, которые показывают этот документ в действии.

Мы решаем это через нашу «организационную пирамиду обучения». Центр обучения АО «НИИАС» выступает тем самым методологическим «хабом»: мы не просто «скидываем» преподавателям Учебных центров профессиональных квалификаций ОАО «РЖД» или ВУЗов папку с документами, мы приглашаем их на повышение квалификации и стажировки, где они сами учатся работать с этими документами на нашем стендовом оборудовании под руководством непосредственных разработчиков передовых технологий. После этого они уже не просто «передают информацию» студентам, а становятся проводниками реальных практик.

Если взглянуть в будущее академического транспортного образования, то видится целесообразным создавать сетевые образовательные программы, где лекции будут читать вузовские теоретики, а практические модули и кейсы будут вести специалисты компаний-разработчиков передовых технологий (таких, как АО «НИИАС») и компании-заказчика обучения (ОАО «РЖД») с прямым доступом к актуальным документам и системам. Это превратит преподавателя из лектора в модератора процесса освоения реальных компетенций.

При этом идеальный формат такого взаимодействия – не «обмен документами», а создание единой цифровой образовательно-производственной экосистемы. Идеальный практикоориентированный образовательный формат – это динамическая, аккредитованная цифровая среда, некий «Виртуальный отраслевой университет» или «Виртуальный Центр отраслевых компетенций», куда стекаются актуальные версии документов, практические кейсы (в том числе на основе вопросов из рабочей практики слушателей), симуляторы и данные с полигонов железных дорог. Студент или слушатель программы повышения квалификации должен работать не с текстовым PDF-файлом, а с интерактивной средой, где документ является частью игрового движка, управляющего виртуальной железнодорожной инфраструктурой.

Модель «РЖД – хранитель секретов, ВУЗ – проситель» в условиях стремительного внедрения инноваций только способствует процессу сопротивления внедрению этих самых инноваций. Мы все – компания-заказчик обучения, компании-разработчики передовых технологий и отраслевые транспортные ВУЗы – должны стать партнёрами в создании человеческого капитала. Это требует глубинной интеграции и совместного доверительного взаимодействия на поле образовательной среды.

Прототипом может являться положительный опыт взаимодействия Центра обучения АО «НИИАС» с Передовой инженерной школой «Академия ВСМ» РУТ (МИИТ).

На основе этого опыта возможно в ближайшем будущем совместными усилиями создать «Цифровой контур подготовки кадров РЖД» – федеральную платформу, объединяющую всех участников системы транспортного образования: школы, детские железные дороги, колледжи, ВУЗы, Учебные центры профессиональных квалификаций ОАО «РЖД» и образовательные направления деятельности компаний-разработчиков передовых инноваций, внедряемых на инфраструктуре российских железных дорог (таких, как АО «НИИАС»). И эта цифровая платформа должна работать по принципу единого источника истины, где все учебные материалы синхронизированы с актуальной производственной повесткой ОАО «РЖД», документацией и стандартами.

4. Взгляд в будущее: формирование профессий для цифровой железной дороги

Центр обучения АО «НИИАС» активно формирует образовательную повестку будущего. В 2026 году запланирован запуск двух новых программ профессиональной переподготовки специалистов и руководителей производственных предприятий железнодорожного транспорта – главных инженеров, главных технологов, главных механиков и энергетиков, инженеров-технологов и других инженерных кадров:

«Бизнес-аналитик по роботизации процессов на железнодорожном транспорте (специалист по роботизации производств)» – выпускники этой программы смогут определять процессы для роботизации, выполнять технико-экономические обоснования проектов роботизации, разрабатывать технические задания по роботизации

производств, осуществлять выбор и внедрять роботизированные ячейки с интеграцией в инновационные решения АО «НИИАС», в целом управлять жизненным циклом роботизированных решений;

«Аудитор по роботизации производственных процессов на транспорте» – выпускники этой программы смогут выполнять аудит предприятий на предмет внедрения максимально эффективных робототехнических решений, определять процессы для роботизации, выполнять технико-экономические обоснования и инициировать проекты роботизации с предложением соответствующих источников финансирования.

Эти программы – прямой ответ на тренды массовой роботизации на транспорте [2, 4]. Они станут не только инструментом внедрения роботизации на транспорте, но и гарантом соответствия технологий стандартам, требованиям безопасности и эффективности.

Таким образом, Центр обучения АО «НИИАС» не просто реагирует на тренды, а сам формирует профессии будущего, готовя кадры для аудита процессов и интеграции роботизированных комплексов, которые только начинают внедряться на инфраструктуре ОАО «РЖД».

Это закономерный этап эволюции: от обучения конкретным операциям – к формированию системных компетенций управления, анализа и контроля над автоматизированными технологическими процессами.

Заключение

Лучший результат обучения на ошибках прошлого – это предотвращённые трагедии будущего. Создавая систему опережающей подготовки кадров, Центр обучения АО «НИИАС» превращается в центр компетенций, выстраивающий интеллектуальную защиту критической инфраструктуры, который готов не только к сегодняшним рискам, но и формирует будущее железнодорожного транспорта. Центр обучения АО «НИИАС» – это Центр инноваций, где каждое обучение – это шаг вперёд.

Благодарности

Автор выражает благодарность руководителям и экспертам АО «НИИАС», а также коллективу Центра обучения АО «НИИАС» за многолетнюю совместную работу, методологическую поддержку и существенный вклад в развитие системы дополнительного профессионально образования железнодорожной отрасли Российской Федерации.

Список литературы

1. «Виртуальная сцепка» на Восточном полигоне: достигнутые эффекты и направления развития / [А.И.Долгий и др.] // Транспорт Российской Федерации. – 2023. – № 5–6. – С. 15–19.

2. Долгий А.И., Хатамаджиян А.Е., Озеров А.В., Бочков А.В. Роботизация на железнодорожном транспорте // Интеллектуальный транспорт. – 2025. – Вып. 3.

3. Информационные материалы сайта ТАСС — ВЦИОМ зафиксировал огромный разрыв между образованием и потребностями работодателей в РФ. — URL (дата обращения 05.11.2025): https://tass.ru/obschestvo/18811605 .

4. Долгий А.И. Технологии интенсивного развития ОАО «РЖД» – эффективный ответ на современные вызовы // Железнодорожный транспорт. – 2025. – № 7.

References

1. "Virtual Coupling" at the Eastern Test Site: Achieved Effects and Directions for Development / A.I. Dolgii et al. // Transport of the Russian Federation. 2023. No. 5–6. – pp. 15–19.

2. A.I. Dolgy, A.E. Khatamajian, A.V. Ozerov, and A.V. Bochkov, "Robotization in Railway Transport," Intelligent Transport, 2025. Issue 3.

3. Information materials from the TASS website. VTsIOM has recorded a significant discrepancy between the education system and the needs of employers in the Russian Federation. URL (accessed 11/5/2025): https://tass.ru/obschestvo/18811605.

4. A.I. Dolgy, "Technologies for the Intensive Development of Russian Railways: An Effective Response to Modern Challenges", Railway Transport. 2025. No. 7.

Сведения об авторе

Капитонов Константин Сергеевич; 109029, Россия, г. Москва, ул. Нижегородская, д. 27, стр. 1; АО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС»), начальник Центра обучения; E-mail: k.kapitonov@vniias.ru.

About the author

Kapitonov Konstantin Sergeevich; 109029, Russia, Moscow, Nizhnyaya Street, 27, Building 1; JSC Research and Design Institute of Informatization, Automation, and Communications in Railway Transport (JSC NIIAS), Head of the Training Center; E-mail: k.kapitonov@vniias.ru.

Вклад автора в статью

Автор **Капитонов К.С.** выполнил концептуализацию исследования, провел анализ исторических этапов развития и трансформации миссии Центра обучения АО «НИИАС», разработал и систематизировал методологию «живого» проблемно-ориентированного обучения, сформулировал принципы каскадной модели интеграции в экосистему «РЖД – НИИАС – ВУЗы», осуществил постановку целей и задач новых программ профессиональной переподготовки по роботизации, подготовил, отрецензировал и отредактировал окончательный текст рукописи.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

7-я Евразийская конференция «Риск-ориентированное проектирование и эксплуатация инфраструктурных систем: парадигма устойчивого развития»

21-23 октября в Азербайджанском государственном университете нефти и промышленности (АГУНП) состоялась церемония открытия 7-й Международной Евразийской конференции по рискам «РИСК-2025». Конференция «Риск-ориентированное проектирование и эксплуатация инфраструктурных систем: парадигма устойчивого развития» собрала ведущих международных экспертов в области инжиниринга, энергетики, управления экосистемами, технологических рисков и устойчивого развития.

Конференция организована совместно компанией AMIR Technical Services, Азербайджанским государственным университетом нефти и промышленности, Форумом Гнеденко Международной группы США по устойчивому развитию, Международной комиссией по ирригации и дренажу (ICID) и Миланским политехническим университетом, Италия.

Выступая на открытии конференции, ректор АГУНП, доцент Руфат Азизов сказал, что в сегодняшнем быстро меняющемся мире безопасное и устойчивое управление инфраструктурными системами имеет глобальное значение. Ректор подчеркнул, что укрепление научного сотрудничества и обмена знаниями в этом направлении, особенно формирование новых перспектив по управлению рисками за счет применения технологий искусственного интеллекта, играет важную роль в подготовке следующего поколения инженеров.

Ректор АГУНП отметил, что конференция RISK-2025 служит важной платформой не только для обмена научными исследованиями, но и для укрепления регионального и международного партнерства. Он выразил уверенность, что результаты конференции внесут практический вклад в планирование инфраструктурных проектов, стратегии энергетической безопасности и устойчивого развития.

Генеральный председатель конференции, профессор Вугар Алиев подробно проинформировал о мероприятии и отметил, что в этом году на встрече рассматрива-

ются новые направления риск-инжиниринга, влияние технологических изменений на экосистемы и роль человеческого фактора с различных аспектов.

Особую ценность конференции придало участие двух лауреатов Нобелевской премии мира – профессора Святослава Тимашева и профессора Елены Никитиной в числе международных гостей.

Руководитель Центра науки и инжиниринга Уральского федерального университета РАН, лауреат Нобелевской премии мира, профессор Святослав Тимашев выступил с докладом на тему «Искусственный интеллект в риск-ориентированном проектировании и эксплуатации инфраструктур: риски и возможности». Он приводил научные аргументы как о потенциальных опасностях, так и о значительных возможностях применения искусственного интеллекта в промышленных системах. Тимашев подчеркнул, что риск – это не только угроза, но и важный этап развития. Он подчеркнул необходимость более глубокого изучения этических аспектов и аспектов безопасности алгоритмов искусственного интеллекта при проектировании инфраструктурных проектов.

Заведующая отделом глобальных экономических проблем Института мирового хозяйства и международных отношений РАН, лауреат Нобелевской премии мира, профессор Елена Никитина выступила с докладами «Изменение климата: развитие международной помощи для глобальной адаптации на Юге» и «Изменение климата в Арктике: адаптация и снижение риска бедствий». Профессор Никитина отметила, что для минимизации последствий изменения климата в южных регионах необходимо укреплять механизмы международного содействия, расширять финансирование экологических проектов и технологическую поддержку. По его словам, адаптация к изменению климата имеет стратегическое значение с точки зрения поддержания глобальной экономической стабильности и социального благополучия.

В рамках конференции в течение дня были организованы панельные и стендовые сессии по принятию решений, ориентированных на риск, новым технологиям в области продовольственной безопасности и мелиорации, а также снижению риска стихийных бедствий.

Инфраструктурные системы в рамках конференции определяются как критически важные физические объекты, объекты коммунальной и оборонной инфраструктуры, критически важные промышленные активы и цепочки поставок, а также критически важные информационно-коммуникационные технологии и сети, разрушение или деградация которых или недоступность

в течение длительного периода существенно повлияют на социальное и экономическое благосостояние стран, устойчивое развитие. Инфраструктурные системы могут быть повреждены, уничтожены или нарушены стихийными бедствиями, халатностью, авариями, компьютерным взломом, преступной деятельностью и злонамеренным ущербом, а также преднамеренными актами терроризма.

Евразийская платформа рисков, созданная компанией «AMIR Technical Services», имеющая опыт успешного проведения шести многосторонних конференций «RISK» (2019 – 2024), ставших эффективной площадкой для генерации идей и смыслов теории риска, поиска путей стимулирования инноваций для минимизации существующих и возникающих рисков изменения климата, претендует на роль международного координационного центра Движения корней инициативы «Зеленая планета 2060» (GPM 2060).

На 7-й Евразийской конференции «RISK-2025» обсуждены текущие исследования взаимозависимости инфраструктурных систем с точки зрения устойчивого развития, рисков безопасности, вызванных природными, технологическими и преднамеренными угрозами.

Организаторы считают важным установление органической связи между минимизацией рисков изменения климата, чрезвычайных ситуаций и устойчивым развитием стран, вовлечение всех заинтересованных сторон и широкой общественности в анализ, оценку и управление рисками, включая популяризацию идей устойчивого развития во всех средствах массовой информации, образовательных и научных средах и всецело поддерживают дальнейшее развитие инновационных позиций и действий в рамках многостороннего и регионального сотрудничества и обмен передовым опытом и решениями в области устойчивого развития на основе основных решений и итогов КС-29.

С пленарным докладом ФАЗОВОЕ ПРОСТРАНСТВО СОСТОЯНИЙ КАК ИНСТРУМЕНТ АНАЛИЗА И УПРАВЛЕНИЯ ПОВЕДЕНИЕМ СЛОЖНЫХ СИСТЕМ в работе конференции принял участие ученый секретарь АО «НИИАС» д.т.н. Бочков Александр Владимирович. Доклад посвящен применению методов хаотической динамики и анализа больших данных для управления сложными системами. Автором предложен инновационный подход, основанный на использовании фазового пространства состояний (ФПС) и квазиаттракторов, который позволяет анализировать и прогнозировать поведение систем в условиях нелинейности и высокой динамичности. В отличие от традиционных статистических методов, данный подход фокусируется на динамике изменений показателей, а не на их абсолютных значениях, что обеспечивает более точное выявление критических точек и ранних признаков кризисов. Особое внимание уделяется концепции квазиаттракторов как областей относительной устойчивости, где система временно сохраняет стабильность перед переходом в новое состояние. Для мониторинга и управления предложено сочетание ФПС с контрольными картами Шухарта, что позволяет отслеживать отклонения и выявлять нестабильность. Практическая значимость метода продемонстрирована на примере анализа пандемии COVID-19, где фазовые траектории и динамика квазиаттракторов позволили оценить эффективность принимаемых мер в разных странах. Подход обладает универсальностью и может быть применен в экономике, экологии, технических и социальных системах. Перспективы дальнейших исследований включают интеграцию с искусственным интеллектом, разработку адаптивных систем управления и расширение методов визуализации для многомерных данных.

Информация о конференции доступна по ссылке: www.eurasianrisk2025.com

Ученый секретарь АО «НИИАС», д.т.н. А.В. Бочков

Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-85-90

Жива ли еще теория надежности?

Ушаков И.А.

Во время банкета на закрытии конференции MMR-2004 Conference (Математические методы в надежности, Санта-Фе, США), один из ведущих Западных специалистов по надежности профессор Университета Джорджа Вашингтона (Вашингтон, США) Нозер Сингпурвалла выступал в качестве ведущего дискуссию. Темой дискуссии им был выбран, скажем прямо, провокационный вопрос: «Жива ли еще теория надежности?» Сама по себе постановка такого вопроса вызвала буквально бурю негодования среди участников: «Да, да, да! Она жива и процветает!»

Что же происходит в наши дни, и почему такой вопрос в принципе возник у серьезного математика, посвятившего многие годы развитию этой самой теории надежности?

Можно попытаться ответить на этот вопрос, хотя ответ этот будет далеко неоднозначным. На правах, если уж, не «динозавра в надежности», то уж, во всяком случае, «мамонта», я берусь обсудить эту непростую тему.

1. Факторы, определявшие и определяющие развитие теории надежности

1.1. Теория зарождается в недрах практики

Вспомним, когда начался бум теории надежности. Шла Корейская война (1950-53 гг.). Военная техника в первые же годы «холодной войны» бурно развивалась: обе стороны в процессе гонки вооружений создавали все более эффективное «миротворческое оружие, системы усложнялись, а промышленность мирного времени едва успевала за потребностями американских и советских «ястребов». Обе стороны несли огромные потери из-за частых отказов военной техники, а но первыми одумались американцы: они всегда лучше считали деньги. В США начали уделять повышенное внимание вопросам качества, надежности и обслуживания техники: начали проводиться ежегодные симпозиумы Института Радиоинженеров (IRE – Institute of Radio Engineers), а позднее, Института Инженеров Электрики и Электроники (IEEE – Institute of Electrical and Electronics Engineers), которые выпускали труды конференций. К 60-м годам прошлого столетия на читателей обрушился мощный поток публикаций по надежности... Примерно в это же время началась активизация работ по надежности и в бывшем Советском Союзе. Академик Аксель Иванович Берг – «отец советской кибернетики» – пустил крылатую фразу: «Надежность – проблема № 1!»

Иными словами, появилась насущная проблема, которая требовала быстрого и квалифицированного решения.

1.2. Уменьшение актуальности проблемы

Не последнюю роль сыграло в спаде интереса к теории надежности среди разработчиков и производителей техники (в особенности электронной), что аппаратура стала существенно надежнее. Если наработка на отказ электронных («вакуумных») ламп в 50-60-х годах измерялась десятками, в лучшем случае – сотнями часов, то нынешние микросхемы, заменяющие по своим функциональным возможностям целые блоки, а то и стойки «ламповой аппаратуры», имеют интенсивность отказа порядка $10^{-6} – 10^{-8}$ 1/час.

Понятно, что в такой ситуации проблема надежности перешла на другой уровень – на уровень больших систем.

1.2.1. Перенасыщенность «научного рынка».

Теория всегда должна опережать нужды сегодняшний практики, иначе она будет держать руку на пульсе уже умершего ©... Однако в настоящее время теория надежности либо слишком сильно «рванула» вперед, либо заползла в «экзотические тупики». Практика с успехом обходится громадным и – нужно отметить – первоклассным общетеоретическим багажом. «Локально» же возникающие текущие проблемы и разрешаются на локальном уровне.

Сейчас, видимо, фирмам-разработчикам выгоднее и эффективнее приглашать на текущие проекты по надежности квалифицированных специалистов со стороны для выполнения конкретных исследований.

1.2.2. Возникновение «теории ради теории».

Если просмотреть первые работы надежности конца 50-х и начала 60-х годов прошлого столетия, то в глаза бросается прагматичность работ по надежности. Даже «чистые математики» писали не для себя, а для «пользователей»: конечные результаты были прозрачны и практическая их применимость была очевидна. Однако уже в 70-е годы стали появляться публикации, либо посвященные изучению «экзотических» (а то и вовсе надуманных) моделей, либо содержащие головоломные математические выкладки (если не сказать – выкрутасы), за которыми терялся и смысл задачи да и конечные результаты представлялись в совершенно неудобоваримой форме. Это были работы, которые, как однажды сказал Борис Владимирович Гнеденко, авторы писали для себя, а не для читателя!

Это, безусловно, положило начало определенной дискредитации теории надежности, что позволило, например, одному из ведущих советских конструкторов космических аппаратов заявить: «Теорией надежностью занимаются те, кто в надежности ничего не понимает. Те же, кто понимает в надежности, те просто делают надежную аппаратуру!» (К несчастью, такое отношение к теории привело к тому, что произошел тот печальный случай, когда при посадке «Союза-11» трое космонавтов погибли из-за непродуманной схемы резервирования в системе разгерметизации: конструкторы не подумали о том, что релейные схемы имеют отказы типа ложного срабатывания как на замыкание, так и на размыкание).

Потеря прагматичности работ по надежности стала с годами пугающей...

1.2.3. Вопросы «современной технической моды».

Однажды я спросил своего давнего друга Роберта Макола, которого многие могут знать по его книге «Системотехника», чем вызвано появление нового направления – Наука управления (Management Science)? Ведь была одно время в моде *кибернетика,* потом она породила *системотехнику,* потом возникло *исследование операций,* а теперь вот *наука управления*... «Так ты уже сам ответил на свой вопрос: смена моды! Каждый раз придумывается новое название, чтобы заставить того, кто платит, раскошелиться – это же новое! Это же лучше, чем то, что было!» – ответил мне Макол.

Конечно, это шутка, но, как говорится, в каждой шутке есть *доля шутки.*

1.2.4. Смещение «центра тяжести» проблемы.

Теория надежности всегда уделяла основное внимание анализу систем: понятно, что на уровне элементов теоретические методы сводились в основном к задачам планирования испытаний и обработки экспериментальных данных. Современные системы все более и более усложняются – посмотрите на глобальные транспортные системы, телекоммуникационные сети, «компьютерные коммуны» ... И здесь, действительно, есть много интересных, сложных и актуальных задач, но от специалиста по надежности уже требуется не написание общетеоретических работ, а решение этих конкретных задач, участие в «живых проектах». Зачастую задачи настолько специфичны, что их решения уже не носят междисциплинарного характера. Но, безусловно, решение этих задач опирается на общеметодологическую и математическую базу современной теории надежности.

Так что слухи о смерти теории надежности представляются преждевременными, как говаривал Марк Твен, хотя пора ее расцвета, несомненно, уже осталась позади...

2. «Фронт работ» по надежности в бывшем Советском Союзе

К концу 50-х в Советском Союзе публикации по надежности стали появляться, как грибы после доброго осеннего дождя, а в 1958 г. состоялась Первая Всесоюзная конференция по надежности, на которой председательствовал В.И. Сифоров.

Стали формироваться научные школы – в Москве, Ленинграде, Киеве, Риге...

Московская школа. К концу 50-х в Москве сформировалась неформальная группа, в основном, из преподавателей Военно-воздушной академии им. Н.Е. Жуковского (Б. Васильев, Г. Дружинин, М. Синица), а также военных специалистов из ЦНИИ-22 Министерства Обороны (В. Кузнецов, И. Морозов, К. Цветаев).

В это же время в Научно-техническом обществе по радиотехнике им. А.С. Попова (председатель ак. В. Сифоров) замечательный организатор науки Яков Михайлович Сорин создал Секцию надежности, где активную роль стал играть Б. Левин. При активной поддержке ак. А. Берга, в 1959 г. Я. Сорин создал первый в Москве (и, видимо, второй в бывшем Советском Союзе) отдел надежности в одном из НИИ Министерства электронной промышленности. В этом отделе родилась первая ведомственная методика расчета надежности электронной аппаратуры, легшая затем в основу общесоюзных стандартов по надежности.

С первого же года существования этого отдела надежности, к его работе были привлечены первоклассные математики во главе с ак. АН Украины Борисом Владимировичем Гнеденко. В эту группы входили профессора Московского Государственного университета им. М.В. Ломоносова Ю. Беляев и А. Соловьев, а также первоклассный статистик Я. Шор из одного московского военного НИИ. Они вместе с Я. Сориным и сотрудником отдела И. Ушаковым стали официальными консультантами Госстандарта СССР, где был (опять же по инициативе Я. Сорина) создан Научно-технический совет по проблеме надежности.

В 1962 г. Б. Гнеденко и Я. Сорин организовали еженедельный Семинар по надежности, который проходил в вечернее время в МГУ. На этом семинаре всегда было очень много слушателей – как говорится, яблоку негде было упасть, хотя заседания проходили не в аудиториях, а в лекционных залах. Чуть позднее этот семинар, который вели Б. Гнеденко, Ю. Беляев и А. Соловьев, а позднее присоединился и И. Коваленко, перерос в Семинар по надежности и массовому обслуживанию, который так и закрепился в МГУ.

«Тандем Сорин-Гнеденко» заработал в полную мощность и не снижал обороты в течение примерно 25 лет, проделав поистине гигантскую организационную и просветительскую работу. Примерно через год Я. Сорин организовывает Кабинет надежности и качества при Московском Политехническом музее. Своей правой рукой он выбирает Б. Гнеденко, делая его научным руководителем, а «всеобщим замом» назначает И. Ушакова. Задачей Кабинета было «нести знания в массы»: в то время при неиссякаемой организаторской и пропагандистской деятельности Я. Сорина через Госстандарт было проведено решение о создании службы надежности во всех промышленных (в основном, оборонных) министерствах.

Громадный коллектив докторов и кандидатов наук работал в этом Кабинете на общественных началах. (Помните шуточный ответ на вопрос: что такое работа на общественных началах? Это когда ты вкалываешь, но бесплатно, а обычная работа – это когда ты ничего не делаешь, но получаешь зарплату).

Был составлен график ежедневных консультаций для инженеров-разработчиков и работников служб надежности. Консультации проводились высококвалифицированными специалистами – как опытными инженерами (А. Аристов, И. Аронов, Б. Бердичевский, Э. Дзиркал, Р. Улинич, И. Ушаков, Ф. Фишбейн и др.), так и математиками (Ю. Беляев, В. Каштанов, А. Соловьев, Я. Шор и др.) Ежедневные консультации собирали по 15-20 человек в день, а на лекции (раз в две недели – две двухчасовых лекции) битком набивалась Главная Аудитория Политехнического музея, причем больше по-

ловины из них были командированные с промышленных предприятий, приезжавшие отовсюду: из Ленинграда и Киева, из Риги и Владивостока (!), из Новосибирска и Ташкента, из Еревана и Тбилиси... Карта СССР, висевшая в кабинете Якова Михайловича, все была утыкана красными флажками с указанием «охваченных» городов.

В 1969 г. при журнале «Стандарты и качество» все тот же неугомонный Я. Сорин создает приложение «Надежность и контроль качества», а своими замами выбирает Б. Гнеденко, И. Ушакова и Я. Шора. После смерти Якова Михайловича Главным редактором стал Б. Гнеденко.

Примерно тогда же в издательстве «Советское радио» (позднее – «Радио и связь») создается Редакционный свет по надежности во главе с Б.В. Гнеденко. Начинается выпуск книг в серии «Библиотека инженера по надежности», которые сыграли огромную роль в воспитании специалистов по надежности во всех уголках бывшего Советского Союза.

Где-то в середине 70-х в журнале «Известия АН СССР. Техническая кибернетика» открывается раздел «Теория надежности».

И, конечно же, нельзя не вспомнить бесконечные «автопробеги по бездорожью и разгильдяйству», которые устраивал Я. Сорин со своими сподвижниками! Это были Киев, Ленинград, Ереван, Тбилиси, Рига и Горький... Именно по его инициативе и с его поддержкой в различных городах нашей страны были созданы кабинеты надежности, аналогичные Московскому (а Московский был с почетом переименован в Центральный).

Трудно перечислить всех представителей Московской школы надежности, но, все же, необходимо упомянуть некоторые имена, без которых картина не была бы полна: А. Аристов, И. Аронов, В. Гадасин, Ю. Коненков, Г. Карташов, И. Павлов, А. Райкин, Р. Судаков, О. Тескин, В. Шпер.

Говоря о Московской школе надежности, нельзя не упомянуть о двух книгах, которые, в определенном смысле, подвели итоги многолетних исследований.

Прежде всего, это прекрасная книга «Математические методы в теории надежности», написанная Б. Гнеденко, Ю. Беляевым и А. Соловьевым [1]. Книга была быстро переведена на английский язык [2]. И сейчас, спустя уже более сорока лет, она, наряду с книгой Р. Барлоу и Ф. Прошана [3, 4], переведенной на русский язык [5, 6], остается лучшей монографией по общей теории надежности.

Во вторую очередь, можно отметить «Справочник по расчету надежности» Б. Козлова и И. Ушакова [7], выдержавший несколько переизданий [8–9] и переводов [10–14]. Этот справочник долгие годы оставался настольной книгой инженеров-разработчиков.

Ленинградская школа. В 1959г. в одном из Ленинградских НИИ Министерства Судостроительной промышленности бы организован первый отечественный отдел надежности, который возглавил И. Маликов. В том же году группа авторов-основоположников ленинградской школы надежности (И. Маликов, А. Половко, Н. Романов и П. Чукреев) выпустила «Основы теории и расчета надежности» [15]. В книге было всего 139 стр., но, как говорится: «Мал золотник, да дорог». Эта была первая – пусть и «худенькая» – монография, где впервые на русском языке была систематически изложена элементарная теория надежности.

Вслед за Московским Кабинетом надежности, в Ленинграде начал функционировать аналогичный кабинет при Доме научно-технической пропаганды. Здесь «организатором и вдохновителем побед» был Анатолий Михайлович Половко, преподававший в Военной академии им. А.Ф. Можайского.

В 1964 г. А. Половко выпустил одну из первых отечественных серьезных монографий по теории надежности [16]. Она же была и первой отечественной книгой, переведенной на Западе [17]. Ленинградская школа надежности дала много интересных и высококвалифицированных ученых: это Л.К. Горский, И.А. Рябинин, Н.М. Седякин, Г.Н. Черкесов, И.Б. Шубинский и др.

Киевская школа. В Киеве в стенах Киевского военно-инженерного радиотехнического училища (КВИРТУ) расцвела школа под руководством Николая Алексеевича Шишонка. В эту группу входили Л. Барвинский, М. Ластовченко, Б. Креденцер, А. Перроте, В. Репкин, С. Сенецкий. В 1964 г. коллектив авторов, возглавлявшийся Н. Шишонком, опубликовала монографию «Основы теории надежности радиоэлектронной аппаратуры» [18].

Параллельно в Киевском Государственном университете, а позднее в Институте кибернетики (ныне им. В.М. Глушкова) очень сильная группа математиков, в основном учеников Б.В. Гнеденко, получила большое число интересных научных результатов в области надежности и массового обслуживания. В этой группе были такие выдающиеся математики, как академики АН Украины В. Королюк и И. Коваленко, а также В. Волкович, В. Заславский, Т. Марьянович, А. Турбин и др.

Рижская школа. «Отцом-основоположником» Рижской школы надежности является Хаим Борисович Кордонский, заведовавшей кафедрой в Рижском Институте инженеров гражданской авиации (ныне Рижский Технический университет). Ученик крупного советского математика ак. Ю. Линника, Х. Кордонский унаследовал черты своего учителя: он был не только прекрасным ученым, но и замечательным преподавателем. Его ученики – А. Андронов, И. Герцбах и Ю. Парамонов были уже в ранние годы известны по всему бывшему Советскому Союзу.

В отличие от многих других школ надежности, Рижская отличалась прагматизмом и ориентацией на насущные инженерные проблемы. В 1963 г. выходит монография Х. Кордонского [19], где уже приведены некоторые модели надежности, а в 1969 г. его книга совместно с И. Герцбахом [20]. Затем в 1969 г. вышла книга И. Герцбаха [21], пожалуй, лучшая из книг по моделям профилактики.

Усилиями Х. Кордонского в Рижском Доме научно-технической пропаганды, что располагался тогда на углу одной из улочек, вливавшихся на площадь Домского Собора, был организован регулярный семинар по надежности.

Независимо в Риге также работали над проблемой надежности В. Левин и В. Леонтьев.

Иркутская школа. Здесь вопросами надежности энергосистем занимался директор Сибирского энергетического института ак. Юрий Николаевич Руденко, собравший в отдел надежности талантливую молодежь (Н. Воропай, В. Зоркальцев, Г. Колосок, Л. Криворуцкий). Он инициировал работы по анализу живучести Единой энергетической системы страны (ЕЭС), за что вместе с И. Ушаковым получил престижную Премию им. Г.М. Кржыжановского от АН СССР. Они же в соавторстве выпустили и первую книгу о надежности энергосистем [22, 23].

Знаменитые «Руденковские семинары» семинары на Байкале привлекали не только экзотикой Сибири... Там собирался весь «цвет» специалистов по надежности в энергетике со всей страны: Ю. Гук, Н. Манов, Е. Червоный, Е. Ставровский, М. Сухарев, Э. Фархад-заде, М. Чельцов, Г. Черкесов, М. Ястрбенецкий и др.

Нельзя не сказать хотя бы несколько слов и о других школах надежности в бывшем советском Союзе.

Ташкент. Здесь работы по надежности и статистическому контролю качества возглавил ставший впоследствии Вице-президентом Узбекской АН Сагды Хасанович Сираждинов, ученик А.Н. Колмогорова. Здесь в области надежности работали такие математики и прикладники, как Т. Азларов, А. Усманов, Ш. Форманов и др.

Горький. Горьковском филиале ВНИИС Госстандарта большую работу по развитию статистических методов надежности и контроля качества проводили Л. Лейфер и В. Лапидус-старший. (Как и в «Двенадцати стульях» Ильфа и Петрова, здесь были также два брата Лапидуса).

Минск. В Минском Высшем инженерном радиотехническом училище (МВИРТУ) работала группа под руководством профессора Александра Михайловича Широкова (В. Скрипник, А. Назин).

Тбилиси. Еще в начале 60-х здесь появился первый кандидат технических наук именно по надежности – Ш. Бебиашвили, ученик ак. В.И. Сифорова. В последующие годы под руководством И. Микадзе работала группа молодых прикладников-математиков.

Ереван. В Ереванском Государственном университете и в Ереванском НИИ электронных машин работало несколько хороших специалистов, прежде всего, Э. Даниелян, а также А. Геворкян, А. Геокчян, Г. Маранджян и др.

Владивосток. В Институте автоматики и процессов управления Дальневосточного Отделения Академии наук работала сильная группа специалистов по надежности (О. Абрамов, А. Супоня).

И все же перечень этот, наверняка, далек от завершения...

3. Краткая история развития отечественной теории надежности

Как уже отмечалось, бурный поток идей в теории надежности хлынул в самом начале «холодной войны», когда стали появляться вес более и более сложные системы вооружения, которые простаивали больше, чем работали.

Первые шаги в развитии того, что мы теперь называем теорией надежности, были сделаны в Америке. Однако отечественные специалисты быстро включились в этот процесс, а вскоре не только сравнялись, но во многом и опередили «законодателей моды».

Не претендуя ни в коей мере на полноту обзора, попытаемся все же дать беглое описание основных научных направлений, которые представляли специфику отечественной школы теории надежности.

Интересный метод оценки доверительных границ для надежности системы, основанных на результатах безотказных испытаний входящих в нее элементов, был получен Р. Мирным и А. Соловьевым [24]. Затем некоторые более общие результаты были получены Ю. Беляевым, который предложил метод, основанный на статистических испытаниях [25, 26]. Большое число новых аналитических результатов для различных случаев было получено И. Павловым [27–29], Р. Судаковым [30], О. Тескиным [31].

Много работ было посвящено анализу сложных систем с деградацией качества функционирования за счет «частичных отказов». Действительно, вряд ли сложную систему можно характеризовать примитивными бинарными критериями работоспособности типа «да–нет» [32–34].

Доказательство двух предельных теорем в теории процессов восстановления (рекуррентных точечных процессов) сыграло решающую роль в развитии теории надежности восстанавливаемых систем. А. Реньи [35] сформулировал и доказал теорему асимптотического «разрежения» точечного потока, и тогда же Г. Ососков [36] доказал теорему об асимптотическом поведении суперпозиции точечных потоков. Позже Ю. Беляев, Григелионис и И. Погожев обобщили эти результаты. Эти асимптотические теоремы позволяют построить практически удобные инженерные методы приближенного анализа сложных высоконадежных систем с восстановлением [37].

Б.В. Гнеденко [38, 39] был первым, кто начал разрабатывать асимптотические методы анализа систем с восстановлением еще в начале 60-х годов. Он рассмотрел дублированную систему и показал, что асимптотическое распределение времени безотказной работы таких систем является экспоненциальным и не зависит от распределения времени восстановления (если это время в среднем мало по сравнению с наработкой на отказ). Эти первые работы открыли новое направление в теории надежности, которое затем успешно развивали, в первую очередь, И. Коваленко [40–42] и А. Соловьев [43–46].

Интересные идеи агрегирования состояний полумарковских процессов с применениями к задачам надежности были предложены В. Королюком и А. Турбиным [47, 48], а затем развиты в ряде работ [49, 50]. Интересные приложения к надежности содержатся в работах В. Анисимова [51] и Д. Сильвестрова [52].

Методы оптимального резервирования получили свое развитие в работах [53–57]. Результаты первых работ по оптимальному обеспечению запасными элементами вошли в разрабатывавшиеся тогда военные стандарты.

Такое важное направление в теории надежности, как ускоренные испытания, возникло на самой заре развития теории надежности. Достаточно вспомнить работы

Н. Седякина [58], Х. Кордонского и И. Герцбаха [59], А. Перроте, Г. Карташова и К. Цветаева [60]. Модели ускоренных испытаний с нагрузками, зависящими от времени, рассмотрели В. Багданавичус и М. Никулин [61].

В заключение хочется отметить прекрасную книгу под общей редакцией Бориса Владимировича Гнеденко [62], в которой подытожены отечественные достижения в области теории надежности.

Заключение

Естественно, что эти краткие заметки не смогли отметить всех тех, кто внес заметный вклад в развитие теории и практики надежности. Автор попытался лишь сделать предельно краткий обзор идей в области теории надежности, в котором – как и во всем чересчур кратком – имеется прорва прорех... Каждый понимает, что подобного рода обзоры всегда страдают от авторского субъективизма и неизбежной некомпетентности в тех или иных вопросах. Более того, это задача к тому же и крайне неблагодарная – можно обидеть друзей, которых забыл вспомнить.

Нас буквально захлестнул шквал публикаций по надежности: десятки книг, сотни статей... Что делать тому, кто ищет в этом океане щепочку правды?.. Одним словом похоже на ситуацию: «Пить – так пить!» – сказал котенок, когда несли его топить...

Найти стоящие книги по теории надежности в нынешнем потопе литературы становится все труднее и труднее... Иногда даже создается впечатление, что какого-либо отбора рукописей для публикации не производится вовсе: издательства просто «зашибают деньгу». Необходимо организовать какой-то Форум специалистов по надежности, который был бы способен осуществлять честную и жесткую оценку публикаций в регулярно издаваемом обзоре новых публикаций. Нужен какой-то «коллективный разум», помогающий выплыть котенку! Может, проще довериться немногим экспертам, которые помогут (пусть даже субъективно) сориентироваться в информационной пучине?

В противном случае, новое поколение специалистов по надежности потеряет всякую ориентацию в этом мире... Нерешенных задач даже чисто организационного толка очень много, и решить их можно только сообща.

Одно можно сказать уверенно: теория надежности жива! Надо использовать знания в нужном направлении. Нужда в чистой теории, может быть, и спала, но нужда в приложениях теории надежности к решению практических задач была, есть и будет!

Библиография

1. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. М.: Наука, 1965. 526 с.

2. Gnedenko B.V., Belyaev Yu.K., Solovyev A.D. Mathematical. Methods of Reliability Theory. New York: Academic Press, 1969. 518 p.

3. Barlow R., Proschan F. Mathematical Theory of Reliability. New York: John Wiley & Sons, 1965. XIII, 256 p.

4. Barlow R., Proschan F. Statistical Theory of Reliability and Life Testing. Probability models. New York: John Wiley & Sons, 1975.

5. Барлоу Р. и Прошан Ф. Математическая теория надежности. Под ред. Б.В. Гнеденко. М.: Сов. Радио, 1969. 488 с.

6. Барлоу Р., Прошан Ф. Статистическая теория надежности и испытания на безотказность / Под ред. И.А. Ушакова. М.: Наука, 1984. 328 с.

7. Козлов Б.А. и Ушаков И.А. Краткий справочник по расчету надежности радиоэлектронной аппаратуры. М.: Сов. радио, 1966. 432 с.

8. Козлов Б.А. и Ушаков И.А. Справочник по расчету надежности аппаратуры радиоэлектроники и автоматики. М.: Сов. радио,1975. 472 с.

9. Надежность технических систем: Справочник / Под ред. И.А. Ушакова. М.: Радио и связь, 1985. 608 с., ил.

10. Kozlov B.A., Ushakov I.A. Reliability Handbook. New York: Holt, Rinehart and Winston, 1970. 391 p.

11. Koslow B.A., Uschakow I.A. Handbbuch zur Berechnung der Zuverlassigkeitin Elektronik undAutomatentechnik. Berlin: Akademie-Verlag, 1978. 626 s.

12. Koslow B.A., Uschakow I.A. Handbbuch zur Berechnung der Zuverlassigkeit fur Ingen ieure. Munchen-Wien: Carl Hansen Verlag, 1979. 620 s.

13. Prorucka Spolehlivosti v Radioelektronice a Automatizacni Technice / I.A. Ushakov (ed.). Praha: SNTL, 1989.

14. Handbook of Reliability Engineering. / I.A. Ushakov (ed.). New York: John Wiley & Sons, 1994. 704 p.

15. Маликов И.М., Половко А.М., Романов Н.А. и др. Основы теории и расчета надежности. Л.: Судпромгиз, 1959. 141 с.

16. Половко А.М. (1964) Основы теории надежности. М.: Наука, 1964. 448 с.

17. Polovko A.M. Fundamentals of Reliability Theory. Amer. Society for Quality, 1985.

18. Шишонок Н.А., Репкин В.Ф., Барвинский Л.Л. Основы теории надежности и эксплуатации радиоэлектронной техники. М.: Сов. радио, 1964. 552 с.

19. Кордонский Х.Б. Приложения теории вероятностей в инженерном деле. М.: Физматгиз, 1963. 436 с.

20. Герцбах И.Б., Кордонский Х.Б. Модели отказов. М.: Сов. Радио, 1966. 166 с.

21. Герцбах И.Б. Модели профилактики. М.: Сов. Радио, 1969. 216 с.

22. Руденко Ю.Н., Ушаков И.А. Надежность систем энергетики / Под ред. Л.А. Мелентьева. М.: Наука, 1986. 252 с.

23. Руденко Ю.Н., Ушаков И.А. Надежность систем энергетики. / Изд. 2-е. Под ред. Б.В. Гнеденко. Новосибирск: Наука, 1989. 328 с.

24. Мирный Р.А, Соловьев А.Д. Оценки надежности системы по результатам испытаний ее компонент. В кн.: Кибернетику на службу коммунизму, т.2. М.: Энергия, 1964.

25. Беляев Ю.К., Дугина Т.Н., Чепурин Е.В. Вычисление нижней доверительной оценки для вероятности безотказной работы сложных систем. // Изв. АН СССР. Техн. кибернетика. 1967. № 2. С. 52-59.

26. Беляев Ю.К. Об упрощенных методах построения доверительных границ для надежности систем по ре-

зультатам испытаний компонент // Изв. АН СССР. Техн. Кибернетика. 1968. № 5.

27. Павлов И.В. Оценка надежности системы по результатам испытаний стареющих элементов // Изв. АН СССР. Техн. кибернетика. 1974. № 3.

28. Павлов И.В. Интервальное оценивание надежности системы по оценкам надежности ее компонент // Надежность и контроль качества. 1976. № 10.

29. Павлов И.В. Статистические методы оценки надежности сложных систем по результатам испытаний / Под ред. И.А. Ушакова. М.: Радио и связь, 1982. 168 с., ил.

30. Судаков Р.С. К вопросу об интервальном оценивании показателя надежности последовательной системы // Изв. АН СССР. Техн. Кибернетика. 1974. № 3.

31. Тескин О.И. Точные доверительные границы для надежности резервированных систем при безотказных испытаниях их элементов // Изв. АН СССР. Техн. Кибернетика. 1969. № 4.

32. Ушаков И.А. Оценка эффективности сложных систем. В кн. «Надежность радиоэлектронной аппаратуры». М.: Сов. радио, 1960.

33. Ушаков И.А. Эффективность функционирования сложных систем. В кн. «О надежности сложных систем». М., Сов. радио, 1966.

34. Дзиркал Э.В. Задание и проверка требований к надежности сложных изделий. М.: Радио и связь, 1974. 318 с.

35. Renyi A. Poisson-folyamat egy jemllemzese // Ann. Math. Statist. 1956. Vol. 1. № 4.

36. Ососков Г.А. Предельная теорема для потоков подобных событий // Теория вероятностей и ее приложения. 1956. Т. 1. № 2. С. 274-282.

37. Gnedenko B.V., Ushakov I.A. Probabilistic Methods in Reliability. New York: John Wiley & Sons, 1995.

38. Гнеденко Б.В. О ненагруженном дублировании // Изв. АН СССР. Техн. кибернетика. 1964. № 4. С. 3-12.

39. Гнеденко Б.В. О дублировании с восстановлением // Изв. АН СССР. Техн. кибернетика. 1964. № 5. С. 111-118.

40. Коваленко И.Н. Асимптотический метод оценки надежности сложных систем / В сб.: О надежности сложных систем. М.:Сов. радио, 1967.

41. Коваленко И.Н. Исследования по анализу надежности сложных систем. Киев: Наукова думка, 1975. 212 с.

42. Коваленко И.Н. Анализ редких событий при оценке эффективности и надежности систем. М.: Сов. радио, 1980.

43. Соловьев А.Д. Предельные теоремы для процесса гибели и размножения // Теория вероятностей и ее применения. 1968. № 4.

44. Соловьев А.Д. Резервирование с быстрым восстановлением. // Изв. АН СССР. Техн. кибернетика. 1970. № 1.

45. Гнеденко Д.Б., Соловьев А.Д. Одна общая модель резервирования с восстановлением // Изв. АН СССР. Техн. кибернетика. 1974. № 6. С. 113-118.

46. Гнеденко Д.Б., Соловьев А.Д. Оценка надежности сложных восстанавливаемых систем // Изв. АН СССР. Техн. кибернетика. 1975. № 3.

47. Королюк В.С., Турбин А.Ф. Математические основы фазового укрупнения сложных систем. Киев: Наукова Думка, 1978. 218 с.

48. Королюк В.С., Турбин А.Ф. Фазовое укрупнение сложных систем. Киев: Вища школа, 1978. 112 с.

49. Korolyuk V.S., Korolyuk V.V. Stochastic Models of Systems. Netherland: Kluwer Academic Publisher, 1999. 185 p.

50. Павлов И.В., Ушаков И.А. Асимптотическое распределение времени до выхода из ядра полумарковского процесса // Изв. АН СССР. Техн. кибернетика. 1978. № 5.

51. Anisimov V.V. Asymptotic analysis of reliability for switching systems in light and heavy traffic conditions. Recent Advances in Reliability Theory. / Ed. by N. Limnios and M. Nikulin. Boston-Basel-Berlin: Birkhauser, 2000.

52. Сильвестров Д.С. Об одном обобщении теоремы восстановления // ДАН СССР. Серия А11. 1976.

53. Ушаков И.А. Методы решения простейших задач оптимального резервирования при наличии ограничений. М.: Сов. радио, 1969. 176 с.

54. Райкин А.Л. Вероятностные модели функционирования резервных устройств. М.: Наука, 1971. 216 с.

55. Райкин А.Л. Элементы теории надежности технических систем. / Под ред. И.А. Ушакова. М.: Сов. Радио, 1978. 280 с., ил.

56. Волкович В.Л., Волошин А.Ф., Заславский В.А., Ушаков И.А. Модели и методы оптимизации надежности сложных систем. Киев: Наукова думка, 1992. 139 с.

57. Вопросы математической теории надежности / Под ред. Б.В. Гнеденко. М.: Наука, 1983. 376 с.

58. Седякин Н.М. Об одном физическом принципе в теории надежности // Изв. Ан СССР. Техн. кибернетика. 1966. № 3. С. 80-87.

59. Кордонский Х.Б., Герцбах И.Б. Модели отказов. М.: Сов. Радио, 1966. 165 с.

60. Перроте А.И., Карташов Г.Д., Цветаев К.Н. Основы ускоренных испытаний на надежность. М.: Сов. Радио, 1968. 224 с.

61. Bagdanavichius V., Nikulin M. Accelerated testing when process of production is unstable // Statist. and Probab. Letters. 1997. Vol. 35.

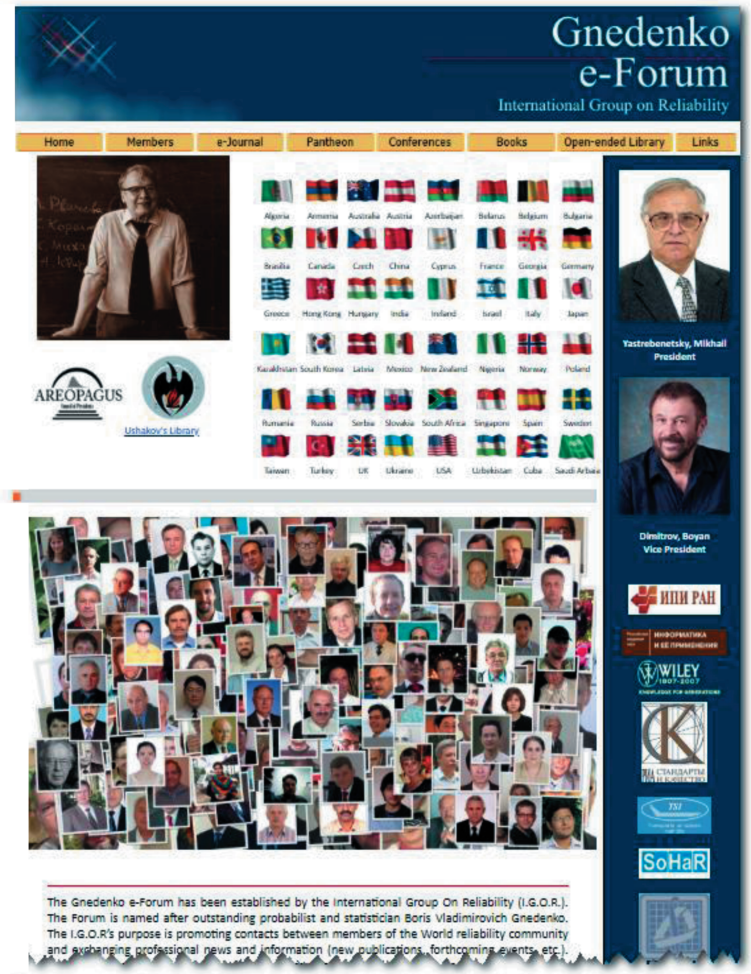
62. Вопросы математической теории надежности / Е.Ю. Барзилович, Ю.К. Беляев, В.А. Каштанов, И.Н. Коваленко, А.Д. Соловьев, И.А. Ушаков. Под ред. Б.В. Гнеденко. М.: Радио и связь, 1983. 376 с.

Об авторе

Игорь Алексе́евич Ушако́в (род. 22 января 1935, Ленинград, СССР, умер 27 февраля 2015, Сан-Диего, США) – профессор, доктор технических наук, советский и российский ученый, специалист в области теории надежности, исследования операций и оптимального резервирования.

GNEDENKO FORUM

INTERNATIONAL GROUP ON RELIABILITY



Gnedenko Forum основан в 2004 году неофициальной международной группой экспертов в области теории надёжности для профессиональной поддержки исследователей всего мира, заинтересованных в изучении и развитии научных, технических и пр. аспектов теории надёжности, анализа рисков и безопасности в теоретической и прикладной областях.

Форум создан в сети Интернет как некоммерческая организация. Его цель – привлечь к совместному обсуждению и общению технических специалистов, заинтересованных в развитии теории надёжности, безопасности и анализа рисков, независимо от места их проживания и принадлежности к тем или иным организациям.

Форум выступает в качестве объективного и нейтрального лица, распространяющего научную информацию для прессы и общественности по вопросам, касающимся безопасности, анализа риска и надёжности сложных технических систем. Он опубликует обзоры, технические документы, технические отчеты и научные эссе для распространения знаний и информации.

Форум назван в честь Бориса Владимировича Гнеденко, выдающегося советского математика, специалиста в области теории вероятностей и её приложений, академика Украинской академии наук. Форум является площадкой для распространения информации о стипендиях, академических и профессиональных позициях, открывающихся в профессиональной области надёжности, безопасности и анализа рисков по всему миру.

В настоящее время в Форуме состоят 500 участников из 47 стран мира.

Начиная с января 2006 года, Форум выпускает свой ежеквартальный журнал Reliability: Theory & Applications (www.gnedenko.net/RTA). Журнал зарегистрирован в Библиотеке Конгресса США (ISSN 1932-2321) и публикует статьи, критические обзоры, воспоминания, информацию и библиографии на теоретические и прикладные аспекты надёжности, безопасности, живучести, технического обслуживания и методы анализа и управления рисками.

С 2017 года журнал индексируется в международной базе Scopus.

Членство в GNEDENKO FORUM не подразумевает никаких обязательств. Достаточно прислать по адресу a.bochkov@gmail.com свою фотографию и краткую профессиональную биографию (резюме). Образцы можно найти на http://www.gnedenko.net/personalities.htm

www.gnedenko.net

ТРЕБОВАНИЯ РЕДАКЦИИ ПО ОФОРМЛЕНИЮ СТАТЕЙ В ЖУРНАЛАХ ИЗДАТЕЛЬСКОЙ ГРУППЫ IDT PUBLISHERS

Требования к формату статьи

Статья представляется в редакцию в электронном формате, в виде файла, созданного в текстовом редакторе MS Word из пакета Microsoft Office (файл с расширением *.doc или *.docx). Текст набирается черным шрифтом на листе формата А4 с полями: левое, верхнее, нижнее – 2 см; правое – 1,5 или 2 см. Минимальный объем статьи – 5 страниц, максимальный (может быть увеличен по согласованию с редакцией) – 12 страниц. При этом статья включает структурные элементы, описание которых представлено ниже.

Структура материала статьи

Представленные ниже структурные элементы статьи отделяются друг от друга *пустой строкой*. Отдельные примеры оформления, как это должно выглядеть в тексте, выделены *синим шрифтом*.

1) Название статьи

Название статьи представляется на русском и английском языках. Название статьи на русском языке должно соответствовать содержанию статьи. Англоязычное название должно быть грамотно с точки зрения английского языка, при этом по смыслу полностью соответствовать русскоязычному названию.

Оформление: Текст названия набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «полужирный». Точка в конце не ставится.

Пример:

Повышение надежности электронных компонентов
The Increasing of dependability of electronic components

2) Фамилия И.О. автора (авторов)

Данный структурный элемент для каждого автора включает:

- на русском языке – его фамилию и инициалы, после которых указывается сноска в виде цифры, набранной верхним индексом (надстрочным), которая ссылается на указание места работы автора. У фамилии автора, который будет контактировать с редакцией, также верхним индексом (после цифры) указывается символ «*»;

- на английском языке – его фамилию, имя и отчество в формате «Имя, инициал отчества, фамилия» (Ivan I. Ivanov). Фамилию на английском языке необходимо указывать в соответствии с заграничным паспортом или так, как она была указана в ранее опубликованных статьях. Если автор не имеет заграничного паспорта и/или публикаций, для транслитерации фамилии и имени необходимо использовать стандарт BSI.

Оформление: Текст ФИО набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «полужирный». ФИО разделяются запятой, точка в конце не ставится.

Пример:

Иванова А.А.[1], Петров В.В.[2*]
Anna A. Ivanova, Victor V. Petrov

3) Место работы автора (авторов)

Место работы авторов приводится на русском языке, перед указанием места набирается верхним индексом (надстрочным) соответствующая цифра сноски, указывающая на имя автора.

Оформление: Текст места работы набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный». Каждое место работы – с новой строки, точки в конце не ставятся.

Пример:

[1]Московский государственный университет, Российская Федерация, Москва
[2]Санкт-Петербургский институт теплоэнергетики, Российская Федерация, Санкт-Петербург

4) Адрес электронной почты автора, который будет вести переписку с редакцией

Оформление: Текст адреса набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный», все символы – строчные. Перед адресом набирается символ сноски «*». Точка в конце не ставится.

Пример:

*petrov_vv@aaa.ru

5) Резюме статьи

Данный структурный элемент включает структурированную аннотацию статьи объемом не менее 350 слов и не более 400 слов. Резюме представляется на русском и английском языках. Резюме должно содержать (желательно в явной форме) следующие разделы: Цель; Методы; Результаты; Выводы (на англ. яз.: Objective, Methods, Results, Conclusion). В резюме статьи не следует включать впервые введенные термины, аббревиатуры (за исключением общеизвестных), ссылки на литературу.

Оформление: Текст резюме набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный», кроме слов «**Резюме.**», «**Цель.**», «**Методы.**», «**Выводы.**» («**Objective.**», «**Methods.**», «**Results.**», «**Conclusion.**»), которые (вместе с точкой) должны иметь начертание шрифта «полужирный». Текст резюме на отдельные абзацы не разделяется (набирается в один абзац).

Пример (на рус. яз.):

Резюме. Цель. Предложить подход … с учетом современных методик. **Методы.** В статье применяются методы математического анализа,…, теории вероятностей. **Результаты.** С использованием предложенного метода получено… **Заключение.** Предлагаемый в статье подход позволяет…

6) Ключевые слова

Указывается 5-7 слов по теме статьи. Желательно, чтобы ключевые слова дополняли резюме (аннотацию) и название статьи. Ключевые слова указываются на русском и английском языках.

Оформление: Текст набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный», кроме слов «**Ключевые слова:**» («**Keywords:**») которые (вместе с двоеточием) должны иметь начертание «полужирный». Текст на отдельные абзацы не разделяется (набирается в один абзац). В конце ставится точка.

Пример (на рус. яз.):

Ключевые слова: надежность, функциональная безопасность, технические системы, управление рисками, техническая эффективность.

7) Текст статьи

Рекомендуется структурировать текст статьи в виде следующих разделов: Введение, Обзор источников, Методы, Результаты, Обсуждение, Заключение (или выводы). Рисунки и таблицы включаются в текст статьи (положение рисунков должно быть «в тексте», а не «за текстом» или «перед текстом»; без «обтекания текстом»).

Оформление:

Заголовки разделов набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, с абзацным отступом слева 1,25 см. Начертание шрифта «полужирный». Заголовки разделов (кроме введения и заключения (выводов)) могут иметь нумерацию арабскими цифрами с точкой после номера раздела. Номер с точкой отделяются от заголовка неразрывным пробелом (Ctrl+Shift+Spacebar).

Текст разделов набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, с абзацным отступом слева 1,25 см. Начертание шрифта «обычный» Текст разделов разделяется на отдельные абзацы. Абзацный отступ не применяется для абзаца, следующего за формулой и содержащего пояснения к формуле, например:

где n – количество изделий.

Пример:

1. Состояние вопроса повышения надежности электронных компонентов

Проведенный анализ отечественной и зарубежной литературы по теме исследования показал, что…

Рисунки (фотографии, скриншоты) должны быть хорошего качества, пригодные для печати. Разрешение рисунка – не хуже 300 dpi. Если рисунок представляет собой схему, диаграмму, чертеж и т.п., то желательно вставлять такой рисунок в текст в редактируемом формате (MS Visio). Все рисунки должны иметь подрисуночные подписи. Рисунки нумеруются арабскими цифрами, по порядку следования в тексте. Если рисунок в тексте один, то он не нумеруется. Отсылки на рисунки оформляются следующим образом: «На рис. 3 указано, что …» или «Указано, что … (см. рис. 3)». Сокращение «рис.» и номер рисунка (если он есть) всегда разделяются неразрывным пробелом (Ctrl+Shift+Spacebar). Подрисуночная подпись включает порядковый номер рисунка и его название. Располагается на следующей строке после рисунка и выравнивается по центру:

Рис. 2. Описание жизненно важных процессов

Точка после подрисуночной подписи не ставится. *При выравнивании по центру абзацный отступ всегда должен отсутствовать!* Все обозначения, приведенные на рисунках, необходимо пояснять в основном или подрисуночном тексте. Недопустимы отличия в обозначениях на рисунках и в тексте (включая различие прямых/наклонных символов). *При проблемах с верстkой рисунков, вставленных в текст, авторы должны по запросу редакции предоставить данные рисунки в графическом формате, в виде файлов с расширениями* *.tiff, *.png, *.gif, *.jpg, *.eps.

Таблицы должны быть хорошего качества, пригодные для печати. Таблицы должны быть пригодны для редактирования (а не отсканированные или в виде рисунков). Все таблицы должны иметь заголовки. Таблицы нумеруются арабскими цифрами, по порядку следования в тексте. Если таблица в тексте одна, то она не нумеруется. Отсылки на таблицы оформляются следующим образом: «В табл. 3 указано, что …» или «Указано, что … (см. табл. 3)». Сокращение «табл.» и номер таблицы (если он есть) всегда разделяются неразрывным пробелом (Ctrl+Shift+Spacebar). Заголовок таблицы включает порядковый номер таблицы и ее название. Располагается на строке, предшествующей таблице и выравнивается по центру:

Табл. 2. Описание жизненно важных процессов

Точка после заголовка таблицы не ставится. *При выравнивании по центру абзацный отступ всегда должен отсутствовать!* Все обозначения (символы), приведен-

ные в таблицах, необходимо пояснять в основном тексте. Недопустимы отличия в обозначениях в таблице и в тексте (включая различие прямых/наклонных символов).

Математические обозначения в тексте набираются заглавными и строчными буквами латинского, греческого и русского алфавитов. Латинские символы всегда набираются наклонным шрифтом (курсивом), кроме обозначений функций, таких как sin, cos, max, min и т.п., которые набираются прямым шрифтом. Греческие и русские символы всегда набираются прямым шрифтом. Размер шрифта основного текста и математических обозначений (включая формулы) должен быть одинаков; верхние и нижние индексы масштабируются в MS Word автоматически.

Формулы могут быть включены непосредственно в текст, например:

Пусть $y = a \cdot x + b$, тогда…,

либо набираться в отдельной строке, с выравниванием по центру, например:

$$y = a \cdot x + b.$$

При наборе формул как в тексте, так и в отдельной строке, знаки препинания должны ставиться по обычным правилам – точка, если формулой заканчивается предложение; запятая (или отсутствие знака препинания), если предложение после формулы продолжается. Для разделения формулы и текста рекомендуется для строки с формулой устанавливать вертикальные отступы (6 пт перед, 6 пт после). Если в тексте статьи делается отсылка на формулу, то такая формула обязательно набирается отдельной строкой, по правому краю которой указывается номер формулы в круглых скобках, например:

$$y = a \cdot x + b. \qquad (1)$$

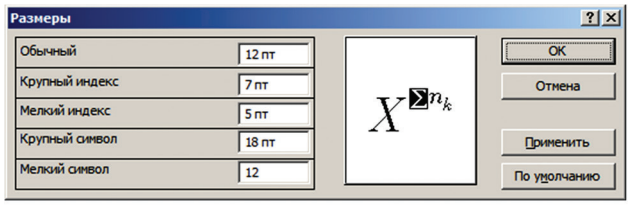
Если формула набирается в отдельной строке и имеет номер, то данная строка выравнивается по правому краю, а формула и номер разделяются знаком табуляции; позиция табуляции (в см) выбирается таким образом, чтобы формула располагалась примерно по центру. Формулы, на которые в тексте делаются отсылки, нумеруются арабскими цифрами, по порядку следования в тексте.

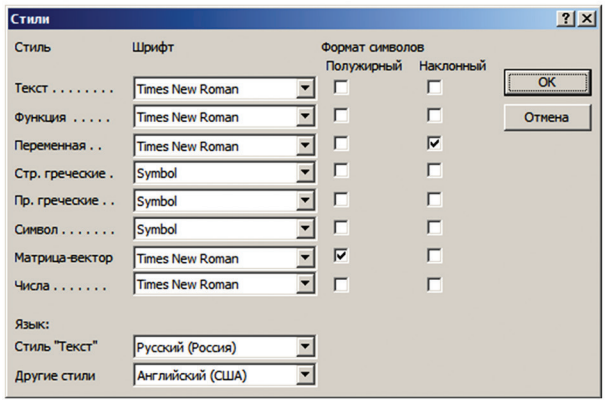
Простые формулы следует набирать без применения формульного редактора (использовать в MS Word русские и латинские буквы, а также меню «Вставка» + «Символ», если требуются греческие буквы и математические операторы), с соблюдением требуемого наклона для латинских символов, например:

$$\Omega = a + b \cdot \theta.$$

Если формула набирается без применения редактора формул, то между буквами и знаками «+», «–», «=» должны быть набраны неразрывные пробелы (Ctrl+Shift+Spacebar).

Сложные формулы набираются с применением редактора формул. Для отсутствия проблем с редактированием формул и их верстской настоятельно рекомендуется использовать редакторы Microsoft Equation 3.0 или MathType 6.x. Для обеспечения корректного ввода формул (размер символов, их наклон и т.д.) рекомендуемые настройки редактора приведены на рисунках ниже.





При наборе формул в редакторе формул, если требуются скобки, то следует использовать скобки из формульного редактора, а не набирать их на клавиатуре (для корректной высоты скобок в зависимости от содержимого формулы), например (Equation 3.0):

$$Z = \frac{a \cdot \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{m} y_i \right)}{n+m}. \qquad (2)$$

Сноски в тексте нумеруются арабскими цифрами, размещаются постранично. В сносках могут быть размещены: ссылки на анонимные источники в сети Интернет, ссылки на учебники, учебные пособия, ГОСТы, статистические отчеты, статьи в общественно-политических газетах и журналах, авторефераты, диссертации (если нет возможности процитировать статьи, опубликованные по результатам диссертационного исследования), комментарии автора.

Отсылка на библиографический источник указывается в тексте статьи в квадратных скобках, а источники приводятся в библиографическом списке в порядке их упоминания в тексте (затекстовые ссылки). Страница указывается внутри скобок, через запятую и пробел после номера источника: [6, с. 8]

8) Благодарности

В этом разделе указываются все источники финансирования исследования, а также благодарности людям, которые участвовали в работе над статьей, но не

являются ее авторами. Участие в работе над статьей подразумевает: рекомендации по совершенствованию исследования, предоставление пространства для исследования, ведомственный контроль, получение финансовой поддержки, одиночные виды анализа, предоставление реагентов/пациентов/животных/прочих материалов для исследования.

Оформление:

Сведения набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

9) Библиографический список

В библиографический список включаются только рецензируемые источники (статьи из научных журналов и монографии), упоминающиеся в тексте статьи. Нежелательно включать в библиографический список авторефераты, диссертации, учебники, учебные пособия, ГОСТы, информацию с сайтов, статистические отчеты, статьи в общественно-политических газетах, на сайтах и в блогах. Если необходимо сослаться на такую информацию, следует поместить информацию об источнике в сноску.

При описании источника следует указывать его DOI, если удается его найти (для зарубежных источников удается это сделать в 95% случаев).

Ссылки на принятые к публикации, но еще не опубликованные статьи должны быть помечены словами «в печати»; авторы должны получить письменное разрешение для ссылки на такие документы и подтверждение того, что они приняты к печати. Информация из неопубликованных источников должна быть отмечена словами «неопубликованные данные/документы», авторы также должны получить письменное подтверждение на использование таких материалов.

В ссылках на статьи из журналов должны быть обязательно указаны год выхода публикации, том и номер журнала, номера страниц.

В описании каждого источника должны быть представлены все авторы.

Ссылки должны быть верифицированы, выходные данные проверены на официальном сайте журналов и/или издательств.

Оформление:

Оформление ссылок (в русскоязычной версии журнала) должно выполняться по ГОСТ Р 7.0.5-2008. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления.

Библиографические ссылки набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, с абзацным отступом слева 1,25 см. Начертание шрифта «обычный» (см. примеры оформления в ГОСТ Р 7.0.5). Каждая запись имеет нумерацию арабскими цифрами с точкой после номера раздела. Номер с точкой отделяются от записи неразрывным пробелом (Ctrl+Shift+Spacebar).

10) Сведения об авторах

Фамилия, имя, отчество полностью (на русском и английском языках); полный почтовый адрес (включая индекс, город и страну); полное наименование места работы, занимаемая должность; ученая степень, ученое звание, почетные звания; членство в общественных союзах, организациях, ассоциациях и т.д.; официальное англоязычное название учреждения (для версии на английском языке); адрес электронной почты; перечень и номера журналов, в которых ранее публиковались статьи автора; фото авторов для публикации в журнале.

Оформление:

Сведения набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

11) Вклад авторов в статью

Следует указать подробно, каким из авторов что сделано в статье. Например: Автором А. выполнен анализ литературы по теме исследования, автором Б. разработана модель объекта в реальных условиях эксплуатации, выполнен расчет примера и т.д. Даже если у статьи один автор, то требуется указание его вклада.

Оформление:

Сведения набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

12) Конфликт интересов

Конфликт интересов – это условия, при которых у людей возникают вступающие в конфликт или конкурирующие интересы, способные повлиять на принятие редакторского решения. Конфликты интересов могут быть потенциальными или осознанными, а также реально существующими. На объективность могут повлиять личные, политические, финансовые, научные или религиозные факторы.

Автор обязан уведомить редакцию о реальном или потенциальном конфликте интересов, включив информацию о конфликте интересов в статью.

Если конфликта интересов нет, автор должен также сообщить об этом. Пример формулировки: «Автор заявляет об отсутствии конфликта интересов».

Оформление:

Текст набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

Содержание выпусков журнала «Надёжность» за 2025 год

Том 25, № 1 (2025)

Том 25, № 2 (2025)

Том 25, № 3 (2025)

Том 25, № 4 (2025)

GUIDELINES FOR PUBLICATION IN THE JOURNAL «DEPENDABILITY»

STRUCTURAL DEPENDABILITY

- Calculation methods, simulation processes and methods, application software packages, practical calculations of complex system dependability
- Mathematical maintenance theory, practical results of complex systems operation, system lifecycle, optimisation of dependability and cost at lifecycle stages
- Test methods, criteria for making decisions based on test results, accelerated tests, methods for assessing the dependability of systems based on test results

FUNCTIONAL DEPENDABILITY

- Object, subject, and objectives of research, functional dependability indicators, terminology, principles and methods of calculation
- Methods for assessing and predicting the dependability of software, hardware and software systems, taking into account faults, software errors, operator errors, input information errors
- Processes and methods of functional dependability: functionally dependable software design processes, methods for building information processing and control algorithms immune to faults and operator errors, methods and techniques of input information error management, practical results

FUNCTIONAL SAFETY OF SYSTEMS

- Functional safety indicators; safety functions, safety integrity
- Mathematical methods and models for defining the requirements for safety integrity and permissible time of hazardous failure detection, functional safety models of multichannel and multilevel systems
- Processes of functional safety assurance at all lifecycle stages

FAULT TOLERANCE OF SYSTEMS

- Methods of passive failure protection, mathematical models of structural redundancy, gradual degradation of redundant systems, fault masking, results of passive failure protection
- Methods of active protection against structural failures and information process errors, principles and methods of active protection, theoretical foundations of active protection, technical solutions, efficiency evaluations of active protection

RISK MANAGEMENT

- General risk theory, matters of risk formalisation methodology
- Facility-related risk classification. Principles and methods of risk assessment Methods for defining acceptable levels of risk. Methodology for managing risks of various nature
- Methods and models for identifying integral risks

CERTIFICATION AND STANDARDISATION

- Accreditation of certification bodies and testing laboratories: the state of the art in Russia and abroad. Methods of certifying software and hardware systems according to the requirements of international functional safety standards
- Mandatory and voluntary certification: experience, opinions, suggestions
- System quality and dependability certification: regulatory requirements, test methods, practical results
- The effect of the Law On Technical Regulation on the development of the theory and practice of dependability and functional safety
- State of the art and future trends in the standardisation of dependability, fault tolerance, and survivability, functional safety and risk management

INNOVATIVE TECHNOLOGIES IN DEPENDABILITY AND SAFETY

- Methods for proactively managing dependability and safety
- Methods for assessing dependability and safety in the absence of complete data
- Standardisation of dependability and safety indicators in large systems
- Methods for designing the dependability and safety of unique critical systems

TECHNICAL EFFICIENCY OF CONTROL AND MANAGEMENT SYSTEMS

- Functional and technical efficiency indicators
- Methods for assessing the technical efficiency of control and management systems
- Design processes for control and management systems with superior efficiency
- Regulatory requirements for technical efficiency of control and management systems

TECHNOLOGICAL ASSET MANAGEMENT

- Technological asset management in large systems
- Methodology of technological asset management
- Management of technological risks in large systems
- Management of resources of composite entities
- Business unit performance evaluation
- Corporate technological asset management platform

BIG DATA. CONTROL AND MANAGEMENT SYSTEMS AND ARTIFICIAL INTELLIGENCE

- Processes of data wrangling and feature selection for machine learning
- Methods and algorithms of machine learning, development and effects of Big Data application
- Predicting the state dynamics of control and management systems
- Using artificial intelligence in dependability and safety

METHODS AND SYSTEMS OF INFORMATION SECURITY

- Methods for protecting information in automated control and management systems
- Methods for ensuring information security in software
- Information security systems
- Methods and processes for comprehensive functional safety and information security in control and management systems
- Processes for confirming compliance with information security requirements

SYSTEMS ANALYSIS IN DEPENDABILITY AND SAFETY

- Methodology of analytical and system research in dependability and safety
- System research in management and decision-making. Strategic and operational management
- Data collection, processing and prediction. Statistics, probability theory, combinatorics, methods for measuring and simulation in systems analysis studies
- Managing information as part of systems analysis, control and management, decision-making systems

INTELLIGENT TRANSPORTATION SYSTEMS

- Purpose and structure of modern ITS. Information and communication technologies and solutions as part of ITS development and operation
- Application and development of international practices in the process of Russian ITS development
- Role and place of safety systems within ITS
- Neural systems and artificial intelligence in ITS
- Reliable data and detection system
- Improved security through video analytics

TERMINOLOGY OF DEPENDABILITY, FAULT TOLERANCE, SAFETY, RISKS, AND SURVIVABILITY

- Methodological matters of dependability, fault tolerance, safety, risk, and survivability terminology research
- Modern concepts in dependability, fault tolerance, safety, risks, and survivability
- The problem of harmonisation and standardisation of terminology in dependability, fault tolerance, safety, risks, and survivability adopted in Russia with the international practice
- Matters of standardisation of the terminology in dependability, fault tolerance, safety, risks, and survivability

ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ

АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
И ПРОЕКТНО-КОНСТРУКТОРСКИЙ ИНСТИТУТ
ИНФОРМАТИЗАЦИИ, АВТОМАТИЗАЦИИ И СВЯЗИ
НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСОРТЕ» (АО «НИИАС»)

АО «НИИАС» — ведущий отраслевой научно-технологический институт холдинга «РЖД» в области автоматизации и управления сложными технологическими процессами на железнодорожном транспорте.

ЦЕЛИ:

- эффективность;
- безопасность;
- надежность перевозок.

Направления деятельности:

- системы интервального регулирования и управления движением поездов;
- бортовые устройства безопасности;
- комплексные решения для цифровой станции;
- роботизация технологических процессов;
- моделирование технологических процессов и логистической инфраструктуры;
- информационная безопасность и кибербезопасность;
- транспортная безопасность;
- геоинформационные системы и технологии ДЗЗ;
- проектно-изыскательские работы;
- BIM-технологии;
- лабораторно-испытательный комплекс.

МЫ — ЛЮДИ ДЕЛА